MAX RADIUS Configuration Guide

Ascend Communications, Inc.
Part Number: 7820-0581-002
For software version 6.0.0

Ascend Customer Service

You can request assistance or additional information by telephone, email, fax, or modem, or over the Internet.

Obtaining Technical Assistance

If you need technical assistance, first gather the information that Ascend Customer Service will need for diagnosing your problem. Then select the most convenient method of contacting Ascend Customer Service.

Information you will need

Before contacting Ascend Customer Service, gather the following information:

- Product name and model
- Software and hardware options
- Software version
- Service Profile Identifiers (SPIDs) associated with your product
- Your local telephone company’s switch type and operating mode, such as AT&T 5ESS Custom or Northern Telecom National ISDN-1
- Whether you are routing or bridging with your Ascend product
- Type of computer you are using
- Description of the problem

How to contact Ascend Customer Service

After you gather the necessary information, contact Ascend in one of the following ways:

Telephone in the United States	800-ASCEND-4 (800-272-3634)
Telephone outside the United States	510-769-8027 (800-697-4772)
Austria/Germany/Switzerland	(+33) 492 96 5672
Benelux	(+33) 492 96 5674
France	(+33) 492 96 5673
Italy	(+33) 492 96 5676
Japan	(+81) 3 5325 7397
Middle East/Africa	(+33) 492 96 5679
Scandinavia	(+33) 492 96 5677
Spain/Portugal	(+33) 492 96 5675
UK	(+33) 492 96 5671
Email	support@ascend.com
Email (outside US)	EMEAsupport@ascend.com

Facsimile (FAX)	510-814-2312
Customer Support BBS by modem	510-814-2302

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
1701 Harbor Bay Parkway
Alameda, CA 94502

Need information about new features and products?

Ascend is committed to constant product improvement. You can find out about new features and other improvements as follows:

- For the latest information about 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`

Important safety instructions

The following safety instructions apply to the MAX:

1 Read and follow all warning notices and instructions marked on the product or included in the manual.

2 The maximum recommended ambient temperature for MAX models is 104° Fahrenheit (40° Celsius). Take care to allow sufficient air circulation or space between units when the MAX is installed in a closed or multi-unit rack assembly, because the operating ambient temperature of the rack environment might be greater than room ambient.

3 Slots and openings in the cabinet are provided for ventilation. To ensure reliable operation of the product and to protect it from overheating, these slots and openings must not be blocked or covered.

4 Installation of the MAX in a rack without sufficient air flow can be unsafe.

5 If installed in a rack, the rack should safely support the combined weight of all equipment it supports. A fully loaded redundant-power MAX weighs 56 lbs (25.5 kg). A fully loaded single-power MAX weighs 30 lbs (13.6 kg).

6 The connections and equipment that supply power to the MAX should be capable of operating safely with the maximum power requirements of the MAX. In the event of a power overload, the supply circuits and supply wiring should not become hazardous. The input rating of the MAX is printed on its nameplate.

7 Models with AC power inputs are intended for use with a three-wire grounding type plug—a plug which has a grounding pin. This is a safety feature. Equipment grounding is vital to ensure safe operation. Do not defeat the purpose of the grounding type plug by modifying the plug or using an adapter.

8 Before installation, use an outlet tester or a voltmeter to check the AC receptacle for the presence of earth ground. If the receptacle is not properly grounded, the installation must not continue until a qualified electrician has corrected the problem. Similarly, in the case of DC input power, check the DC ground(s).

9 If a three-wire grounding type power source is not available, consult a qualified electrician to determine another method of grounding the equipment.

10 Models with DC power inputs must be connected to an earth ground through the terminal block Earth/Chassis Ground connectors. This is a safety feature. Equipment grounding is vital to ensure safe operation.

11 Before installing wires to the MAX's DC power terminal block, verify that these wires are not connected to any power source. Installing live wires (that is, wires connected to a power source) is hazardous.

12 Connect the equipment to a 48VDC supply source that is electrically isolated from the AC source. The 48VDC source should be reliably connected to earth ground.

13 Install only in restricted-access areas in accordance with Articles 110-16, 110-17, and 110-18 of the National Electrical Code, ANSI/NFPA 70.

14 Do not allow anything to rest on the power cord, and do not locate the product where persons will walk on the power cord.

15 Do not attempt to service this product yourself. Opening or removing covers can expose you to dangerous high voltage points or other risks. Refer all servicing to qualified service personnel.

16 General purpose cables are provided with this product. Special cables, which might be required by the regulatory inspection authority for the installation site, are the responsibility of the customer.

17 When installed in the final configuration, the product must comply with the applicable Safety Standards and regulatory requirements of the country in which it is installed. If necessary, consult with the appropriate regulatory agencies and inspection authorities to ensure compliance.

18 A rare phenomenon can create a voltage potential between the earth grounds of two or more buildings. If products installed in separate buildings are *interconnected*, the voltage potential might cause a hazardous condition. Consult a qualified electrical consultant to determine whether or not this phenomenon exists and, if necessary, implement corrective action before interconnecting the products.

In addition, if the equipment is to be used with telecommunications circuits, take the following precautions:

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.

  Avoid using equipment connected to telephone lines (other than a cordless telephone) during an electrical storm. There is a remote risk of electric shock from lightning.
- Do not use a telephone or other equipment connected to telephone lines to report a gas leak in the vicinity of the leak.

Contents

Chapter 8 Setting Up RADIUS Accounting 8-1

Chapter 9 Reference to RADIUS Attributes 9-1

Figures

Tables

About This Guide

How to use this guide

This guide describes how to install and start up the RADIUS daemon, and provides details on how to set up authentication, WAN connections, routing and bridging configurations, ATMP tunnels, and accounting records in RADIUS. Use this guide in conjunction with other manuals in the documentation set.

What this guide contains

This guide contains:

- Chapter 2, “Installing and Starting RADIUS,” describes how to install and start up the RADIUS daemon.
- Chapter 1, “Getting Acquainted with RADIUS,” introduces RADIUS authentication and accounting, and provides an overview of RADIUS files and attributes.
- Chapter 8, “Setting Up RADIUS Accounting,” describes how to use RADIUS for your accounting needs.
- Chapter 3, “Setting Up RADIUS Authentication,” describes the initial steps you must take to set up RADIUS to authenticate MAX users.
- Chapter 4, “Setting Up WAN Connections in RADIUS,” shows you how to set up WAN connections and specify the services, protocols, and other MAX features that an operator is permitted to access.
- Chapter 5, “Setting Up Frame Relay in RADIUS,” describes how to configure a frame relay connection in a RADIUS user profile.
- Chapter 6, “Setting Up Routing and Bridging Links,” describes how to configure IP routing, IPX routing, and protocol-independent bridging for RADIUS user profiles.
- Chapter 7, “Setting Up Virtual Private Networks in RADIUS,” describes how to use RADIUS to set up an Ascend Tunnel Management Protocol (ATMP) configuration.
- Chapter 9, “Reference to RADIUS Attributes,” provides a description of each RADIUS attribute.
- Appendix A, “Troubleshooting, ” provides strategies for diagnosing and resolving problems that may occur when you use RADIUS with the MAX.
- Appendix B, “Attribute and Parameter Cross Reference, ” provides tables that cross reference RADIUS attributes and MAX parameters.

This guide also contains an index.

Who should read this guide

This guide is intended for the person who will configure and maintain RADIUS and the MAX. You must have a basic understanding MAX security and configuration, and be familiar with authentication servers and networking concepts.

For information about MAX security, see the *MAX Security Supplement*. For details on how to configure the MAX, see the *MAX ISP and Telecommuting Configuration Guide*.

Documentation conventions

This section explains all the special characters and typographical conventions in this manual.

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

Manual set

The MAX 6000 Series Documentation Set consists of the following manuals:

- *RADIUS Configuration Guide (this guide)*
- *Getting Started*
- *ISP and Telecommuting Configuration Guide*
- *MIF Supplement*
- *Reference Guide*
- *Security Supplement*

Related publications

This guide and documentation set do not provide a detailed explanation of products, architectures, or standards developed by other companies or organizations.

Here are some related publications that you may find useful:

- *The Guide to T1 Networking, William A. Flanagan*
- *Data Link Protocols, Uyless Black*
- *The Basics Book of ISDN, Motorola University Press*
- *ISDN, Gary C. Kessler*
- *TCP/IP Illustrated, W. Richard Stevens*
- *Firewalls and Internet Security, William R. Cheswick and Steven M. Bellovin*

Getting Acquainted with RADIUS

1

This chapter introduces RADIUS authentication and accounting, and provides an overview of the files and attributes that the RADIUS server uses. This chapter contains:

How does the MAX use RADIUS?

RADIUS provides a central location for storing these types of information:

- Authentication attributes
- Configuration data for establishing a WAN connection for an incoming call
- Dialout information
- Static routes and filters
- Accounting information

RADIUS maintains authentication, incoming call configuration, dialout, routing, and filter information in individual user profiles. Each user profile consists of a series of attributes. These attributes indicate a user name and password, and enable you to configure routing, bridging, call management, and restrictions on the types of MAX resources a caller can access.

How does RADIUS authentication work?

A single RADIUS server can administer multiple security systems, maintaining profiles for thousands of users. RADIUS vastly increases the number of authentication entries that the MAX can support. Without RADIUS, you must limit yourself to the number of local Connection profiles the MAX supports.

When you use RADIUS authentication, these events take place:

1. A user dialing in from a modem, ISDN terminal adaptor, or bridge/router attempts to open a connection to the MAX, and the MAX determines that it must use a RADIUS user profile to authenticate the user.
2. The MAX sends the user connection request to the RADIUS server.
3. The RADIUS server carries out one or more of these tasks:
   - Performs Calling Line ID (CLID) authentication on incoming calls by checking the calling party's phone number.
   - Performs called-number authentication on incoming calls by checking the number the user dialed to reach the MAX. Called-number authentication is also known as Dialed Number Information Service (DNIS) authentication.
   - Obtains the user's name and password using Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), or Microsoft CHAP (MS-CHAP) authentication. PAP is a PPP authentication protocol that provides a simple method for a host to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment, and does not use encryption. CHAP is also a PPP authentication protocol, but it is more secure than PAP. CHAP provides a way to periodically verify the identity of a host using a three-way handshake and encryption. Authentication takes place upon initial link establishment. The MAX can repeat the authentication process any time after the connection takes place. MS-CHAP is the Windows NT version of CHAP, which uses DES and MD4 encryption. Using MS-CHAP, an Ascend unit can authenticate a Windows NT system, and a Windows NT system can authenticate an Ascend unit.
   - Performs a UNIX login.
   - Forwards the connection request to an external authentication server, such as a Security Dynamics ACE/Server or Enigma Logic SafeWord server.
4. The RADIUS server sends an authentication response to the MAX.

   If authentication is unsuccessful, the MAX refuses the connection. If authentication is successful, the MAX receives a list of attributes from the user profile in the RADIUS server's database and establishes network access for the caller.
5. The MAX notifies the RADIUS server that the session has begun.

   The MAX also notifies the RADIUS when the session ends. If you enable accounting, the RADIUS server can generate accounting records.

How does RADIUS accounting work?

RADIUS accounting is a way to log information about three types of events:

- Start session

  This event denotes the beginning of a session with the MAX. Information about this event appears in an accounting Start record.
- Stop session

  This event denotexs the end of a session with the MAX. Information about this event appears in an accounting Stop record.
- Failure-to-start session

This event denotes that a login attempt has failed. Information about this event appears in an accounting Failure-to-start record.

When the MAX recognizes one of these events, it sends an accounting request to RADIUS. When the accounting server receives the request, it combines the information into a record and timestamps it. Each type of accounting record contains attributes associated with an event type, and can show the number of packets the MAX transmitted and received, the protocol in use, the user name and IP address of the client, and so on.

You can use RADIUS accounting for either of these purposes:

- To gather billing information.

  You can use the information in an accounting record to determine who called, how long the session lasted, and how much traffic occurred during the session.
- To perform troubleshooting of RADIUS and MAX operations.

  Accounting records can contain information about how many login failures occurred, and can describe the characteristics of the failed attempts.

What types of applications does RADIUS support?

This section describes some common RADIUS applications.

Simple RADIUS authentication and accounting

In Figure 1-1, the RADIUS server performs both authentication and accounting. This configuration does not use a backup server.

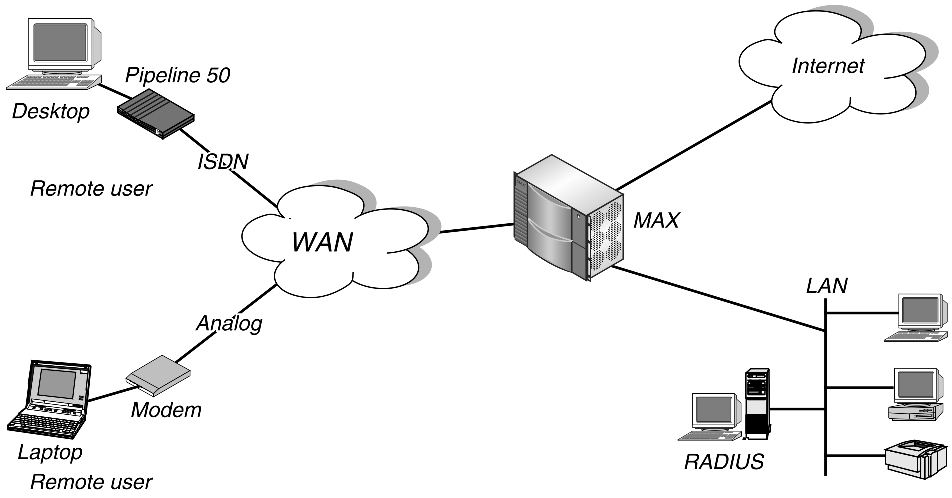

Figure 1-1. Simple RADIUS authentication and accounting

This configuration is ideal for cost-conscious service providers and corporations that do not want to invest in different machines for security and backup.

RADIUS authentication and accounting with a backup server

In Figure 1-2, a service provider or corporate office has a second RADIUS server acting as a backup. If the primary RADIUS server fails, the MAX automatically contacts the secondary RADIUS server to authenticate a user. If the secondary server fails, you can bring in a third RADIUS server as a backup. You can use the secondary server as a backup accounting server as well.

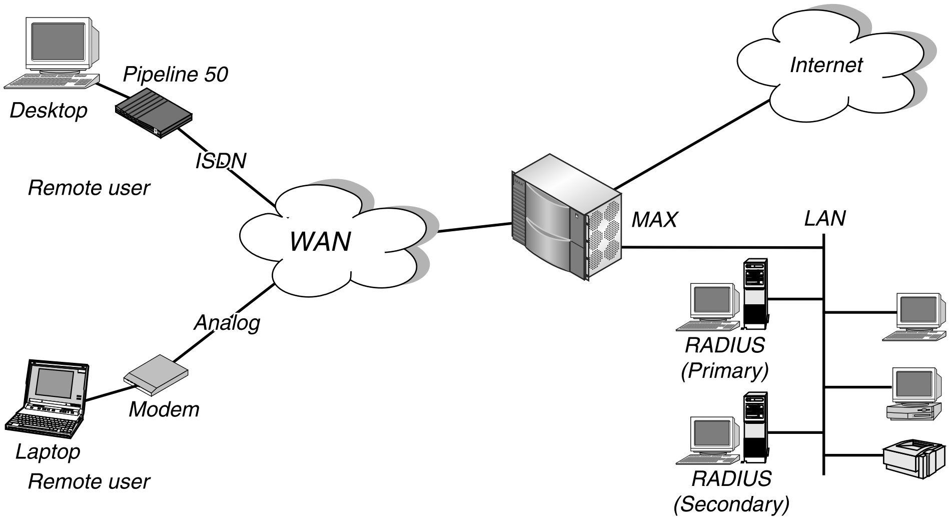

Figure 1-2. RADIUS authentication and accounting with a backup server

RADIUS with an external security-card server

For more secure networks, a service provider or corporate office can use RADIUS as a front end to a security-card authentication server, such as Security Dynamics ACE/Server or Enigma Logic's SafeWord server.

Figure 1-3 illustrates an environment that includes an Ascend Pipeline as the calling unit, an NAS (the MAX), a RADIUS server, and an external authentication server.

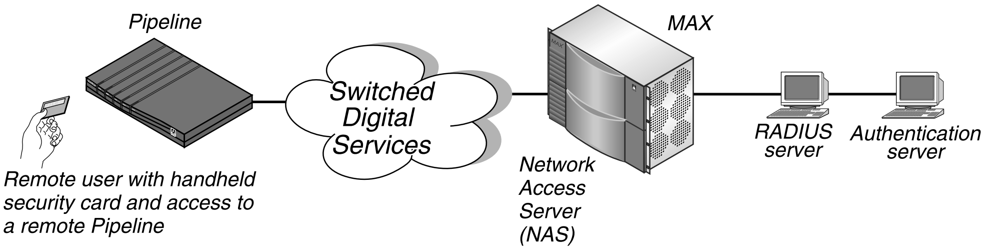

Figure 1-3. RADIUS with an external security-card server

For complete information on configuring RADIUS to work with security-card authentication servers, see "Setting up security-card authentication" on page 3-25.

Using RADIUS to sign up new customers

In Figure 1-4, the server provider has a RADIUS server and a separate registration server. When a new customer connects to the network using the name and password specified in the company's advertising, the MAX passes the request to the registration server. The server prompts the user to enter sign-up information.

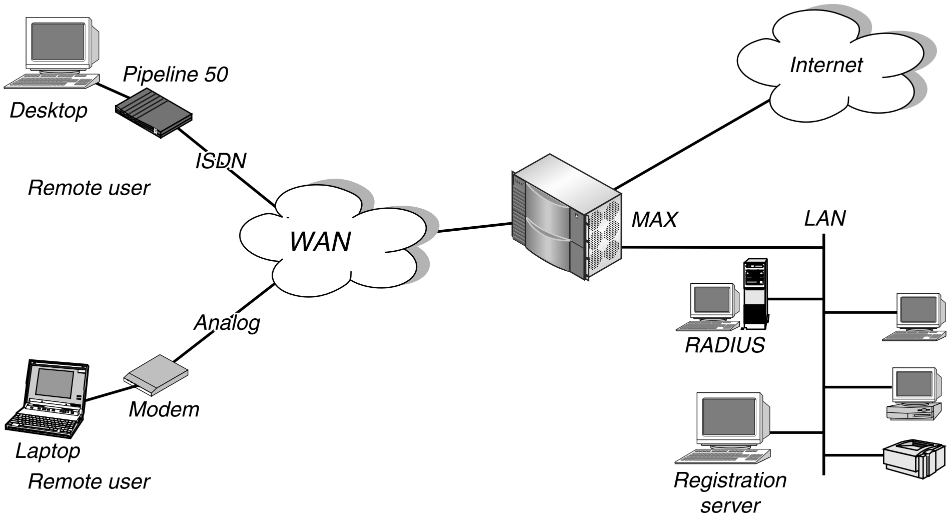

Figure 1-4. Using RADIUS to sign up new customers

A user cannot access any other resource on the system until he or she provides all the registration details and signs up for the service. After a user completes the registration procedure, the server issues a permanent user name and password.

What files does RADIUS use?

The RADIUS server uses the files listed in Table 1-1.

Table 1-1. RADIUS files

File name	Default location	Description
radiusd	/etc/raddb	The RADIUS daemon you use with a flat ASCII users file. If you require RADIUS accounting or any of the attributes provided by Ascend as extensions to the Livingston RADIUS daemon, you must use the Ascend RADIUS daemon, version 1.16 (dated 7/25/95) or later. For information on running the radiusd daemon, see "Running the daemon with a flat ASCII users file" on page 2-7.

Table 1-1. RADIUS files (continued)

File name	Default location	Description
radiusd.dbm	/etc/raddb	The RADIUS daemon you use with a UNIX DBM database. If you require RADIUS accounting or any of the attributes provided by Ascend as extensions to the Livingston RADIUS daemon, you must use the Ascend RADIUS daemon, version 1.16 (dated 7/25/95) or later. For information on running the radiusd.dbm daemon, see "Running the daemon with a UNIX DBM database" on page 2-9.
dictionary	/etc/raddb	The Ascend RADIUS dictionary. This file contains a list of all the attributes the daemon supports, along with the possible values for each attribute. You must install the dictionary on your RADIUS server in the same directory as the Ascend RADIUS daemon, and it must have the same date as the Ascend RADIUS daemon. The RADIUS daemon reads the dictionary when it starts up. If you update the dictionary file while the daemon is running, you must stop the daemon process and then restart it to make the new attributes available. For further information about the dictionary file, see "Dictionary file" on page 1-7.
clients	/etc/raddb	A file that identifies each client permitted to send requests to the RADIUS server. For overview information about the clients file, see "Clients file" on page 1-7. For details on setting up the clients file, see step 8 on page 1-2.
users	/etc/raddb	A file that contains a set of user profiles. Each user profile consists of attributes describing the user's name, his or her password, and the MAX features to which the user has access. For introductory information on the users file, see "Users file" on page 1-8.
logfile	/etc/raddb	A file containing error messages. You must create this file yourself.
detail	/usr/adm/*NAS-name*/radacct	A file containing accounting records.

Dictionary file

Every attribute has an associated name, ID, and value type. The dictionary file provides a complete list of attributes, and contains the information described in Table 1-2.

Table 1-2. Dictionary file format

Attribute element	Description
Name	An ASCII string denoting the attribute, such as User-Name or Password.
ID	A number between 1 and 255 associated with each attribute. For example, the User-Name attribute is attribute 1 and the Password attribute is attribute 2.
Value type	A specification denoting the type of values the attribute can contain: string—A character sequence, not necessarily null terminated (0–253 bytes). abinary—An Ascend binary filter (0–253 bytes). ipaddr—An IP address in network-byte order (4 bytes). integer—A 32-bit value in big-endian order (4 bytes). date—The number of seconds that have elapsed since 00:00:00 GMT, January 1, 1970 (4 bytes).

The first several lines of a typical dictionary file might look like this:

```
ATTRIBUTE      User-Name           1            string
ATTRIBUTE      Password            2            string
ATTRIBUTE      Challenge-Response  3            string
ATTRIBUTE      NAS-Identifier      4            string
ATTRIBUTE      NAS-Port            5            string
```

Clients file

A client is the MAX or another machine that sends requests to the RADIUS server. The RADIUS clients file defines the client machines permitted to make requests to the RADIUS server. For the RADIUS daemon to respond to client requests from the MAX, you must specify the MAX unit’s name and password in the clients file.

A sample line in the clients file looks like this one:

```
   Ascend3   bXSAMpy
```

Users file

The users file contains an entry for each user that RADIUS will authenticate. Each entry is called a user profile, and consists of attributes describing a user and the services he or she can access. A users file can contain comment lines, user profiles, and blank lines. Table 1-3 lists each element.

Table 1-3. Users file elements

Element	Description
Comment line	A comment line begins with the # character at column one, with text that extends to the end of the line. You can embed a comment line anywhere in a user profile.
User profile	A user profile consists of a first line (also called an authentication line), followed by the rest of the profile, followed by a final line. The first line consists of a user name, followed by a space or tab, followed by an attribute list containing authentication information, such as the user's password and the password's expiration date. The attributes on the first line are called check attributes because RADIUS must check the attributes before it can grant access to the MAX. Any characters can appear at columns one and two except the # character, a space, or a tab. Starting at the third column, the first line can contain one or more spaces or tabs, followed by an attribute list (without a trailing comma) and a newline. Each subsequent line in the rest of the record has a space or tab in the first column, followed by zero or more spaces or tabs, an attribute list, a comma, and a newline. The final line is identical to each line after the first one, except that it contains no trailing comma.
Blank line	A blank line cannot appear within a user profile, but can be present anywhere outside a user profile. It must end with a newline.

This portion of a users file contains two comment lines, a blank line, and a user profile:

```
# This user profile is for PPP sessions only, and uses a # local password.

Ascend1 Password="Pipeline"
    User-Service=Framed-User,
    Framed-Protocol=PPP,
    Framed-Address=10.0.1.1,
    Framed-Netmask=255.255.255.0,
    Ascend-Metric=2,
    Framed-Routing=None,
    Ascend-Idle-Limit=30
```

The user profile consists of a first line containing the user name (Ascend1) and password (Pipeline) that the RADIUS server uses for authentication. Subsequent lines contain attributes describing the type of service the user can access, the type of protocol in use, and so on. Note that each line of the profile, except the first line and last line, contains a trailing comma.

Overview of RADIUS attributes

Attributes associated with authentication, connection setup, and user sessions can appear in the following types of packets:

- Access-Request
- Access-Accept
- Access-Reject
- Access-Terminate-Session
- Ascend-Access-Event-Request
- Ascend-Access-Event-Response

The sections that follow describe the attributes in the packets listed above. For information on attributes associated with accounting, see “Understanding accounting records” on page 8-13.

Access-Request attributes

When it receives an incoming call, the MAX first checks its local Connection profiles. If it doesn’t find a Connection profile for the call and you configured the MAX to communicate with RADIUS, the MAX sends an Access-Request packet 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 1-4.

Table 1-4. Access-Request attributes

Attribute	Description	Default
Ascend-Send-Passwd (232)	Specifies the password that the MAX sends to the remote end of a connection on outgoing calls.	The default value is null.
Ascend-Send-Secret (214)	Specifies that the system encrypts the password when passing it between the RADIUS server and the MAX on outgoing calls.	The default value is null.
Caller-Id (31)	Specifies the calling party number, indicating the phone number of the user that wants to connect to the MAX.	The default value is null.
Challenge-Response (3)	Indicates the password that a Challenge Handshake Authentication Protocol (CHAP) user enters in response to a password challenge.	The default value is null.

Table 1-4. Access-Request attributes (continued)

Attribute	Description	Default
Class (25)	Enables access providers to classify their user sessions, such as for the purpose of billing users depending on the service option they choose. The MAX sends the Class attribute in Access-Request packets under CLID authentication.	The default value is null.
Client-Port-DNIS (30)	Specifies the called-party number, indicating the phone number the user dialed to connect to the MAX.	The default value is null.
Framed-Protocol (7)	Specifies the type of protocol a link can use. This attribute does not appear in an Access-Request packet if Auth Send Attr 6, 7=No in the Ethernet > Mod Config > Auth menu.	By default, the MAX does not restrict the type of protocol a link can use.
NAS-Identifier (4)	Indicates the IP address of the MAX.	The default value is 0.0.0.0/0.
NAS-Port (5)	Specifies the interface and service the session is using.	The default value for the RADIUS daemon appears in the /etc/services file.
NAS-Port-Type (61)	Specifies the type of physical port the MAX is using to authenticate the client.	The default value is Async.
Password (2)	Specifies the user’s password for an incoming or outgoing call.	The default value is null.
User-Name (1)	Specifies the user’s name.	The default value is null.
User-Service (6)	Indicates whether the link can use framed or unframed services. You can specify Framed-User, Login-User, or Dialout-Framed-User. This attribute does not appear in an Access-Request packet if Auth Send Attr 6, 7=No in the Ethernet > Mod Config > Auth menu.	By default, the MAX does not restrict the services that a link can use.

Access-Accept attributes

If the attribute values that the MAX submits to RADIUS match the attribute values in the user profile, the RADIUS server authenticates the call and returns an Access-Accept packet containing a list of attributes characterizing that user. Table 1-5 lists the RADIUS attributes defined in the Livingston RADIUS draft.

Table 1-5. Livingston/Ascend RADIUS Access-Accept attributes

Attribute	Description	Default
Caller-Id (31)	Specifies the calling party number, indicating the phone number of the user that wants to connect to the MAX.	The default value is null.
Change-Password (17)	Specifies a value used internally by the MAX and the RADIUS server to change an expired password. When a user specifies an expired password, RADIUS prompts the user for a new password. When the user enters the new password, the MAX sends an Access-Password-Request packet that contains both the old password (as the value of the Change-Password attribute), and the new password (as the value of the Password attribute). If the RADIUS server accepts the new password, it tries to edit the users file and replace the expired password with the new one. Note that the RADIUS server can make this change in the user profile only in the flat file. It cannot make this change in the database version of the users file.	This attribute has no default value, because it does not appear in a user profile.
Class (25)	Enables access providers to classify their user sessions, such as for the purpose of billing users depending on the service option they choose. If you include the Class attribute in the RADIUS user profile, the RADIUS server sends it to the MAX in the Access-Accept packet when the session begins.	The default value is null.
Client-Port-DNIS (30)	Specifies the called-party number, indicating the phone number the user dialed to connect to the MAX.	The default value is null.
Framed-Address (8)	Indicates the IP address of the user.	The default value is 0.0.0.0.
Framed-Compression (13)	Turns TCP/IP header compression on or off.	By default, the MAX turns compression on.
Framed-MTU (12)	Specifies the maximum number of bytes the MAX can receive in a single packet on a PPP, Frame Relay, EU-UI, or EU-RAW link.	The default value is 1524.
Framed-Netmask (9)	Indicates the subnet mask associated with the IP address of a station or router at the remote end of the link.	The default value is 0.0.0.0.
Framed-IPX-Network (23)	Indicates a virtual IPX network required for the home agent to route IPX packets to the mobile node.	The default value is null.

Table 1-5. Livingston/Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default
Framed-Protocol (7)	Specifies the type of protocol a link can use.	By default, the MAX does not restrict the type of protocol a link can use.
Framed-Route (22)	Indicates a static IP route when User-Service= Dialout-Framed User.	***host_ipaddr***=0.0.0.0 ***/subnet_mask***=/0 ***router_ ipaddr***=0.0.0.0 ***metric***=8 ***private***= “n” ***profile_name***=null ***preference***=120
Framed-Routing (10)	Specifies whether the MAX sends RIP packets, receives RIP packets, or both.	By default, the MAX neither sends nor receives RIP packets.
Login-Host (14)	Specifies the host to which the automatically connects when you set User-Service=Login-User and specify a value for the Login-Service attribute.	The default value is 0.0.0.0. This setting specifies no host.
Login-Service (15)	Specifies the type of terminal service connection to an IP host that occurs immediately after authentication.	By default, the MAX does not grant immediate access to any type of terminal server session.
Login-TCP-Port (16)	Specifies the port number to which a TCP session connects.	The default value is null.
Reply-Message (18)	Specifies text that appears to the terminal server operator who is using the menu-driven interface. You can specify up to 16 entries per user profile.	The default value is null.
User-Service (6)	Indicates whether the link can use framed or unframed services. You can specify Framed-User, Login-User, or Dialout-Framed-User.	By default, the MAX does not limit the services that a link can use.

Table 1-6 lists Ascend extensions to the RADIUS attributes. These are defined only in the Ascend RADIUS dictionary file and require the Ascend RADIUS daemon.

Table 1-6. Ascend RADIUS Access-Accept attributes

Attribute	Description	Default
Ascend-Add-Seconds (240)	Specifies the number of seconds that average line utilization (ALU) for transmitted data must exceed the threshold indicated by the Ascend-Target-Util attribute before the MAX begins adding bandwidth to a session.	The default value is 5.
Ascend-Ara-PW (181)	Indicates the password of the incoming caller over AppleTalk Remote Access (ARA).	The default value is null.
Ascend-Assign-IP-Client (144)	Specifies the IP address of an Ascend unit that can use global IP address pools.	The default value is 0.0.0.0.
Ascend-Assign-IP-Global-Pool (146)	Specifies the global address pool from which RADIUS should assign a user an address.	The default value is null.
Ascend-Assign-IP-Pool (218)	Specifies the address pool that incoming calls use.	The default value is 1.
Ascend-Assign-IP-Server (145)	Specifies the IP address of the host running radipad.	The default value is 0.0.0.0.
Ascend-Authen-Alias (203)	Sets the MAX unit’s login name during PPP authentication.	The default is the value of the Name parameter in the System profile.
Ascend-backup (176)	Specifies the name of a backup profile for a nailed-up link.	The default value is null.
Ascend-BACP-Enable (134)	Specifies whether Bandwidth Allocation Control Protocol (BACP) is enabled for the link.	The default is BACP-No.
Ascend-Base-Channel-Count (172)	Specifies the initial number of channels the MAX sets up when originating calls for a PPP, MP+, MP, or Combinet multichannel link.	The default value is 1.
Ascend-Billing-Number (249)	Indicates a billing number for charges incurred on the line.	The default value is null.
Ascend-Bridge (230)	Enables or disables protocol-independent bridging for the link.	The default it to disable bridging.

Table 1-6. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default
Ascend-Bridge-Address (168)	Specifies a bridge entry.	***`MAC_address`***=000000000000 ***`profile_name`***=null ***`IP_address`***=0.0.0.0
Ascend-Callback (246)	Enables or disables callback.	By default, the MAX disables callback.
Ascend-Call-By-Call (250)	Specifies the T1 PRI service that the MAX uses when placing a call.	By default, the MAX uses ACCUNET Switched Digital Services from AT&T.
Ascend-Call-Filter (243)	Defines a call filter.	The default value is null.
Ascend-Call-Type (177)	Specifies the type of nailed-up connection in use.	The default value is Nailed.
Ascend-Client-Gateway (132)	Specifies the default route for IP packets coming from the user on this connection.	The default value is 0.0.0.0.
Ascend-Data-Filter (242)	Defines a data filter.	The default value is null.
Ascend-Data-Svc (247)	Specifies the type of data service the link uses.	The default value is Switched-56 service.
Ascend-DBA-Monitor (171)	Specifies how the MAX monitors traffic on an MP+ call.	By default, the MAX adds or subtracts bandwidth based on the amount of data it transmits—that is, the default value is DBA-Transmit.
Ascend-Dec-Channel-Count (237)	Indicates the number of channels the MAX removes when bandwidth changes either manually or automatically during a call.	The default value is 1.
Ascend-DHCP-Maximum-Leases	Specifies the maximum number of dynamic addresses to assign to NAT clients using a connection	The default value is 4.
Ascend-DHCP-Pool-Number (148)	Specifies the address pool to use for allocating an IP address to a Dynamic Host Configuration Protocol (DHCP) client or a NAT client on a connection.	The default value is 0 (zero).
Ascend-DHCP-Reply (147)	Specifies whether the MAX processes Dynamic Host Configuration Protocol (DHCP) packets and acts as a DHCP server on this connection.	The default is to disable DHCP functionality (DHCP-Reply-No).

Table 1-6. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default
Ascend-Dial-Number (227)	Specifies the phone number the MAX dials to reach the bridge, router, or node at the remote end of the link.	The default value is null.
Ascend-Dialout-Allowed (131)	Specifies whether the user associated with the RADIUS user profile can dial out using one of the MAX unit's digital modems.	The default value is Dialout-Not Allowed.
Ascend-Expect-Callback (149)	Specifies whether a user calling out should expect the remote end to call back.	The default value is no callback (Expect-Callback-No).
Ascend-First-Dest (189)	Specifies the destination IP address of the first packet the MAX receives on a connection after it has authenticated the link.	This attribute has no default value, because it does not appear in a user profile.
Ascend-Force-56 (248)	Indicates whether the MAX uses only the 56-Kbps portion of a channel, even when all 64 Kbps appear to be available.	By default, the MAX attempts to use all 64 Kbps (Force-56-No).
Ascend-FR-Circuit-Name (156)	Indicates the Permanent Virtual Connection (PVC) for which the user profile is an endpoint.	The default value is null.
Ascend-FR-DCE-N392 (162)	Specifies the number of errors during Ascend-FR-DCE-N393-monitored events that cause the network side to declare the user side's procedures inactive.	The default value is 3.
Ascend-FR-DCE-N393 (164)	Specifies the DCE-monitored event count.	The default value is 4.
Ascend-FR-Direct (219)	Specifies whether the MAX uses a gateway connection or a redirect connection.	By default, the MAX uses a gateway connection (FR-Direct-No).
Ascend-FR-Direct-DLCI (221)	Identifies the user profile to the frame relay switch as a logical link on a physical circuit for a redirect connection.	The default value is 16.
Ascend-FR-Direct-Profile (220)	Specifies the name of the Frame Relay profile that carries the redirect connection to the frame relay switch.	The default value is null.

Table 1-6. Ascend RADIUS Access-Accept attributes (continued)

Attribute	**Description**	**Default**
Ascend-FR-DLCI (179)	Indicates the Data Link Connection Indicator (DLCI) that identifies the RADIUS user profile to the frame relay switch as a logical link on a physical circuit in a gateway connection.	The default value is 16.
Ascend-FR-DTE-N392 (163)	Specifies the number of errors during Ascend-FR-DTE-N393-monitored events that cause the network side to declare the user side's procedures inactive.	The default value is 3.
Ascend-FR-DTE-N393 (165)	Specifies the DTE-monitored event count.	The default value is 4.
Ascend-FR-Link-Mgt (160)	Specifies the type of frame relay link management in use for the profile.	By default, the MAX does not use link management (Ascend-FR-No-Link-Mgt).
Ascend-FR-LinkUp (157)	Indicates whether a link comes up automatically.	By default, the link does not come up automatically.
Ascend-FR-N391 (161)	Specifies the interval at which the MAX requests a Full Status Report.	The default value is 6.
Ascend-FR-Nailed-Grp (158)	Indicates the nailed channel number for a frame relay datalink.	The default value is 1.
Ascend-FR-Profile-Name (180)	Specifies the name of the Frame Relay profile the MAX uses in building a gateway connection.	The default value is null.
Ascend-FR-T391 (166)	Sets up the Link Integrity Verification polling time.	The default value is 10.
Ascend-FR-T392 (167)	Sets up the timer for the verification of the polling cycle— the length of time the unit should wait between Status Enquiry messages. An error results if the MAX does not receive a Status Enquiry message within the number of seconds you specify for this attribute.	The default value is 15.
Ascend-FR-Type (159)	Specifies the type of frame relay connection.	By default, the MAX assumes a UNI-to-DTE connection (Ascend-FR-DTE).

Table 1-6. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default
Ascend-FT1-Caller (175)	Indicates whether the MAX initiates an FT1-AIM or an FT1-B&O call, or whether it waits for the remote end to initiate these types of calls.	By default, the MAX waits for the remote end to initiate the call (FT1-No).
Ascend-Group (178)	Points to the nailed-up channels that the WAN link uses.	The default value is 1.
Ascend-Handle-IPX (222)	Specifies how the MAX handles NCP watchdog requests on behalf of IPX clients during IPX bridging.	By default, the MAX does not handle NCP watchdog requests (Handle-IPX-None).
Ascend-History-Weigh-Type (239)	Indicates which Dynamic Bandwidth Allocation (DBA) algorithm to use for calculating average line utilization (ALU) of transmitted data.	The default value is History-Quadratic.
Ascend-Home-Agent-Password (184)	Indicates the password that the foreign agent sends to the home agent during ATMP operation.	The default value is null.
Ascend-Home-Agent-UDP-Port (186)	Specifies the UDP port number to use when the foreign agent sends ATMP packets to the home agent.	The default value is 5150.
Ascend-Home-Network-Name (185)	Indicates the name of the Connection profile through which the home agent sends all packets it receives from the mobile node during ATMP operation.	The default value is null.
Ascend-Host-Info (252)	Specifies the IP address and description of the first, second, third, and fourth hosts to which a user can establish a Telnet session as listed in the terminal server menu-driven interface.	The default address is 0.0.0.0/0 and the default description is null.
Ascend-Idle-Limit (244)	Indicates the number of seconds the MAX waits before clearing a call when a session is inactive.	The default value is 120 seconds.
Ascend-IF-Netmask (154)	Specifies the subnet mask in use for the local numbered interface.	The default value is 0.0.0.0.
Ascend-Inc-Channel-Count (236)	Specifies the number of channels the MAX adds when bandwidth changes either manually or automatically during a call.	The default value is 1.

Table 1-6. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default
Ascend-IP-Direct (209)	Indicates the IP address to which the MAX redirects packets from the user.	The default value is 0.0.0.0. This setting specifies that the MAX does not perform IP redirection.
Ascend-IP-Pool-Definition (217)	Specifies the first IP address in an IP address pool and the number of addresses in the pool.	The default number of the pool is 1. The default for the first address is 0.0.0.0. The default number of addresses is 0 (zero).
Ascend-IPX-Alias (224)	Indicates an IPX network number to use when connecting to IPX routers that require numbered interfaces.	The default value is 00000000.
Ascend-IPX-Node-Addr (182)	Specifies a unique IPX node address on the Framed-IPX-Network. This value completes the IPX address of a mobile node.	The default value is 000000000001.
Ascend-IPX-Peer-Mode (216)	Specifies whether the caller is an Ethernet client with its own IPX network address or a dial-in PPP client.	By default, the MAX assumes an Ethernet client with its own IPX network address (IPX-Peer-Router).
Ascend-IPX-Route (174)	Defines a static IPX route.	***profile_name***=null ***network#***=00000000 ***node#***=000000000001 ***socket#***=0000 ***server_type***=0000 ***hop_count***=1 ***tick_count***=12 ***server_name***=null
Ascend-Link-Compression (233)	Turns data compression on or off for a PPP link.	The default is no compression.
Ascend-Maximum-Call-Duration (125)	Specifies the maximum number of minutes an incoming call can remain online.	The default value is 0 (zero).
Ascend-Maximum-Channels (235)	Specifies the maximum number of channels allowed on an MP+ call.	The default value is 1.
Ascend-Maximum-Time (194)	Indicates the maximum length of time in seconds that any session is allowed.	The default value is 0 (zero), which specifies no time limit.
Ascend-Menu-Item (206)	Defines a single menu item for a user profile.	By default, the MAX uses the standard terminal server menu.

Table 1-6. Ascend RADIUS Access-Accept attributes (continued)

Attribute	**Description**	**Default**
Ascend-Menu-Selector (205)	Specifies a string as a prompt for user input in the terminal server menu interface.	The default value is `Enter Selection (1-`*`num`*`, q)`, where *`num`* is the number of items on the menu.
Ascend-Metric (225)	Indicates the virtual hop count of the route.	The default value is 7.
Ascend-Minimum-Channels (173)	Specifies the minimum number of channels an MP+ call maintains.	The default value is 1.
Ascend-MPP-Idle-Percent (254)	Specifies a percentage of bandwidth utilization below which the MAX clears a single-channel MP+ call.	The default value is 0 (zero).
Ascend-Multicast-Client (152)	Specifies whether the user is a multicast client of the MAX.	The default value is Multicast-No.
Ascend-Multicast-Rate-Limit (153)	Specifies how many seconds the MAX waits before accepting another packet from a multicast client.	The default value is 100.
Ascend-Multilink-ID (187)	Indicates the ID number of the Multilink bundle when the session closes. A Multilink bundle is a multichannel MP or MP+ call.	This attribute has no default value, because it does not appear in a user profile.
Ascend-Netware-timeout (223)	Indicates 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.	The default value is 0 (zero).
Ascend-Num-In-Multilink (188)	Indicates the number of sessions remaining in a Multilink bundle when the session closes.	This attribute has no default value, because it does not appear in a user profile.
Ascend-PPP-Address (253)	Specifies the IP address reported to the calling unit during PPP IPCP negotiations.	The value of this attribute is always negotiated.
Ascend-PPP-Async-Map (212)	Gives the Ascend PPP code the async control character map for the PPP session.	The default value is the standard async control character.
Ascend-PPP-VJ-1172 (211)	Instructs the Ascend PPP code whether to use the 0x0037 value for the VJ compression type.	By default, the MAX uses VJ compression type 0x002d.

Table 1-6. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default
Ascend-PPP-VJ-Slot-Comp (210)	Instructs the Ascend PPP code whether to use slot compression when sending VJ-compressed packets.	By default, the MAX uses slot compression (VJ-Slot-Comp-Yes).
Ascend-Preempt-Limit (245)	Specifies the number of idle seconds the MAX waits before using one of the channels of an idle link for a new call.	The default value is 60 seconds.
Ascend-Pre-Input-Octets (190)	Records the number of input octets before authentication.	This attribute has no default value, because it does not appear in a user profile.
Ascend-Pre-Input-packets (192)	Specifies the number of input packets before authentication.	This attribute has no default value, because it does not appear in a user profile.
Ascend-Pre-Output-Octets (191)	Indicates the number of output octets before authentication.	This attribute has no default value, because it does not appear in a user profile.
Ascend-Pre-Output-packets (193)	Records the number of output packets before authentication.	This attribute has no default value, because it does not appear in a user profile.
Ascend-Primary-Home-Agent	Specifies the first home agent the foreign agent tries to reach when setting up an ATMP tunnel, and indicates the UDP port the foreign agent uses for the link.	The default IP address is 0.0.0.0. and the default UDP port is 5150.
Ascend-PRI-Number-Type (226)	Indicates the type of phone number the MAX dials under the extended dial plan.	The default value is National-Number.
Ascend-PW-Expiration (21)	Specifies an expiration date for the user's password.	The default is no expiration date.
Ascend-PW-Lifetime (208)	Indicates on a per-user basis the number of days that a password is valid.	The default is the value of the Lifetime-In-Days attribute from the Ascend dictionary.
Ascend-Receive-Secret (215)	Specifies a value the MAX receives from a dial-in user in order to verify an encrypted password.	The default value is null.
Ascend-Remote-Addr (155)	Specifies the IP address of the link's remote interface to the WAN.	The default value is 0.0.0.0.

Table 1-6. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default
Ascend-Remove-Seconds (241)	Specifies the number of seconds that average line utilization (ALU) for transmitted data must fall below the threshold indicated by the Ascend-Target-Util attribute before the MAX begins removing bandwidth from a session.	The default value is 10.
Ascend-Require-Auth (201)	Indicates whether additional authentication is required for calls that have already passed CLID or called-number authentication. Called-number authentication is also known as Dialed Number Information Service (DNIS) authentication.	By default, the MAX does not require additional authentication (Not-Require-Auth).
Ascend-Route-IP (228)	Enables or disables the routing of IP data packets over the link.	By default, the MAX enables IP routing.
Ascend-Route-IPX (229)	Enables or disables IPX routing.	By default, the MAX disables IPX routing.
Ascend-Secondary-Home-Agent	Specifies the secondary home agent the foreign agent tries to reach when the primary home agent (Ascend-Primary-Home-Agent) is unavailable. Also indicates the UDP port the foreign agent uses for the link.	The default IP address is 0.0.0.0. and the default UDP port is 5150.
Ascend-Seconds-Of-History (238)	Specifies the number of seconds the MAX uses as a sample for calculating average line utilization (ALU) of transmitted data.	The default value is 15.
Ascend-Send-Auth (231)	Indicates the protocol to use for name-password authentication.	By default, the MAX does not use an authentication protocol.
Ascend-Send-Passwd (232)	Specifies the password that the MAX sends to the remote end of a connection on outgoing calls.	The default value is null.
Ascend-Send-Secret (214)	Specifies that the system encrypts the password when passing it between the RADIUS server and the MAX on outgoing calls.	The default value is null.
Ascend-Target-Util (234)	Specifies the percent bandwidth utilization at which the MAX adds or subtracts bandwidth dynamically.	The default value is 70.

Table 1-6. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default
Ascend-Third-Prompt (213)	Indicates an additional prompt for user input after the login and password prompts.	By default, the MAX does not display an additional prompt.
Ascend-Token-Expiry (204)	Sets the lifetime of a cached token—that is, the lifetime of hand-held security-card authentication.	The default value is 0 (zero). This setting specifies that token caching is not allowed.
Ascend-Token-Idle (199)	Specifies the maximum length of time in minutes a cached token can remain alive between authentications if a call is idle.	By default, the token remains alive until the value of Ascend-Token-Expiry is reached.
Ascend-Token-Immediate (200)	Establishes how RADIUS treats the password it receives from a Login-User when the user profile specifies a hand-held security card server.	By default, the MAX does not use a cached token (Tok-Imm-No).
Ascend-Transit-Number (251)	Specifies the U.S. Interexchange Carrier (IEC) to use for long-distance calls over a T1 PRI or E1 PRI line.	The default value is null.
Ascend-TS-Idle-Limit (169)	Specifies the number of seconds that a terminal server connection must be idle before the MAX disconnects the session.	The default value is 120.
Ascend-TS-Idle-Mode (170)	Specifies whether the MAX uses a terminal server idle timer and, if so, whether both the user and host must be idle before the MAX disconnects the session.	By default, the MAX disconnects the session if the user is idle for a length of time greater than the value of the Ascend-TS-Idle-Limit attribute.The default value is TS-Idle-Input.

Access-Reject attributes

If the attribute values submitted to RADIUS do not match the attribute values in the user profile, the RADIUS server does not authenticates the call and returns an Access-Reject packet containing one or more of the values listed in Table 1-7.

Table 1-7. Access-Reject attributes

Attribute	Description	Default
Login-TCP-Port (16)	Specifies the port number to which a TCP session connects.	The default value is null.
Reply-Message (18)	Specifies text that appears to the terminal server operator who is using the menu-driven interface. You can specify up to 16 entries per user profile.	The default value is null.

Access-Terminate-Session attributes

If the RADIUS server determines that the MAX should terminate the session, it sends an Access-Terminate-Session packet containing the Reply-Message attribute. This attribute carries message text from the RADIUS server to RADIUS clients such as the MAX.

Ascend-Access-Event-Request attributes

The MAX can report the number of sessions by class to the RADIUS authentication server specified by Auth Host #*n* when Auth=RADIUS/LOGOUT in the Ethernet > Mod Config > Auth menu. In addition, the MAX can report on sessions to the RADIUS accounting server specified by the Acct Host #*n* parameter in the Ethernet > Mod Config > Accounting menu.

The MAX reports the number of sessions by sending an Ascend-Access-Event-Request (33) packet type at the interval defined by the Sess Timer parameter in the Ethernet > Mod Config > Auth menu (for authentication requests) or in the Ethernet > Mod Config > Accounting menu (for accounting requests).

Table 1-8 lists the attributes in an Ascend-Access-Event-Request packet.

Table 1-8. Ascend-Access-Event-Request attributes

Attribute	Description	Default value
NAS-Identifier (4) (for both authentication and accounting requests)	Indicates the IP address of the MAX.	The default value is 0.0.0.0/0.
Password (2) (for authentication requests only)	Specifies the user’s password for an incoming or outgoing call.	The default value is null.
Ascend-Event-Type (150) (for both authentication and accounting requests)	Specifies that the MAX is informing the RADIUS server of a coldstart (for an accounting request), or sending a session report (for an authentication request).	The default is Ascend-Coldstart (1) for an accounting request and Ascend-Session-Event (2) for an authentication request.

Table 1-8. Ascend-Access-Event-Request attributes (continued)

Attribute	Description	Default value
Ascend-Number-Sessions (202) (for both authentication and accounting requests)	Specifies the number of active user sessions of a given class (as specified by the Class attribute). In the case of multichannel calls, such as MP+ calls, each separate connection counts as a session.	The default value is 0 (zero).

Ascend-Access-Event-Response attributes

Table 1-9 lists the attributes in an Ascend-Access-Event-Response packet.

Table 1-9. Ascend-Access-Event-Response attributes

Attribute	Description	Default value
NAS-Identifier (4) (for both authentication and accounting responses)	Indicates the IP address of the MAX.	The default value is 0.0.0.0/0.
Ascend-Event-Type (150) (for both authentication and accounting responses)	Specifies that the MAX is informing the RADIUS server of a coldstart (for an accounting request), or sending a session report (for an authentication request).	The default is Ascend-Coldstart (1) for an accounting request and Ascend-Session-Event (2) for an authentication request.
Ascend-Number-Sessions (202) (for both authentication and accounting responses)	Specifies the number of active user sessions of a given class (as specified by the Class attribute). In the case of multichannel calls, such as MP+ calls, each separate connection counts as a session.	The default value is 0 (zero).

Overview of RADIUS packet formats

Each RADIUS packet consists of the fields listed in Table 1-10.

Table 1-10.RADIUS packet fields

Element	Description
Code (8 bits)	Specifies the packet type. For a list of packet types, see Table 1-11 on page 1-25.
Identifier (8 bits)	Enables RADIUS to match requests with responses. Each new request has a unique identifier. Each response carries the identifier of the corresponding request.
Length (16 bits)	Indicates the total packets size in bytes.

Table 1-10.RADIUS packet fields (continued)

Element	Description
wAuthenticator (16 bytes)	Authenticates packets between the NAS and the authentication server. The NAS and the authentication server share a secret. The MAX uses this shared secret with the authenticator field to provide password encryption and packet authentication. The shared secret resides in the clients file on the authentication host. The MAX checks all authentication and accounting packets to ensure that they come from known sources. This checking makes use of the shared secret, the authenticator field, and MD5 encoding. In addition, all passwords that the MAX sends are encrypted with MD5, CHAP, or DES. Passwords that the authentication server sends can be encrypted with MD5.
Attribute list (variable length)	Consists of zero or more attributes. Each attribute consists of these fields: Attribute ID (8 bits)—These IDs are listed in the dictionary file. Attribute length (8 bits)—This field shows the combined length of the ID, length, and value fields. Attribute value (variable length)—The length and format of this value depend on the attribute type.

Table 1-11 lists the packet types that can appear in the code field.

Table 1-11.Code field packet types

Number	Name	Description
1	Access-Request	A request for access that the MAX sends to the RADIUS server on behalf of a client attempting to establish a connection.
2	Access-Accept	A packet that the RADIUS server sends to inform the MAX that it has granted a client’s request for access.
3	Access-Reject	A packet that the RADIUS server sends to inform the MAX that it has not granted a client’s request for access. The RADIUS server can send this packet for one of the following reasons: The user entered an unknown user name. The user failed to enter the correct password. The user entered an expired password.

Table 1-11.Code field packet types (continued)

Number	Name	Description
4	Accounting-Request	A request for accounting information that the MAX sends to the RADIUS accounting server.
5	Accounting-Response	A packet containing accounting information that the RADIUS accounting server sends to the MAX.
7	Access-Password-Request	A request for a password change that the MAX sends to the RADIUS server.
8	Access-Password-Ack	A response from the RADIUS server informing the MAX that it has accepted the new password.
9	Access-Password-Reject	A response from the RADIUS server informing the MAX that it has rejected the new password.
11	Access-Challenge	A request for the user to enter a password using a hand-held security card. The authentication server sends this packet through the RADIUS server and the NAS to the user dialing in.
29	Ascend-Access-Next-Code	A response from the RADIUS server informing the MAX that it should request access again, but with the next password in the sequence.
30	Ascend-Access-New-Pin	A response from the RADIUS server informing the MAX that it should request access again, but with the next PIN in the sequence.
31	Ascend-Terminate-Session	A response from the RADIUS server informing the MAX that it should terminate the session and display the message sent in the packet.

Table 1-11.Code field packet types (continued)

Number	Name	Description
32	Ascend-Password-Expired	A response from RADIUS server to the MAX indicating that the password the user entered matches the one in the user profile, but has expired. (That is, the Access-Request packet sent a valid but expired password.) When a user specifies an expired password, RADIUS prompts the user for a new password. When the user enters the new password, the MAX sends an Access-Password-Request packet that contains both the old password (as the value of the Change-Password attribute), and the new password (as the value of the Password attribute).
33	Ascend-Access-Event-Request	A packet containing a notification that the MAX has started up, or a request for the RADIUS server to record the number of open sessions.
34	Ascend-Access-Event-Response	A response from the RADIUS server reporting the number of open sessions or the fact that the MAX has started up, and informing the MAX that it has received and recorded the MAX unit's ID.
40	Disconnect-Request	A message from a client of the MAX asking to disconnect the session.
41	Disconnect-Request-ACKed	A message that the MAX sends to the client if it found at least one session to disconnect.
42	Disconnect-Request-NAKed	A message that the MAX sends to the client if it could not find a session to disconnect.
43	Change-Filter-Request	A request to change the filters for a bridging/ routing session.
44	Change-Filter-Request-ACKed	A message that the MAX sends if it found at least one bridging/routing session for which it could change filters.
45	Change-Filter-Request-NAKed	A message that the MAX sends if could not find a bridging/routing session for which it could change filters.

Installing and Starting RADIUS

2

This chapter describes how to install and start the RADIUS daemon.This chapter contains:

What is RADIUS?

Remote Authentication Dial-In User Service (RADIUS) is a protocol originally developed by Livingston Enterprises, and extended by Ascend Communications, Inc. Using the Ascend RADIUS daemon, you can perform these tasks:

- Exchange session authentication and configuration information between a Network Access Server (NAS) such as the MAX, and an authentication server.
- Carry accounting information from an NAS to a RADIUS server.

  A RADIUS server is the machine on which the RADIUS daemon is running.

What you need before you start

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

- A UNIX workstation or PC to run the RADIUS daemon.
- A TCP/IP connection between the RADIUS server and the MAX.

Installing the RADIUS daemon

To install the RADIUS daemon, follow these steps:

1 Use anonymous FTP to download the most recent RADIUS files from ftp.ascend.com.

2 Decompress (unzip) and separate (tar) the files.

3 Read the README file, installation instructions, and makefiles.

The installation instructions on the Ascend FTP server always provide the latest information on installing RADIUS.

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.

5 Move the file called *dictionary* to /etc/raddb.

This file is the Ascend RADIUS dictionary, and contains a list of all attributes that the RADIUS server supports.

You must install the dictionary on your RADIUS server in the same directory as the Ascend RADIUS daemon, and it must have the same date as the Ascend RADIUS daemon. If you find a discrepancy in the dates between the daemon and the dictionary, download the latest dictionary file from ftp.ascend.com, and copy it into the same directory as the daemon.

Note that the RADIUS daemon reads the dictionary when it starts up. If you update the dictionary file while the daemon is running, you must stop the daemon process and then restart it to make the new attributes available.

For further information about the dictionary file, see "Dictionary file" on page 1-7.

6 Use a text editor to open the /etc/services file and add a line identifying the RADIUS daemon's authentication port.

For example, enter this line:

```
radius   1645/udp
```

The port number you specify must match the port number specified by the Auth Port parameter in the Ethernet > Mod Config > Auth menu.

7 To enable the RADIUS host and the MAX to communicate on the IP network, make sure that you include the MAX unit's name and IP address in the /etc/hosts file on the RADIUS host or in the Yellow Pages database.

8 Create a file called *clients* in the /etc/raddb directory.

The RADIUS server does not simply authenticate incoming calls. It must also authenticate the Network Access Server (NAS) from which it receives requests. The MAX is an NAS and a client of the RADIUS server.

For the RADIUS daemon to respond to requests from the MAX, you must specify the MAX unit's name and password in the clients file.

- For the name, :specify the value of the Name parameter in the System profile.
- For the password, specify the value of the Auth Key parameter in the Ethernet > Mod Config > Auth menu.

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

```
Ascend3   bXSAMpy
```

The argument Ascend3 is the value specified by the Name parameter. The argument bXSAMpy is the password specified by the Auth Key parameter in the Ethernet > Mod

Config > Auth menu. The name you specify must be resolvable on the IP network (through DNS, the Yellow Pages, and so on). Otherwise, you must specify the IP address of the MAX.

If the accounting process of the daemon will be running on the same server as the authentication process (rather than on a separate host), the same password must also serve for the Acct Key parameter in the Ethernet > Mod Config > Accounting menu.

9 Create a file called *users* in the /etc/raddb directory.

A user is a caller that connects to the MAX. 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 unit's memory. RADIUS authentication occurs when the caller's name and password match an entry in the RADIUS users file.

For introductory information on the users file and its format, see “Users file” on page 1-8. For details on creating user profiles to carry out various tasks, see the remaining chapters in this guide.

10 Create the *logfile* in the /etc/raddb directory.

RADIUS writes error messages to /etc/raddb/logfile. The Syslog daemon does not create the RADIUS log file, so you must create the file yourself.

Installing radipad for global IP pools

You can use RADIUS to specify pools of IP addresses that a MAX can use to dynamically allocate IP addresses to incoming callers. By default, each MAX handles dynamic IP address allocation individually from a pool of addresses pre-assigned to each MAX. However, you can also set up your system to allocate IP addresses from a global pool of addresses that many units share. To do so, you must install radipad. Follow these steps:

1 Install radipad in the same directory in which you installed the RADIUS daemon.

2 Add the following lines to /etc/services on the hosts where both radipad and the RADIUS daemon reside:

```
radipad   9992/tcp #RADIUS IP address allocation from global
pools
```

The port number 9992 is the default. You can change it as required.

3 Modify your startup script to start radipad when the system comes up:

```
#
# Start up radipad for remote users
#
if [ -f /usr/local/bin/radipad ]; then
        /usr/local/bin/radipad; echo -n ’ radipad’
fi
```

Multiple hosts can run the RADIUS daemon, but only one host on the network should run radipad. Radipad is the central manger for global IP address pools on a network.

You must start up radipad manually the first time. To do so, you must be the user root.

For information on configuring global IP address pools, follow the instructions in “Configuring global IP address pools shared by several MAX units” on page 6-11.

Configuring the MAX to use the RADIUS server

This section describes how to configure the MAX to communicate with the RADIUS daemon. For additional information on each parameter you set, see the MAX *Reference Guide* and the MAX *Security Supplement*.

Note: This section describes the basic configuration procedure. It does not cover how to configure RADIUS for accounting purposes. For information on setting up accounting, see “Setting up RADIUS accounting” on page 8-3.

1 Open the Ethernet menu.

2 Open the Mod Config menu.

3 Open the Auth menu.

4 Set the Auth parameter to RADIUS or RADIUS/LOGOUT.

If you set Auth=RADIUS/LOGOUT, RADIUS keeps track of session logouts.

5 For each Auth Host parameter, specify the IP address of a RADIUS server.

You can have up to three RADIUS servers on your network. One is the primary server. Two additional servers can serve as backups. If the primary RADIUS server fails, the MAX automatically contacts the secondary RADIUS server to authenticate a user.

The MAX first tries to connect to Auth Host #1. If it receives no response within the time specified by the Auth Timeout parameter, it tries to connect to Auth Host #2. If it again receives no response within the time specified by Auth Timeout, it tries to connect to Auth Host #3. If the MAX unit’s request again times out, it reinitiates the process with Auth Host #1. The MAX can complete this cycle of requests a maximum of ten times.

When it successfully connects to an authentication server, the MAX uses that machine until it fails to serve requests. By default, the MAX does not use the first host until the second machine fails, even if the first host has come online while the second host is still servicing requests. However, you can use SNMP to specify that the MAX use the first host again. For details, see “Using SNMP to specify the primary RADIUS server” on page 2-6.

You can also specify the same address for all three Auth Host parameters. If you do so, the MAX keep trying to create a connection to the same server.

6 For the Auth Port parameter, enter the UDP port number you specified for the daemon in the /etc/services directory.

The MAX and the daemon must agree about which UDP port to use for communication, so make sure that the number you specify for the Auth Port parameter matches the number specified for the daemon.

7 To specify the number of seconds the MAX waits for a response to a RADIUS authentication request, set the Auth Timeout parameter.

If the MAX does not receive a response within the time specified by Auth Timeout, it sends the authentication request to the next authentication server specified by the Auth Host parameter.

By default, if authentication fails on a PPP connection because of a bad password or an authentication server timeout, the Ascend unit gracefully shuts down the PPP connection by sending an LCP-CLOSE request to the dial-up user. When Windows 95 (MSN) receives the LCP-CLOSE during authentication, it assumes a rejected password, and displays a message telling the user that his or her password is invalid. If authentication fails because of a RADIUS timeout, this message gives the user incorrect information.

To specify that the Ascend unit simply hangs up a PPP connection on a RADIUS timeout without closing down cleanly, set Disc on Auth Timeout=Yes in the Answer profile. The resulting message to the user specifies that the network failed.

8 For the Auth Key parameter, enter the RADIUS client password exactly as it appears in the RADIUS clients file.

The password is case sensitive.

9 Set the Auth Pool parameter to specify whether the MAX sends the IP address from pool #1 to the RADIUS server when it requests authentication.

For information on the Auth Pool parameter, see “Configuring accounting with dynamic IP addressing” on page 8-11.

10 If you want to enforce CLID authentication for connections with Id Auth=Require, set Auth Req=Yes.

This setting specifies that the MAX requires a response from the RADIUS server for CLID authentication. If the MAX makes a request to the RADIUS server for the caller’s user profile and the request times out, the MAX rejects the call.

If you set Auth Req=No and the RADIUS query times out the MAX accepts the connection, even though Id Auth=Require and the MAX has not verified the user’s ID. This type of setup assumes that the MAX performs an additional level of authentication.

If Id Auth=Prefer or Id Auth=Ignore, the MAX ignores the Auth Req parameter.

For detailed information on CLID authentication, see “Setting up CLID authentication” on page 3-34.

11 To specify information about the host running the APP Server utility, set the APP Server, APP Host, and APP Port parameters.

For more information, see “Configuring the MAX to recognize the APP Server utility” on page 3-28.

12 To configure the MAX to recognize a security-card authentication server, set the Password Server and Password Port parameters.

For more information, see “Configuring the MAX to recognize the authentication server” on page 3-27.

13 To specify whether the MAX first checks for a local Connection profile when attempting to authenticate a connection, set the Local Profile First parameter.

You can specify either Yes or No.

- Yes indicates that the MAX checks for a local Connection profile, then a Password profile, and then a remote profile when attempting to authenticate a connection.

  Yes is the default.

- No indicates that the MAX checks for a remote profile, then a local Connection profile, and then a Password profile when attempting to authenticate a connection.

14 Set the Sess Timer parameter (if Auth=RADIUS/LOGOUT).

The MAX can report the number of sessions by class to a RADIUS authentication server when Auth=RADIUS/LOGOUT. The Sess Timer parameter specifies the interval in seconds in which the MAX sends session reports. You can specify a number between 0 and 65535.The default value is 0 (zero), which indicates that the MAX does not send reports on session events.

15 To specify the source port to use for sending a remote authentication request, set the Auth Src Port parameter.

Specify a port number between 0 and 65535. The default value is 0 (zero). If you accept this value, the Ascend unit can use any port number between 1024 and 2000. You can specify the same source port for authentication and accounting requests.

16 Set the Auth Send Attr 6, 7 parameter.

This parameter specifies whether the MAX sends values for the User-Service (6) and Framed-Protocol (7) attributes in Access-Request packets to the RADIUS server. While some RADIUS servers require these attributes in authentication requests, other RADIUS servers should not receive them.

Set this value to Yes if you want to generate the appropriate values for attributes 6 and 7 for an incoming call and send them in authentication requests to the RADIUS server. For example, if you set Auth Send Attr 6, 7=Yes, the MAX sets User-Service=Framed-User and Framed-Protocol=PPP for incoming PPP calls. The default value is Yes.

Set this value to No if your RADIUS server does not require attributes 6 and 7 in authentication requests.

17 Save your changes.

Using SNMP to specify the primary RADIUS server

By default, if the MAX uses a secondary RADIUS authentication server because the primary one goes out of service, the MAX does not use the first host until the second machine fails. This situation occurs even if the first host has come online while the second host is still servicing requests. However, you can use an SNMP set command to specify that the MAX use the first host again. Such a need might arise if you shut down the primary server for service and then make it available again.

Every time you reset the server using the set command, the MAX generates an SNMP trap. The MAX also generates a trap if it changes to the next server because the current server fails to respond. The trap is an Enterprise Specific Trap (18) and is accompanied by the Object ID and IP address for the new server. The Object ID for Authentication Server is 1.3.6.1.4.1.529.13.3.1.11.*x.* where *x* is the index of the current server (1–3).

For details, see the Ascend Enterprise MIB. You can download the most up-to-date version of the Ascend Enterprise MIB by logging in as `anonymous` to ftp.ascend.com. (No password is required.)

Starting the RADIUS daemon

You can use two different RADIUS daemons:

- radiusd

  Run this daemon when you use a flat ASCII users file.
- radiusd.dbm

  Run this daemon when you convert the flat ASCII users file to a standard UNIX DBM database.

Because RADIUS must search the flat ASCII file sequentially, you might find that using this type of file slows down access time, especially if you have many users and many authentication requests. If you use the DBM database, RADIUS can locate a record by index with only a few database accesses.

The DBM database is no more difficult to use than the flat ASCII file, and is much faster. However, if you reset passwords, these passwords take effect only after you rebuild the database. If resetting expired passwords is an important component of your system, you may not wish to use the DBM database.

Running the daemon with a flat ASCII users file

To start the RADIUS daemon with a flat ASCII users file, enter this command:

```
radiusd [-A acct[-a acctdir]] [-c] [-d dbdir] [-p] [-s]
[-u usrfile] [-v] [-w] [-x]
```

To enable call logging using RADIUS, start the RADIUS daemon with the `-A` option by entering this command line

```
radiusd -A services | incr
```

If you specify the `services` argument, the daemon creates the call-logging process, but only if a line defining the UDP port to use for call-logging appears in the `/etc/services` file. Otherwise, the daemon does not start.

If you specify the `incr` argument, the daemon creates the call-logging process with the UDP port specified as the call-logging port in the `/etc/services` file. If you have not defined the port, the daemon increments the UDP port specified for `radiusd` and uses that port number. This action is the default if you do not specify the `-A` argument.

Table 2-1 lists each argument.

Table 2-1. List of radiusd arguments

Argument	Description
-A *acct*	This argument controls the creation of the RADIUS accounting process. You can specify one of these values for ***`acct`***: none—The daemon does not create the accounting process. services—The daemon creates the accounting process only if a line defining the UDP port to use for accounting appears in the /etc/services file. Otherwise, daemon does not start. incr—The daemon creates the accounting process with the UDP port specified as the accounting port in the /etc/services file. If you have not defined the port, the daemon increments the UDP port you specify for radiusd and uses that port number. This action is the default you do not specify the `-A` argument.
-a *acctdir*	By default, RADIUS stores accounting records in a file named *detail* that resides in the /usr/adm/radacct. You can use the -a argument to specify a different directory for the file. ***`acctdir`*** must already exist. For example, you might enter this command line: **`radiusd -a /home/radacct`** The accounting process in the daemon creates a file named *detail* that contains accounting records in the /home/radacct directory.
-c	This argument enables cache-token authentication in the daemon.
-d *dbdir*	The default directory for the RADIUS clients, users, dictionary, and log files is /etc/raddb. You can use the -d argument to specify a different directory for the files. ***`dbdir`*** must already exist. For example, you might enter this command line: `radiusd -d /radius/raddb`
-p	This argument enables each user to change his or her own expired password through a dial-in modem connection.
-s	This argument specifies that the daemon runs in single-process mode. In this mode, the daemon receives, processes, and returns one request before going to the next one. This mode is much slower than the default multiprocess mode, in which the daemon receives, processes, and returns several requests concurrently.
-u *usrfile*	This argument assigns the file name specified by ***`usrfile`*** to the RADIUS users file. The default name is *users*.
-v	This argument prints the daemon's version number, extension, date, and the arguments selected in the makefile compilation.

Table 2-1. List of radiusd arguments (continued)

Argument	Description
-w	This argument makes the RADIUS daemon generate warnings about syntax errors it finds in the users file when the daemon is running. RADIUS generates a warning only when the daemon examines the 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 argument.
-x	This argument produces debug output.

Running the daemon with a UNIX DBM database

To run the daemon with a UNIX DBM database, you must carry out three tasks:

1 Create two executable files: builddbm and radiusd.dbm.

- The builddbm file enables you to create the DBM database.
- The radiusd.dbm file is the version of the RADIUS daemon that you run when using the DBM database.

2 Create the database.

3 Start the RADIUS daemon.

Creating the executable files

To create the builddbm and radius.dbm executable files, enter this command:

```
make dbm
```

Creating the DBM database

Before running radiusd.dbm, you must create the DBM database. To do so, enter this command line:

```
builddbm [-d dbdir] [-e] [-h] [-u usrfile] [-v]
```

Note: You must run builddbm each time you modify the users file. If remote users are able to change their own expired passwords, you must run builddbm after each password change.

Table 2-2 lists each argument for the builddbm command.

Table 2-2. List of builddbm arguments

Argument	Description
`-d` *`dbdir`*	The default output directory for the database file is /etc/raddb. You can use the -d argument to specify a different directory for the file. ***`dbdir`*** must already exist. For example, you might enter this command line: **`builddbm -d /radius/raddb`** This command results in two database files—/radius/raddb/users.dir and /radius/raddb/users.pag.
-e	This argument causes the builddbm program to report syntax errors and duplicate entries it finds in the users file during the indexing process. The daemon writes the messages to standard output. If you do not specify the -e argument, the daemon writes the entries to standard error output instead.
-h	This argument displays help.
`-u` *`usrfile`*	This argument specifies the RADIUS users file for which a database is being built. The default name is *users*. If the daemon runs with the –u argument, the name you specify when you run the daemon must be the same name you specify here. The users file must already exist in ASCII format. The resulting database files are named users.dir and users.pag.
-v	This argument runs builddbm in verbose mode.

Starting the RADIUS daemon for a DBM database

To start the RADIUS daemon in DBM mode, enter this command:

```
radiusd.dbm
```

The radiusd.dbm command supports the same set of arguments described for the radiusd command in “Running the daemon with a flat ASCII users file” on page 2-7, with one exception: the –p argument is restricted when the daemon is running in DBM mode. The users file database will not contain the user’s new password until you run builddbm again.

If you have enabled call-logging, start RADIUS daemon by entering this command line:

```
radiusd.dbm -A services
```

You must specify the `services` argument when you start the daemon in DBM mode.

Setting Up RADIUS Authentication

3

This chapter discusses how to configure the RADIUS server to authenticate MAX clients. This chapter contains:

This chapter discusses authentication only. It does not discuss how to configure RADIUS attributes to restrict user access to MAX features and services. For information on specifying the MAX features users can access, see Chapter 4, "Setting Up WAN Connections in RADIUS."

Overview of RADIUS authentication

This section describes how the MAX uses RADIUS authentication when answering a call.

By default, when you require a profile for authentication, the MAX always checks for a Connection profile. If it cannot find one, it checks for a Password profile. If neither a Connection profile nor a Password profile exists, the MAX checks for a remote RADIUS, TACACS, or TACACS+ profile.

However, you can change this default by setting Local Profile First=No in the Ethernet > Mod Config > Auth menu. When Local Profile First=No, the MAX first looks for a remote profile. If it cannot find one, the MAX looks for a local Connection profile. If none exists, the MAX looks for a Password profile.

This section assumes that the MAX looks for a local profile first. For an incoming call, the MAX carries out these steps:

1 Before the MAX answers a call, it checks its Answer profile to see whether either CLID authentication or called-number authentication is required.

When CLID authentication is required, the caller's phone number must match a phone number specified in a local Connection profile or RADIUS user profile.When called-number authentication is required, the number called must match a phone number is a local Connection profile or RADIUS user profile. Called-Number authentication is also known as Dialed Number Information Service (DNIS) authentication.

2 If CLID authentication is required (Id Auth=Require in the Answer profile) or if called-number authentication is required (Id Auth=Called Require in the Answer profile), the MAX first looks for a matching phone number in a local Connection profile.

If one does not exist, it then looks for a matching phone number in a RADIUS user profile. If it cannot find the correct phone number, the MAX hangs up.

3 If CLID or called-number authentication is not required (Id Auth=Prefer, Fallback, Ignore, or Called Prefer in the Answer profile), or if the MAX finds a matching phone number in a local Connection profile or RADIUS user profile, it answers the call.

4 The MAX checks its other Answer profile settings.

5 If the Answer profile specifies the type of link encapsulation the call uses, the MAX continues checking Answer profile parameters.

If the Answer profile does not enable the type of link encapsulation the call uses, the MAX drops the call.

6 The MAX checks the value of the Profile Reqd parameter in the Answer profile.

If Profile Reqd=Yes, the MAX must find a Connection profile, Password profile, RADIUS user profile, TACACS profile, or TACACS+ profile to authenticate the call.

7 If a profile is required, the MAX checks to see whether the profile must contain a matching user name and password.

These Answer profile settings require a matching name and password as a condition of authentication:

– Recv Auth=PAP, CHAP, MS-CHAP, or Either (for PPP, MP, and MP+ calls)

– Password Reqd=Yes (for Combinet calls)

8 If name and password authentication is required, the MAX attempts to match the caller's name and password to a local Connection profile.

If authentication succeeds using a local Connection profile, the MAX uses the parameters specified in the profile to build the connection.

9 If it cannot find a matching Connection profile, the MAX looks for a Password profile.

If the MAX finds a Password profile, it uses the name and password in the Password profile and builds the connection using the settings in the Answer profile. The Password profile applies only to ARA, PPP, MP, MP+, and terminal server calls.

10 If it cannot find a matching Password profile, the MAX looks for a RADIUS, TACACS, or TACACS+ profile containing a matching name and password.

If authentication succeeds using a RADIUS user profile, the MAX uses the specified RADIUS attributes to build the connection. The MAX can then forward the call to its bridge/router or other destination. For example, the MAX might forward a terminal server call to a Telnet or TCP host.

If authentication succeeds using a TACACS or TACACS+ profile, the MAX must make a request to the server for information on the resources and services the user can access.

11 If name and password authentication is not required (Recv Auth=None or Password Reqd=No in the Answer profile), the MAX can match IP-routed PPP calls using the IP address specified by the Connection profile.

12 If the Answer profile does not require a profile (Profile Reqd=No), the MAX uses Answer profile parameters to build the connection.

Overview of RADIUS authentication attributes

Table 3-1 summarizes the attributes you can use to set up RADIUS authentication. For more detail on these attributes, see “Reference to RADIUS Attributes” on page 9-1.

Table 3-1. RADIUS authentication attributes

Attribute	Description	Possible values
Ascend-Ara-PW (181)	Indicates the password of the incoming caller over AppleTalk Remote Access (ARA).	Text string containing up to 20 characters. The default value is null. If the caller is to be authenticated by a SecurID server and Auth=RADIUS/LOGOUT, the username must be “SecurID,” and there must be no password.
Ascend-Authen-Alias (203)	Sets this MAX unit’s login name during PPP authentication.	Text string containing up to 16 characters. The default is the value of the Name parameter in the System profile.
Ascend-Callback (246)	Enables or disables callback.	Callback-No (0) Callback-Yes (1) The default value is Callback-No.
Ascend-CBCP-Enable (112)	Specifies how the MAX responds to requests by callers to support CBCP.	• CBCP-Enabled (0)—Specifies that the MAX will positively acknowledge, during LCP negotiations, support for CBCP. • CBCP-Not-Enabled (1)—Specifies that the MAX will reject any request to support CBCP.

Table 3-1. RADIUS authentication attributes (continued)

Attribute	Description	Possible values
Ascend-CBCP-Mode (113)	Specifies what method of callback the MAX offers the incoming caller.	• CBCP-No-Callback (1)—Applies for Windows NT or Windows 95 clients who must not be called back. Because CBCP has been negotiated initially, the Windows clients must have validation from the MAX that no callback is used for this connection. • CBCP-User-Callback (2)—Specifies that the caller will supply the number the MAX uses for the callback. • CBCP-Profile-Callback (3)—Specifies that the MAX will use the number in Ascend-Dial-Number for the callback • CBCP-User-Or-No (7)—Specifies that the caller has the option of either supplying the number to dial or specifying that no callback is used for the call. If no callback is chosen, the call will not be disconnected by the MAX.
Ascend-CBCP-Trunk-Group (115)	Assigns the callback to a MAX trunk group. This attribute is used only when the caller is specifying the phone number the MAX uses for the callback. The value in Ascend-CBCP-Trunk-Group is prepended to the caller-supplied number when the MAX calls back.	Specify a number between 4 and 9, inclusive. The default is 9.
Ascend-Dial-Number (227)	Specifies the phone number the MAX dials to reach the bridge, router, or node at the remote end of the link.	A telephone number containing up to 21 characters, limited to the following: **1234567890()[]!z-*#|** The MAX sends only the numeric characters to place a call. The default value is null.
Ascend-PW-Expiration (21)	Specifies an expiration date for the user's password.	A date in the format ***month day year***. The default is no expiration date.
Ascend-PW-Lifetime (208)	Indicates on a per-user basis the number of days that a password is valid.	Integer. The default is the value of Lifetime-In-Days from the Ascend dictionary.

Table 3-1. RADIUS authentication attributes (continued)

Attribute	Description	Possible values
Ascend-Require-Auth (201)	Indicates whether the MAX requires additional authentication after CLID authentication or called-number authentication. Called-number authentication is also known as Dialed Number Information Service (DNIS) authentication.	Not-Require-Auth (0) Require-Auth (1) The default value is Not-Require-Auth.
Ascend-Receive-Secret (215)	Specifies a value that the RADIUS server uses to authenticate incoming calls from a user while his or her token is cached and alive. The cached token resides on the MAX during the initial security-card authentication process.	Text string containing up to 20 characters. The default value is null.
Ascend-Send-Auth (231)	Specifies the authentication protocol that the MAX requests when initiating a connection using PPP or MP+ encapsulation. The answering side of the connection determines which authentication protocol, if any, the connection uses.	Send-Auth-None (0) Send-Auth-PAP (1) Send-Auth-CHAP (2) The default value is Send-Auth-None.
Ascend-Send-Passwd (232)	Specifies the password that the MAX sends to the remote end of a connection on outgoing calls.	Text string containing up to 20 characters. The default value is null.
Ascend-Send-Secret (214)	Specifies that the system encrypts the password when passing it between the RADIUS server and the MAX on outgoing calls.	Text string containing up to 20 characters. The default value is null.
Ascend-Token-Expiry (204)	Sets the lifetime of a cached token in minutes—that is, the lifetime of hand-held security card authentication.	Integer. The default value is 0 (zero). This setting specifies that token caching is not allowed.
Ascend-Token-Idle (199)	Specifies the maximum length of time in minutes a cached token can remain alive between authentications if a call is idle.	Integer. By default, the token remains alive until the value of Ascend-Token-Expiry is reached.
Ascend-Token-Immediate (200)	Establishes how RADIUS treats the password it receives from a login-user when the user profile specifies a hand-held security card server.	Tok-Imm-No (0) Tok-Imm-Yes (1) The default value is Tok-Imm-No.

Table 3-1. RADIUS authentication attributes (continued)

Attribute	Description	Possible values
Caller-Id (31)	Specifies the calling party number, indicating the phone number of the user that wants to connect to the MAX.	A telephone number containing up to 37 characters, limited to the following: **1234567890()[]!z-*#|** The default value is null.
Challenge-Response (3)	Indicates the password that a Challenge Handshake Authentication Protocol (CHAP) user enters in response to a password challenge.	Alphanumeric string containing up to 252 characters. The default value is null.
Change-Password (17)	Specifies the expired password in an Access-Password-Request packet. When a user specifies an expired password, RADIUS prompts the user for a new password. When the user enters the new password, the MAX sends an Access-Password-Request packet that contains both the old password (as the value of the Change-Password attribute), and the new password (as the value of the Password attribute).	Alphanumeric string containing up to 252 characters. This attribute has no default value, because it does not appear in a user profile.
Class (25)	Enables access providers to classify their user sessions, such as for the purpose of billing users depending on the service option they choose. The MAX sends the Class attribute in Access-Request packets under CLID authentication. Suppose the MAX starts CLID authentication by sending an Access-Request packet and receives the Class attribute in an Access-Accept packet. If the MAX requires further authentication, it includes Class in the Access-Request packet.	Alphanumeric text string containing up to 253 characters. The default value is null.
Client-Port-DNIS (30)	Specifies the called-party number, indicating the phone number the user dialed to connect to the MAX. DNIS stands for Dialed Number Information Service. You use this attribute to set up called-number authentication, also known as DNIS authentication.	A telephone number containing up to 18 characters, limited to the following: **1234567890()[]!z-*#|** The default value is null.

Table 3-1. RADIUS authentication attributes (continued)

Attribute	Description	Possible values
Framed-Protocol (7)	Specifies the type of framed protocol allowed to the user.	PPP (1) SLIP (2) MPP (256) EURAW (257) EUUI (258) COMB (260) FR (261) ARA (262) FR-CIR (263) By default, the MAX does not restrict the type of protocol a user can access.
NAS-Identifier (4)	Indicates the IP address of the MAX.	IP address in dotted decimal notation *n.n.n.n/nn*, where *n* is an integer between 0 and 255, and *nn* is a subnet mask between 8 and 32. The default value is 0.0.0.0/0.
NAS-Port (5)	Specifies the interface and service the session is using.	A 5-digit value in this format: `service line channel` The default value for the RADIUS daemon appears in the /etc/services/ file.
Password (2)	Specifies the user's password. The RADIUS server uses this attribute to authenticate an inbound call using Password Authentication Protocol (PAP) or terminal server authentication.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Name (1)	Specifies the user's name.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Service (6)	Specifies the type of services the user can access.	Login-User (1) Framed-User (2) Dialout-Framed-User (5) By default, the MAX does not restrict a user's access to services.

Specifying a user name

You can specify a user name using the Ascend-Authen-Alias and User-Name attributes, as described in Table 3-2.

Table 3-2. User name attributes

Attribute	Possible values
Ascend-Authen-Alias (203)	Text string containing up to 16 characters. The default is the value of the Name parameter in the System profile.
User-Name (1)	Alphanumeric string containing up to 252 characters. The default value is null. The user name must be the first word in a user profile. You need not specify the name of the attribute.

Because the MAX uses the first matching name for an incoming caller, you must not specify a duplicate user name in any RADIUS user profile.

Setting the User-Name attribute

The following sections describe the specifications you can make for the User-Name attribute.

Using the caller's name

In most instances, the User-Name attribute specifies the name of the calling device or dial-in user. Consider this first line in a user profile:

```
Emma Password="pwd", Ascend-PW-Expiration="Jan 30 1997"
```

The user name is Emma. The RADIUS server tests the user's name and password against the values the user provides when making a request for access. If the RADIUS server does not find a match, it denies the request for access.

Using the caller's MAC address (for Combinet calls)

When Password Reqd=Yes in the Answer profile for a Combinet call, the MAX compares the caller's MAC address to the value of the User-Name attribute, and the value of the caller's password to the value of the Password attribute. When Password Reqd=No, the MAX uses the caller's MAC address only.

Consider this first line in a user profile:

000145CFCF01 Password="m2dan", User-Service=Framed-User

The user name is the MAC address 000145CFCF01.

Note that Combinet bridging cannot use PAP, CHAP, or MS-CHAP authentication. The MAX must use the caller's MAC address and password to authenticate calls.

Using the keyword Default

The RADIUS server uses the Default profile to determine the kind of access it grants to users who do not appear in the users file. You can configure only one Default profile. It must specify the user name Default, and it must be the *last profile* in the users file.

For example, this first line in a profile enables a terminal server user to log in using his or her UNIX account name or password:

```
Default Password="UNIX"
```

Make sure that the Default profile is last one in the file. RADIUS ignores any profiles that follow the Default profile.

Using the incoming phone number (for CLID authentication)

You can require RADIUS to authenticate incoming calls by checking the calling party's phone number. The RADIUS server performs Calling Line ID (CLID) authentication before enabling the MAX to answer an incoming call. You can thereby ensure that the call originates at a known location.

For complete information on configuring CLID authentication, see "Setting up CLID authentication" on page 3-34.

Using the called number (for called-number authentication)

Called-number authentication works much like CLID authentication, except that the MAX uses the number the remote end calls to authenticate the connection. The called number appears in an ISDN message as part of the call when Dialed Number Information Service (DNIS) is in use. Called-number authentication is also known as DNIS authentication.

For complete information on called-number authentication, see "Setting up called-number authentication" on page 3-42.

Using a keyword representing a pseudo-user profile

A pseudo-user profile contains information that the MAX can query. It does not exist for the purpose of authenticating a user. Rather, it enables you to specify static route configurations, Frame Relay profile information, bridging entries, and other types of data. For information on pseudo-user profiles, see one or more of the sections listed in Table 3-3.

Table 3-3. Pseudo-user references

Usage	**Section and page**
Creating a message text and list of hosts in the menu-driven terminal server interface.	"Configuring the message text and a list of hosts" on page 4-42
Configuring outgoing calls	"Setting up outgoing calls" on page 4-58
Setting up a Frame Relay profile	"Setting up the logical link to a Frame Relay switch" on page 5-7

Table 3-3. Pseudo-user references (continued)

Usage	**Section and page**
Setting up a frame relay user profile	"Setting up Frame Relay user connections" on page 5-13
Creating IP address pools	"Defining a pool of IP addresses for dynamic assignment" on page 6-8
Setting up a static IP route	"Configuring static IP routes" on page 6-15
Setting up static IPX routes	"Configuring static IPX routes" on page 6-28
Setting up bridging	"Configuring bridge entries" on page 6-36

Setting the Ascend-Authen-Alias attribute

When the MAX places an outgoing call, it identifies itself by a login name and password. The login name is either its system name (as specified by the Name parameter in the System profile) or the value you specify for the Ascend-Authen-Alias attribute.

This example uses the Ascend-Authen-Alias attribute in an outgoing profile:

```
Homer-Out Password="Ascend", User-Service=Dialout-Framed-User
        User-Name="Homer",
        Ascend-Authen-Alias="myMAXcallingU",
        Ascend-Send-Auth=Send-Auth-PAP,
        Ascend-Send-Secret="passwrd1",
        Ascend-Dial-Number="31",
        Framed-Protocol=PPP,
        Framed-Address=10.0.100.1,
        Framed-Netmask=255.255.255.0,
        Ascend-Metric=2,
        Framed-Routing=None,
        Framed-Route="10.5.0.0/24 10.0.100.1 1",
        Ascend-Idle-Limit=30
```

Specifying a password

A user profile—an entry in the RADIUS users file—must contain an encrypted password to authenticate the caller. You can specify a password using the attributes described in Table 3-4.

Table 3-4. Password attributes

Attribute	Possible values
Ascend-Ara-PW (181)	Text string containing up to 20 characters. The default value is null. The RADIUS server uses this attribute to authenticate an incoming call for an ARA user.
Ascend-Send-Passwd (232)	Text string containing up to 20 characters. The default value is null.
Ascend-Send-Secret (214)	Text string containing up to 20 characters. The default value is null.
Password (2)	Alphanumeric string containing up to 252 characters. The default value is null. The password must appear in the first line of the user profile. The RADIUS server uses this attribute to authenticate an inbound call using Password Authentication Protocol (PAP) or terminal server authentication. You cannot use Challenge Handshake Authentication Protocol (CHAP) or Microsoft CHAP (MS-CHAP) with the UNIX, SAFEWORD, or ACE keywords.

Setting the Password attribute

Table 3-5 lists the specifications you can make for the Password attribute.

Table 3-5. Password specifications

Type	Description	Example
Static	A static password represents a string the user must enter in order to gain access to the MAX.	**Emma Password="pwd"**
UNIX	You can request validation using the / etc/password file on the UNIX host by setting the Password attribute to UNIX. Setting the password to UNIX provides authentication through the normal UNIX authentication procedure.	**John Password="UNIX"**

Table 3-5. Password specifications (continued)

Type	Description	Example
SAFEWORD	You can request validation from the Enigma Logic SafeWord dynamic password library by setting the Password attribute to SAFEWORD.	**Mike Password="SAFEWORD"**
ACE	You can request validation from the Security Dynamics ACE dynamic password library by setting the Password attribute to ACE.	**Connor Password="ACE"**
Ascend-CLID	You can request Calling Line ID (CLID) authentication by setting the Password attribute to Ascend-CLID. If the caller is using ARA and is to be authenticated by a SecurID server and Auth=RADIUS/LOGOUT, the username must be “SecurID,” and there must be no password.	**Emma Password="Ascend-CLID"**
Ascend-DNIS	You can request called-number authentication by setting the Password attribute to Ascend-DNIS.	**Emma Password="Ascend-DNIS"**

Setting the Ascend-Send-Passwd and Ascend-Send-Secret attributes

When the MAX places an outgoing call, it identifies itself by a login name and password. The login name is either the system name (as specified by the Name parameter in the System profile) or the value you specify for the Ascend-Authen-Alias attribute. The password is the value of Send PW (in the local Connection profile) or the value of Ascend-Send-Passwd or Ascend-Send-Secret (in the outgoing RADIUS user profile).

```
This example uses the Ascend-Send-Secret attribute:
Homer-Out Password="Ascend", User-Service=Dialout-Framed-User
        User-Name="Homer",
        Ascend-Authen-Alias="myMAXcallingU",
        Ascend-Send-Auth=Send-Auth-PAP,
        Ascend-Send-Secret="passwrd1",
        Ascend-Dial-Number="31",
        Framed-Protocol=PPP,
        Framed-Address=10.0.100.1,
        Framed-Netmask=255.255.255.0,
        Ascend-Metric=2,
        Framed-Routing=None,
        Framed-Route="10.5.0.0/24 10.0.100.1 1",
        Ascend-Idle-Limit=30
```

Setting the Ascend-Ara-PW attribute

When you set up an ARA connection, you specify a User-Name and Password. Then, you set the Ascend-Ara-PW attribute to the same value specified by the Password attribute. The MAX requires both the Password and the Ascend-Ara-PW attributes. The ARA software in the Ascend unit uses DES to encrypt and decrypt the ARA password. If the caller is to be authenticated by a SecurID server and Auth=RADIUS/LOGOUT, the username must be "SecurID," and there must be no password.

For more information on configuring an ARA link, see "Setting up an ARA connection" on page 4-31.

Configuring password expiration

The Ascend RADIUS daemon supports password aging and expiration, and includes a method for enabling dial-in users to replace expired passwords. A dial-in user can replace expired passwords under these conditions:

- A RADIUS server authenticates the expired password.
- The expired password is not a reserved RADIUS password.

  ACE, SAFEWORD, and UNIX are reserved RADIUS passwords. Although a programmer with access to the daemon source code can change these passwords, they are the default reserved passwords, and typically remain so.
- The password belongs to a user in a terminal server session.

  Users who dial in as an IP router, IP bridge, host-to-bridge, or bridge cannot replace an expired password.

The Ascend RADIUS daemon supports password aging and expiration using the attributes listed in Table 3-6.

Table 3-6. Password expiration attributes

Attribute	Possible values
Ascend-PW-Expiration (21)	A date in the format ***`month day year`***. The default is no expiration date.
Ascend-PW-Lifetime (208)	Integer. The default is the value of Lifetime-In-Days from the Ascend dictionary.

To set up password expiration, follow these steps:

1. On the first line of a RADIUS user profile, specify the Ascend-PW-Expiration attribute.

   Ascend-PW-Expiration specifies an expiration date for a user's password in a user profile. Specify a date in the format ***`month day 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. The values 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.

You must specify Ascend-PW-Expiration when you first create a user and it must appear on the first line of the user profile. If it appears after the first line, RADIUS does not check the expiration date and could accept an expired password. Your specification might look like this one:

```
Emma Password="pwd", Ascend-PW-Expiration="Jan 1, 1997"
```

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.

2 On any line other than the first line of the user profile, set the Ascend-PW-Lifetime attribute.

Ascend-PW-Lifetime specifies the number of days that a password is valid. Your specification might look like this one:

```
Emma Password="pwd", Ascend-PW-Expiration="Jan 1, 1997"
     Ascend-PW-Lifetime=30.
     ...
```

Ascend-PW-Lifetime applies only to the process of renewing an expired password. When the user wants to renew the password, the MAX adds the value you specify for Ascend-PW-Lifetime to the current date and updates the user profile.

How Ascend-PW-Expiration and Ascend-PW-Lifetime work

If a password expires and the user resets it, the RADIUS server adds the value of Ascend-PW-Lifetime to the date on which the user resets the password. The resulting date becomes the new value for Ascend-PW-Expiration.

For example, suppose that today's date is March 1, 1997 and these lines appear in a user profile:

```
Emma Password="pwd", Ascend-PW-Expiration="Jan 1, 1997"
     Ascend-PW-Lifetime=30,
     ...
```

If the user resets the password today, the value of Ascend-PW-Expiration becomes today's date + Ascend-PW-Lifetime, or March 31, 1997.

If the password has not expired, the value of Ascend-PW-Lifetime is irrelevant. For example, suppose that today's date is January 1, 1997 and these lines appear in a user profile:

```
Emma Password="pwd", Ascend-PW-Expiration="Jan 15, 1997"
     Ascend-PW-Lifetime=30
     ...
```

The password expires on January 15, 1997.

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.

Note: If you run the Ascend RADIUS daemon with a flat ASCII file, RADIUS accepts a user’s replacement for an expired password only if you start the daemon with the -p option. For details, see “Running the daemon with a flat ASCII users file” on page 2-7. If you run the daemon in DBM mode, RADIUS accepts a user’s replacement for an expired password if you specify the -p option, but does not recognize the new password until you rebuild the users file database by running builddbm again. For information, see “Creating the DBM database” on page 2-9.

Changing a non-expired password

The MAX supports a password command that enables a RADIUS-authenticated terminal server user to change his or her password. To change a password, follow these steps:

1 Enable password expiration in the user profile.

When you change a non-expired password, the MAX uses the same mechanism that enables you to enter a new password when an older one has expired. To enable password expiration, follow the instructions in “Configuring password expiration” on page 3-13.

2 At the terminal server prompt, enter this command:

```
ascend% password
```

This text displays:

```
ascend% password
Enter old password:
Enter new password:
Re-type new password:
```

3 At the `Enter old password` prompt, specify the current password.

4 At the `Enter new password` and `Re-type new password` prompts, enter the new password.

The new password cannot be null, and must differ from the old password. If the password change is successful, this message displays:

```
Password Updated
```

If the update fails for any reason, this text displays:

```
Password NOT Changed
```

There is no indication of why the password change failed. You may have entered the old password incorrectly. Or, you might be trying to change a UNIX password. You cannot change a UNIX password using the password command, because a UNIX password does not reside in the RADIUS database.

Changing an expired password

When a user attempts to establish a terminal server connection using an expired password, these events take place:

1 The MAX informs the user that the authentication failed because the password has expired.

2 The MAX prompts the user for a new password.

If the new password is null or matches the old password, the MAX prompts the user again for a new password.

If the new password is valid, the MAX asks the user to re-enter it for confirmation. If the two entries do not match, the MAX prompts again for a new password.

3 After receiving a valid confirmation of the new password, the MAX contacts the RADIUS server for acceptance of the new password.

If the RADIUS server accepts the new password, it reports the successful change.

If the RADIUS server rejects the new password, it informs the user and prompts again for a new password. The RADIUS server can reject the password change for any of these reasons:

- You did not start the RADIUS daemon with the -p option.
- The file system containing the RADIUS users file is full and the system cannot update the entry.
- The RADIUS users file is locked against writing.
- The RADIUS daemon is running in DBM mode.

  When the daemon is running in DBM mode, a user can successfully change an expired password, but cannot gain access to the network immediately. Access using the new password can take place only after you rebuild the RADIUS database with the modified users file containing the new password.

Specifying the MAX unit's IP address

When the MAX sends an Access-Request packet, it uses the NAS-Identifier attribute to indicate its IP address to the RADIUS server. Table 3-7 describes this attribute.

Table 3-7. NAS-Identifier attribute

Attribute	**Possible values**
NAS-Identifier (4)	IP address in dotted decimal notation *n.n.n.n/nn*, where *n* is an integer between 0 and 255, and *nn* is a subnet mask between 8 and 32. The default value is 0.0.0.0/0.

NAS-Identifier example

In most cases, you never need to specify the NAS-Identifier attribute in a user profile.

However, you might want to specify it if multiple MAX units use a single RADIUS server, and you want to specify the MAX to which a particular user can connect. In this case, the NAS-Identifier value in the Access-Request packet and the NAS-Identifier value in the user profile must match for the RADIUS server to authenticate the connection. The NAS-Identifier value must appear in the first line of the user profile.

Suppose that the user Emma is allowed to dial into the MAX at IP address 200.65.212.46. The first line of the user profile might look like this one:

```
Emma Password="pwd", NAS-Identifier=200.65.212.46
```

Setting up the MAX for callback

There are two types of callback security: Ascend callback and Microsoft’s callback security.

Ascend callback security

Callback security instructs the MAX to hang up and call back when it receives an incoming call. You can require callback to ensure that the MAX makes a connection with a known device. You can specify callback for switched lines only.

To set up the MAX for callback, use the attributes listed in Table 3-8.

Table 3-8. Callback attributes

Attribute	Possible values
Ascend-Callback (246)	Callback-No (0) Callback-Yes (1) The default value is Callback-No.
Ascend-Dial-Number (227)	A telephone number containing up to 21 characters, limited to the following: **1234567890()[]!z-*#|** The MAX sends only the numeric characters to place a call. The default value is null.
Ascend-Send-Passwd (232)	Text string containing up to 20 characters. The default value is null.
Ascend-Send-Secret (214)	Text string containing up to 20 characters. The default value is null.

To set up the MAX for callback, follow these steps:

1. Set Ascend-Callback=Callback-Yes.
2. Set Ascend-Dial-Number to the phone number of the remote device.

   The MAX can also use the CLID in order to reach the remote end of the connection, if the CLID is available.
3. Set Ascend-Send-Secret or Ascend-Send-Passwd.

   Both of these attributes specify the password that the MAX sends to the remote end of a connection on outgoing calls. If the value you specify for Ascend-Send-Secret or Ascend-Send-Password does not match the remote end's value for Ascend-Receive-Secret (in a RADIUS user profile) or Recv PW (in a Connection profile), the remote system rejects the call.

   Use Ascend-Send-Passwd only if your version of the MAX does not support Ascend-Send-Secret.

When you set Ascend-Callback=Callback-Yes, these events occur:

1. The MAX hangs up after receiving an incoming call that matches the one specified in the RADIUS user profile.
2. The MAX then calls back the device at the remote end of the link using these values:
   – The number specified by the Ascend-Dial-Number attribute or the CLID
   – The password specified by Ascend-Send-Passwd or Ascend-Send-Secret

Note: If you set up a RADIUS user profile for callback and CLID-only authentication, the MAX never answers the call. The caller can therefore avoid billing charges.

Callback example

Consider these lines from a user profile:

```
Emma Password="pwd"
     Ascend-Callback=Callback-Yes,
     Ascend-Dial-Number=555-1213,
     Ascend-Send-Secret="mysecret",
     ...
```

When a user named Emma dials in, the MAX hangs up and calls the number 555-1213.

Microsoft's Callback Control Protocol (CBCP)

Microsoft developed CBCP to address a need for greater security with PPP connections. The standardized callback option defined in RFC 1570 has a potential security risk because the authentication is performed after the callback. CBCP callback like Ascend's proprietary callback, occurs after authentication, leaving no potential security hole.

CBCP also offers features not available with the standard callback defined in RFC 1570. The client side supports a configurable time delay to allow users to initialize modems or enable supportive software before the MAX calls the client. You can configure the MAX with a phone number to use for the callback, or you can configure it to allow the client to specify the phone number used for the callback.

Currently, Microsoft's Windows NT 4.0 and Windows 95 software support client-side authentication using CBCP. The MAX now supports a CBCP central-site solution.

Ascend's implementation of CBCP

CBCP is an option negotiated during the LCP negotiation of a PPP session. While support for CBCP is configured systemwide on the MAX, not every connection must negotiate its use. Parameters for configuring CBCP on the MAX are in the Answer Profile under Ethernet > Answer > PPP Options, and in each User Profile. The calling and called sides of a PPP session initiate authentication after acknowledging that CBCP is to be used.

Note: Currently, the MAX does not initiate LCP negotiation of CBCP. The MAX responds to *caller* requests to configure CBCP.

The MAX employs the user name and password to link a caller with a specific RADIUS User profile. Configured CBCP parameters in that User profile specify variables for the callback. If, at any point, the client and the MAX disagree about any CBCP variables, the MAX drops the connection.

Both sides of the connection must agree on whether the callback phone number is supplied by the client or by the MAX. The trunk group parameter Ascend-CBCP-Trunk-Group, configured on the MAX, supplies a trunk group that is prepended to phone numbers supplied by the client.

Table 3-9 lists Microsoft's callback parameters on the MAX.

Table 3-9. Microsoft's CBCP parameters for RADIUS

Attribute	Possible values
Ascend-CBCP-Enable (112)	CBCP-Enabled (0) CBCP-Not-Enabled (1)
Ascend-CBCP-Mode (113)	
Ascend-CBCP-Trunk-Group (115)	

Negotiation of CBCP

Following are the steps from initial connection to MAX callback:

1 Caller connects to MAX.

2 LCP negotiations begin.
Caller and MAX must agree to use CBCP. Otherwise, the MAX terminates the connection.

3 After successful LCP negotiation, both sides have acknowledged that CBCP will be used.

4 Caller authenticates itself to the MAX. If authentication fails, the MAX terminates the connection.

5 CBCP begins if the MAX verifies that the profile has Ascend-CBCP-Mode set.

6 The MAX sends a request to determine if a callback is to occur. The caller's configuration must match the Ascend-CBCP-Mode value on the MAX.
The client also supplies to the MAX the number of seconds it should delay before initiating the callback, and, if applicable, the phone number.

7 If both sides agree on which phone number the MAX will dial, the client clears the connection.

8 The MAX delays the callback on the basis of the previous negotiation.

9 The MAX dials the client, by applying information from the same profile used in previous negotiation.

Configuring Microsoft's CBCP to use a User Profile

To configure CBCP to work with a User profile:

1 Open the Ethernet > Answer > PPP Options menu.

2 Set CBCP Enable = Yes.

3 Find the user profile you want to add callback.

4 Set Ascend-CBCP-Mode to the callback mode to be offered the caller.

5 If the caller is supplying the phone number, set Ascend-CBCP-Trunk Group to the value (4 through 9) that the MAX prepends to the number when calling back.

6 Save your changes.

Specifying an access protocol for incoming calls

The answering unit always determines the authentication method to use for the call. By default, the MAX allows incoming calls without authentication. This section summarizes different types of authentication protocols you can require for incoming calls.

Requiring PAP, CHAP, or MS-CHAP for PPP, MP, and MP+ calls

To specify an authentication protocol for name and password authentication of PPP, MP, and MP+ calls, set the Recv Auth parameter in the Ethernet > Answer > PPP Options menu to one of the values listed in Table 3-10.

Table 3-10.Recv Auth values

Setting	Description
PAP	A PPP authentication protocol that provides a simple method for the MAX to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment, and does not use encryption. The remote device must support PAP.
CHAP	A PPP authentication protocol that is more secure than PAP. CHAP provides a way for the remote device to periodically verify the identity of the MAX using a three-way handshake and encryption. Authentication takes place upon initial link establishment. A device can repeat the authentication process any time after the connection takes place. The remote device must support CHAP.

Table 3-10.Recv Auth values (continued)

Setting	Description
MS-CHAP	The Windows NT version of CHAP, which uses DES and MD4 encryption. Using MS-CHAP, an Ascend unit can authenticate a Windows NT system, and a Windows NT system can authenticate an Ascend unit.
Either	Specifies that the Ascend unit allows authentication if the remote unit uses any of the designated authentication schemes. The MAX first tries to use MS-CHAP. If the remote end of the connection does not support it, the MAX then attempts to use CHAP. If the remote end of the connection does not support CHAP, the MAX uses PAP instead.

If the incoming PPP call does not include a source IP address, the MAX requires PAP, CHAP, or MS-CHAP authentication. PAP, CHAP, and MS-CHAP authentication is not available for Combinet, ARA, modem, V.110, V.120 calls, or X.75 calls.

For PAP, CHAP, and MS-CHAP authentication, the calling unit and the MAX share a different secret with the RADIUS server:

- The calling unit's secret is called the remote secret. The MAX does not know the value of this secret.
- The MAX unit's secret is called the NAS secret (because the MAX is an NAS). The calling unit does not know the value of this secret.

How PAP works

For PAP authentication, these events take place:

1. The calling unit sends the remote secret in the clear to the MAX.
2. The MAX encrypts the remote secret using the NAS secret.
3. The RADIUS server decrypts the remote secret using the NAS secret.
4. The RADIUS server validates the remote secret, or passes the clear copy of the remote secret to a UNIX or other password validation system.

How CHAP and MS-CHAP work

For CHAP and MS-CHAP authentication, these events take place:

1. The MAX sends a random, 128-bit challenge to the calling unit.
2. The calling unit calculates an MD5 digest using the remote secret, the challenge, and the PPP packet ID.
3. The calling unit sends the MD5 digest, the challenge, and the PPP packet ID (but not the remote secret) to the MAX.

   The MAX never has the remote secret.

4 The MAX forwards the digest, along with the original challenge and PPP packet ID to RADIUS.

No encryption is necessary, because MD5 creates a one-way code that cannot be decoded. In addition, RADIUS cannot extract the remote secret. Therefore, it cannot provide a password to a UNIX password system. For this reason, CHAP and UNIX authentication cannot work together.

5 The RADIUS server looks up the remote secret from a local database, and calculates an MD5 digest using the local version of the remote secret, along with the challenge and the PPP packet ID it received from the MAX.

6 The RADIUS server compares the calculated MD5 digest with the digest it received from the MAX.

If the digests are the same, the remote secrets used by the calling unit and the RADIUS server are the same, and the MAX authenticates the call.

Requiring PAP-TOKEN, CACHE-TOKEN, or PAP-TOKEN-CHAP

You can set up SafeWord and ACE security-card authentication of incoming calls using PAP-TOKEN, CACHE-TOKEN, or PAP-TOKEN-CHAP authentication. This section provides an overview of these access methods. For details on configuring security-card authentication, see “Setting up security-card authentication” on page 3-25.

How PAP-TOKEN works

PAP-TOKEN specifies an extension of PAP authentication. In PAP-TOKEN, the user authenticates his or her identity by entering a password derived from a hardware device, such as a hand-held security card. The MAX prompts the user for this password, possibly along with a challenge key. It obtains the challenge key from a security server that it accesses through RADIUS.

For information on setting up PAP-TOKEN authentication, see “Configuring PAP-TOKEN authentication” on page 3-29.

How CACHE-TOKEN works

CACHE-TOKEN authentication uses a shared secret, and simplifies the authentication process by caching the user’s token for the fixed length of time specified by the Ascend-Token-Expiry attribute. During the lifetime of the token, subsequent calls by the user require only CHAP authentication without the use of a hand-held security card.

For information on setting up CACHE-TOKEN authentication, see “Configuring CACHE-TOKEN authentication” on page 3-30.

How PAP-TOKEN-CHAP works

PAP-TOKEN-CHAP authentication uses an encrypted CHAP password with which the answering unit authenticates the second and subsequent channels of an MP+ call. You verify only the initial connection using a hand-held security card. CHAP verifies any additional channels. For information on setting up PAP-TOKEN-CHAP authentication, see "Configuring PAP-TOKEN-CHAP authentication" on page 3-32.

Note: You can also set up an ACE server to authenticate multiple users behind a remote router. For information on carry out this task, see "Configuring ACE authentication for remote bridge/router users" on page 3-33.

Using different access methods with local authentication

Some authentication methods do not work the same way with a local Connection profile as with a RADIUS user profile. Table 3-11 shows the specific information you need to consider if you use a particular method with a local profile.

Table 3-11.Access methods and local authentication

Method	Remote Authentication Considerations
PAP	None. PAP works the same way with both local and remote authentication.
CHAP	None. CHAP works the same way with both local and remote authentication.
PAP-TOKEN	Works with both local and remote authentication, but does not produce a challenge with a local profile. This response defeats the security of using PAP-TOKEN.
PAP-TOKEN-CHAP	Brings up one channel, but all other channels fail.
CACHE-TOKEN	If the remote side has ever authenticated using a challenge, CACHE-TOKEN does not work with a local profile. If the remote side has not ever authenticated, no problem occurs with a local profile.

Requesting an access protocol for outgoing calls

To request an authentication protocol for an outgoing PPP or MP+ call, use the attributes described in Table 3-12.

Table 3-12.Authentication protocol attributes

Attribute	Possible values
Ascend-Send-Auth (231)	Send-Auth-None (0) Send-Auth-PAP (1) Send-Auth-CHAP (2) The default value is Send-Auth-None.
Ascend-Send-Passwd (232)	Text string containing up to 20 characters. The default value is null.

Table 3-12.Authentication protocol attributes (continued)

Attribute	Possible values
Ascend-Send-Secret (214)	Text string containing up to 20 characters. The default value is null.

To specify an authentication protocol for an outgoing PPP or MP+ call, follow these steps:

1 Set the Ascend-Send-Auth attribute.

The Ascend-Send-Auth attribute specifies the authentication protocol that the MAX requests when initiating a connection using PPP or MP+ encapsulation. The answering side of the connection determines which authentication protocol, if any, the connection uses. You can set Ascend-Send-Auth to one of these values:

– Send-Auth-None (0) specifies that the MAX does not request an authentication protocol for outgoing calls. This setting is the default.

– Send-Auth-PAP (1) specifies that the MAX requests Password Authentication Protocol (PAP). If you choose this setting, the MAX requests PAP authentication, but uses CHAP authentication if the called unit requires CHAP. Choose this setting for non-token card authentication if you want to send your password unencrypted.

For details on how PAP operates, see “How PAP works” on page 3-21

– Send-Auth-CHAP (2) specifies that the MAX requests Challenge Handshake Authentication Protocol (CHAP). If you choose this setting, the MAX does not bring up the connection using PAP. Choose this setting for non-token card authentication if you do not wish to send your password unencrypted—that is, if you do not wish to use PAP authentication.

For details on how CHAP operates, see “How CHAP and MS-CHAP work” on page 3-21.

2 If you request PAP or CHAP authentication, you must also specify a password using Ascend-Send-Secret or Ascend-Send-Passwd.

Both of these attributes specify the password that the MAX sends to the remote end of a connection on outgoing calls. If the value you specify for Ascend-Send-Secret or Ascend-Send-Password does not match the remote end’s value for Ascend-Receive-Secret (in a RADIUS user profile) or Recv PW (in a Connection profile), the remote system rejects the call.

Use Ascend-Send-Passwd only if your version of the MAX does not support Ascend-Send-Secret.

For complete information on setting up an outgoing call in RADIUS, see “Setting up outgoing calls” on page 4-58.

CHAP example

In this example, the user profile requests CHAP as the authentication method for an outgoing PPP call:

```
Homer-Out Password="Ascend", User-Service=Dialout-Framed-User
        User-Name="Homer",
        Ascend-Send-Auth=Send-Auth-CHAP,
        Ascend-Send-Secret="passwrd1",
        Ascend-Dial-Number="31",
        Framed-Protocol=PPP,
        Framed-Address=10.0.100.1,
        Framed-Netmask=255.255.255.0,
        Ascend-Metric=2,
        Framed-Routing=None,
        Framed-Route="10.5.0.0/24 10.0.100.1 1",
        Ascend-Idle-Limit=30
```

Setting up security-card authentication

This section covers the following topics:

- Introducing security-card authentication
- Configuring the MAX to recognize the authentication server
- Configuring the MAX to recognize the APP Server utility on each workstation
- Configuring PAP-TOKEN authentication
- Configuring CACHE-TOKEN authentication
- Configuring PAP-TOKEN-CHAP authentication

Note: You can use RADIUS to set up security-card authentication of *incoming calls only*. If you want to configure the MAX as the calling unit and enable local security-card users to call a remote site, you must configure a Connection profile in the MAX configuration interface. For details, see the MAX *Security Supplement*.

Introducing security-card authentication

You can set up your network site to require that users change passwords very frequently, many times per day. When you do so, you use an external authentication server, such as a Security Dynamics ACE/Server or an Enigma Logic SafeWord server.The external server syncs up with hand-held personal security “cards”, devices the size and shape of a credit card. The security card provides a user with a current password in real time. The LCD on the user’s card displays the current, one-time-only password required to gain access at that moment to the secure network.

Figure 3-1 illustrates an environment that includes an Ascend Pipeline as the calling unit, an NAS (the MAX), a RADIUS server, and an external authentication server.

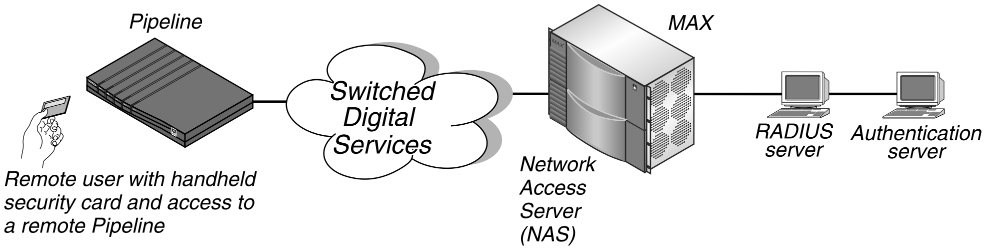
Pipeline
Remote user with handheld security card and access to a remote Pipeline
Switched Digital Services
MAX
Network Access Server (NAS)
RADIUS server
Authentication server

Figure 3-1. Using an external authentication server

When you use security-card authentication, these events take place:

1 A user attempts to open a connection to the MAX, sending his or her user name.

This user is a client of the MAX. The user can be in terminal server mode or use the APP Server utility during the authentication phase. When authentication is complete, the user can switch to PPP mode.

2 The MAX determines that it must use a RADIUS user profile to authenticate the user.

3 The MAX sends the user connection request to the RADIUS server in an Access-Request packet.

The MAX is a client of the RADIUS server.

4 The RADIUS server forwards the connection request to the ACE or SafeWord client residing on the same system as RADIUS.

5 The ACE client forwards the information to the ACE/Server authentication server, and the SafeWord client forwards the information to the SafeWord authentication server.

In these cases, the RADIUS server is a client of the authentication server.

6 The authentication server sends an Access-Challenge packet back through the RADIUS server and the MAX to the user dialing in.

7 The user sees the challenge message and obtains the current password from his or her security card.

If the authentication server is an ACE/Server, the user has a SecurID token card that displays a randomly generated access code. This code changes every 60 seconds.

If the authentication server is a SafeWord server, the user can have one of these types of token cards:

- ActivCard
- CryptoCard
- DES Gold
- DES Silver
- SafeWord SofToken
- SafeWord MultiSync
- DigiPass
- SecureNet Key
- WatchWord

8 The user enters the current password he or she obtained from the security card in response to the challenge message.

This password travels back through the NAS and the RADIUS server to the authentication server.

9 The authentication server sends a response to the RADIUS server, specifying whether the user has entered the proper user name and password.

Note: If the caller is using AppleTalk Remote Access (ARA) there must be no password, and the username must be “SecurID.” Once the user makes the initial connection, SecurID authentication begins with a pop-up screen on the Macintosh. At this point, the user must enter the "User ID" and "Passcode". If the user enters incorrect values, he or she gets two more tries to authenticate before the connection fails.

If the user enters an incorrect password, the ACE/Server or SafeWord server returns another challenge and the user can again attempt to enter the correct password. The server sends up to three challenges. After three incorrect entries, the MAX terminates the call.

10 The RADIUS server sends an authentication response to the MAX.

If authentication is unsuccessful, the MAX receives an Access-Reject packet. If authentication is successful, the MAX receives an Access-Accept packet containing a list of attributes from the user profile in the RADIUS server’s database. The MAX then establishes network access for the caller.

Configuring the MAX to recognize the authentication server

For the MAX to communicate with the authentication server, you must set the parameters in Table 3-13.

Table 3-13.Authentication server parameters

Location	Parameters with sample values
Ethernet > Mod Config > DNS	Password Host=10.0.0.1
Ethernet > Mod Config > Auth	Password Port=10 Password Server=Yes

All of the parameters apply only to outgoing calls using security-card authentication. For the parameters to work, you must meet these conditions:

- The MAX must request PAP-TOKEN authentication. For details, see “Configuring PAP-TOKEN authentication” on page 3-29.
- You must have the APP Server utility running on a UNIX or Windows workstation on the local network.

  Ascend Password Protocol (APP) is a UDP protocol from Ascend. For details on installing the APP Server utility, see the MAX *Security Supplement*.

To configure the MAX to recognize the authentication server, follow these steps:

1 Open the Ethernet menu.

2 Open the Mod Config menu.

3 Open the DNS menu.

4 For the Password Host parameter, specify the IP address of the authentication server on the remote network.

5 Return to the Mod Config menu and open the Auth menu.

6 For the Password Port parameter, specify the User Datagram Protocol (UDP) port number that the server indicated by Password Host is monitoring.

Valid port numbers range from 0 to 65535. The default value is 0 (zero). This setting indicates that the authentication server is not monitoring a UDP port.

7 Set Password Server=Yes.

This setting specifies that callers use security-card authentication rather than terminal server authentication.

8 Save your changes.

Configuring the MAX to recognize the APP Server utility

To allow users to supply token passwords from a PC or UNIX host on the local network, you must configure the MAX to communicate with the APP Server utility on that host. Table 3-14 lists the parameters to set.

Table 3-14.APP Server parameters

Location	Parameters with sample values
Ethernet > Mod Config > Auth	APP Server=Yes APP Host=10.65.212.1 APP Port=7001

Ascend Password Protocol (APP) is a UDP protocol whose default port is 7001. The communication between the MAX and the host running the APP Server may be unicast (when both the MAX and the host have an IP address) or broadcast (when the host may not have an IP address)

To setup the MAX to communicate with the APP Server utility, follow these steps:

1 Open the Ethernet menu.

2 Open the Mod Config menu.

3 Open the Auth menu.

4 Set APP Server=Yes.

This setting enables the MAX to communicate password challenges to the host running the APP Server utility.

5 Specify the IP address of the host running the APP Server utility.

For example, you must enter this setting:

```
APP Host=10.65.212.1
```

If the host obtains its address at boot time from a BOOTP or DHCP server, or if it has no IP address, you can specify the IP broadcast address (255.255.255.255).

6 Specify the UDP port to use for communicating with the host running the APP Server.

7001 is the default UDP port for the APP Server. If you change this number, you must specify the new UDP port number in the APP Server utility (DOS), the WIN.INI file (Windows), or the /etc/services file (UNIX). The MAX and the host running the APP Server utility must agree about the UDP port number.

7 Save your changes.

Configuring PAP-TOKEN authentication

To set up PAP-TOKEN authentication, use the attributes listed in Table 3-15.

Table 3-15.PAP-TOKEN attributes

Attribute	Possible values
Password (2)	SAFEWORD or ACE. The default value is null.
User-Name (1)	Text string containing up to 252 characters. The default value is null.

To set up PAP-TOKEN authentication, follow these steps:

1 Set the User-Name attribute to the remote bridge/router’s system name.

2 Set the Password attribute to SAFEWORD or ACE.

You can request validation from the Enigma Logic SafeWord dynamic password library by setting the Password attribute to SAFEWORD, as shown in this first line of a user profile:

```
Mike Password="SAFEWORD"
```

You can request validation from the Security Dynamics ACE dynamic password library by setting the Password attribute to ACE, as shown in this first line of a user profile:

```
Connor Password="ACE"
```

PAP-TOKEN example for Security Dynamics ACE/Server

This example shows how to set up RADIUS for use with the Security Dynamics ACE/Server. The remote end consists of a PC running Appserv and a Pipeline 50 unit. The local end consists of a MAX and a UNIX device running RADIUS, ACE/Client, and ACE/Server. Figure 3-2 shows the WAN configuration.

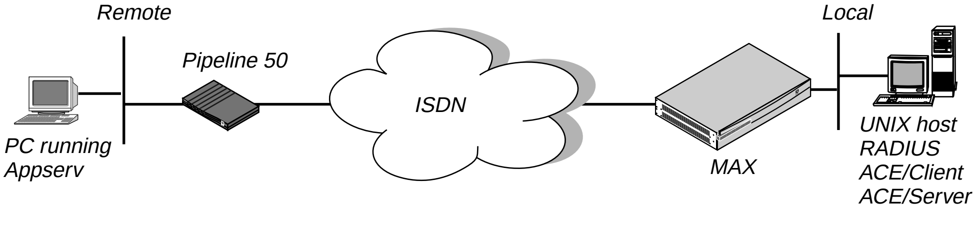

Figure 3-2. ACE/Server configuration

At the remote end, the Appserv process constantly monitors for authentication requests. When it receives one from the Pipeline 50, it sends the request to the MAX. The MAX tries to match the caller's Name to the value of the Station parameter in a Connection profile. If the MAX does not find a match, it forwards the request to RADIUS. RADIUS then checks its profiles. If it finds one whose password is set to ACE, it requests that Appserv prompt the Pipeline 50 for a passcode.

To modify an existing profile for ACE/Server authentication, simply change the password to ACE, as in this example:

```
Connor Password="ACE"
       User-Service=Framed-User,
       Framed-Protocol=MPP,
       Framed-Address=200.72.138.1,
       Framed-Netmask=255.255.255.0,
       Ascend-Idle-Limit=300,
       Framed-Routing=None
```

Configuring CACHE-TOKEN authentication

To set up CACHE-TOKEN authentication, use the attributes listed in Table 3-16.

Table 3-16.CACHE-TOKEN attributes

Attribute	Possible values
Ascend-Receive-Secret (215)	Text string containing up to 20 characters. The default value is null.
Ascend-Token-Expiry (204)	Integer. The default value is 0 (zero). This setting specifies that token caching is not allowed.
Ascend-Token-Idle (199)	Integer. By default, the token remains alive until the value of Ascend-Token-Expiry is reached.
Ascend-Token-Immediate (200)	Tok-Imm-No (0) Tok-Imm-Yes (1) The default value is Tok-Imm-No.
Password (2)	SAFEWORD or ACE. The default value is null.
User-Name (1)	Text string containing up to 252 characters. The default value is null.

To set up CACHE-TOKEN authentication, follow these steps:

1. Set the User-Name attribute to the remote bridge/router's system name.
2. Set the Password attribute to SAFEWORD or ACE.

   You can request validation from the Enigma Logic SafeWord dynamic password library by setting the Password attribute to SAFEWORD, as shown in this first line of a user profile:

   ```
   Mike Password="SAFEWORD"
   ```

You can request validation from the Security Dynamics ACE dynamic password library by setting the Password attribute to ACE, as shown in this first line of a user profile:

```
Connor Password="ACE"
```

3 On the first line of the user profile, set the Ascend-Token-Expiry attribute to a nonzero value.

The Ascend-Token-Expiry attribute specifies the lifetime in minutes of a cached token. When the cached token is still alive, CHAP authenticates subsequent CACHE-TOKEN access requests from the same user without the use of a hand-held security card. When the cached token has expired, the ACE or SAFEWORD server authenticates CACHE-TOKEN access requests.

If the Ascend-Token-Expiry is not specified in the user profile or is set to 0 (zero), the MAX rejects subsequent calls.

4 On the first line of the user profile, set the Ascend-Token-Idle attribute (optional).

The Ascend-Token-Idle attribute specifies the maximum length of time in minutes a cached token can remain alive between authentications. This attribute is useful for enforcing authentication when a connection comes up again after an idle period. If you do not specify this attribute, the cached token remains alive until the value of the Ascend-Token-Expiry attribute causes it to expire. Typically, the value of Ascend-Token-Idle is lower than the value of Ascend-Token-Expiry.

5 On the first line of the user profile, set the Ascend-Token-Immediate attribute.

The Ascend-Token-Immediate attribute establishes how RADIUS treats the password it receives from a login user when the user profile specifies a hand-held security card server. Use this attribute in an ACE or SAFEWORD user profile that contains the setting User-Service=Login-User.

Ascend-Token-Immediate can have one of the following values:

– Tok-Imm-No (0) indicates that RADIUS ignores the password. Choose this value for a security server that requires that a user enter a challenge using a security card before the security server derives a password.

– Tok-Imm-Yes (1) specifies that RADIUS sends the password to the security server for authentication.

6 On any line of the profile after the first one, set the Ascend-Receive-Secret attribute to the same password as the Send PW parameter in the Connection profile that places the incoming call.

The RADIUS server uses this value to authenticate incoming calls from a user while his or her token is cached and alive. The cached token resides on the MAX during the initial security-card authentication process.

7 When you start the radius daemon, specify the -c option to enable cache-token authentication.

CACHE-TOKEN example for Enigma Logic server

The following example shows the settings necessary for a user called John to use an Enigma Logic server. After MP+ authentication, the user receives the IP address 200.0.5.1 and subnet mask 255.255.255.0. The profile specifies a 90-minute token cache and an 80-minute idle limit. Notice that the Ascend-Token-Expiry, Ascend-Token-Idle, and Ascend-Token-Immediate attributes must appear on the first line of the profile, along with the user name and ACE or SAFEWORD password. RADIUS sends the password to the security server for authentication.

```
John  Password="SAFEWORD", Ascend-Token-Expiry=90, Ascend-
Token-Idle=80, Ascend-Token-Immediate=Tok-Imm-Yes
      Ascend-Receive-Secret="shared-secret",
      User-Service=Framed-User,
      Framed-Protocol=MPP,
      Framed-Address=200.0.5.1,
      Framed-Netmask=255.255.255.0
```

Configuring PAP-TOKEN-CHAP authentication

To set up PAP-TOKEN-CHAP authentication, use the attributes listed in Table 3-17.

Table 3-17.PAP-TOKEN-CHAP attributes

Attribute	Possible values
Ascend-Receive-Secret (215)	Text string containing up to 20 characters. The default value is null.
Password (2)	SAFEWORD or ACE. The default value is null.
User-Name (1)	Text string containing up to 252 characters. The default value is null.

To set up PAP-TOKEN-CHAP authentication, follow these steps:

1. Set the User-Name attribute to the remote bridge/router's system name.
2. Set the Password attribute to SAFEWORD or ACE.

   You can request validation from the Enigma Logic SafeWord dynamic password library by setting the Password attribute to SAFEWORD, as shown in this first line of a user profile:

   ```
   Mike Password="SAFEWORD"
   ```

   You can request validation from the Security Dynamics ACE dynamic password library by setting the Password attribute to ACE, as shown in this first line of a user profile:

   ```
   Connor Password="ACE"
   ```

3. Set Ascend-Receive-Secret to the value of the Aux Send PW parameter in the Connection profile the remote end uses to dial the call.

   The RADIUS server sends this value to your MAX in order to verify an encrypted password.

   In PAP-TOKEN-CHAP authentication, you need to verify only the initial connection using a hand-held security card. CHAP verifies any additional channels. That is, whenever the MAX adds channels to a PPP or MP+ call using PAP-TOKEN-CHAP, the calling unit sends the encrypted value of Aux Send PW, and the answering unit checks this password against Ascend-Receive-Secret. The answering unit receives Ascend-Receive-Secret from the RADIUS server when the first channel of the call connects.

PAP-TOKEN-CHAP example for Enigma Logic server

The following example shows the settings necessary for a user called Emma 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 subnet mask 255.255.255.0. Because this profile includes the attribute Ascend-Receive-Secret, the MAX can authenticate additional channels through CHAP without having to go to the SAFEWORD server for authentication.

```
Emma  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"
```

Configuring ACE authentication for remote bridge/router users

To set up ACE authentication for users behind a remote bridge/router, use the attributes listed in Table 3-18.

Table 3-18.ACE authentication attributes for remote users

Attribute	Possible values
Password (2)	Text string containing up to 252 characters. The default value is null. In this instance, specify ACE.
User-Name (1)	Text string containing up to 252 characters. The default value is null. In this instance, specify the system name of the remote router.

To specify that the RADIUS server use an ACE profile to authenticate multiple users behind a single remote bridge/router (such as an Ascend Pipeline unit), follow these steps:

1. Set the User-Name attribute to the remote router's system name.
2. Set the Password attribute to ACE.

When the user enters the dynamic password from a security card, he or she must enter it in this format:

`password.`*`realname`*

`realname` is the user's real name. The RADIUS server presents the *`realname`* argument, rather than the name of the Pipeline, to the ACE server. Token caching still functions normally. All users share the same profile, and all accounting uses the Pipeline name, not the real user name.

Setting up CLID authentication

You can require RADIUS to authenticate incoming calls by checking the calling party's phone number. The RADIUS server performs Calling Line ID (CLID) authentication before enabling the MAX to answer an incoming call. You can thereby ensure that the call originates at a known location.

This section describes how to set up a RADIUS user profile for CLID authentication. You can choose from these configurations:

- Authenticate all callers using name, password, and caller ID. For details, see "Scenario 1: Authentication using name, password, and caller ID" on page 3-35.
- Authenticate all callers using a caller ID only. For details, see "Scenario 2: Authentication using a caller ID only" on page 3-36.
- Use an external authentication server, such as a token-card authentication server, to authenticate users after CLID authentication. For details, see "Scenario 3: External authentication after CLID authentication" on page 3-38.
- Request PAP, CHAP, or MS-CHAP after CLID authentication. For details, see "Scenario 4: PAP, CHAP, or MS-CHAP after CLID authentication" on page 3-39.

Before you begin

Before you set up CLID in RADIUS, you must set parameters in the MAX configuration interface that affect CLID authentication. Follow these steps:

1 Open the Ethernet menu.

2 Open the Answer menu.

3 If you want to authenticate callers by name, password, and caller ID, set Id Auth=Prefer.

This setting specifies that whenever CLID is available, the MAX checks the calling party's phone number against the value of the Caller-Id attribute in a RADIUS user profile. If it finds a match, and the profile does not require any further authentication, the MAX accepts the call. If the CLID is not available, or if the MAX cannot find a match to the calling party number, the MAX applies authentication using the Recv Auth parameter in the PPP Options menu.

4 If you want to authenticate callers by caller ID only, set Id Auth=Require or Fallback.

The Require setting indicates that the calling party's phone number must match the value of the Caller-Id attribute before the MAX can answer the call. If CLID is not available, the MAX does not answer the call.

The Fallback setting handles the case of RADIUS server timeouts. If the RADIUS server query times out so that the MAX cannot complete CLID authentication, the MAX does not drop the call. Instead it looks for a resident Connection profile to use for standard PAP, CHAP, MS-CHAP, or terminal server authentication. Therefore, if you set Id Auth=Fallback, you must also set up a Connection profile. For details, see the MAX *Security Supplement*.

5 Open the PPP Options menu.

6 If you plan to use PAP, CHAP, or MS-CHAP after CLID authentication, set the Recv Auth parameter to the appropriate value.

7 Open the Ethernet > Mod Config > Auth menu.

8 Specify the value of the Disconnect message the MAX returns when CLID authentication fails.

When CLID authentication fails in an ISDN connection, the MAX sends a Disconnect message. The Cause element in the Disconnect message can indicate why CLID authentication failed. You can set two parameters that affect Disconnect messages:

– The CLID Timeout Busy parameter specifies whether to return User Busy when CLID authentication fails due to a RADIUS timeout. You can specify Yes or No. The default value is No, which indicates Normal Call Clearing.

– The CLID Fail Busy parameter specifies whether to return User Busy when CLID authentication fails for reasons other than a RADIUS timeout. You can specify Yes or No. The default value is No, which indicates Normal Call Clearing.

General guidelines

Before you set up CLID authentication, keep these limitations in mind:

- In some installations, the WAN provider might not be able to deliver CLIDs, or a caller might choose to keep a CLID private.
- CLID authentication applies only where CLID is available end-to-end and Automatic Number Identification (ANI) applies to the call.
- T1 access lines and Switched-56 lines do not support CLID.
- When a user dials into the MAX using MP or MP+, the calling device may have more than phone number associated with it.

  In these types of cases, the CLID is the phone number associated with the channel in use.

Scenario 1: Authentication using name, password, and caller ID

To set up CLID authentication in this scenario, use the attributes listed in Table 3-19.

Table 3-19.CLID authentication attributes: Scenario 1

Attribute	**Possible values**
Caller-Id (31)	A telephone number containing up to 37 characters, limited to the following: **1234567890()[]!z-*#|** The default value is null. In this instance, specify Caller-Id on the first line of the user profile.
User-Name (1)	Text string containing up to 252 characters. The default value is null.
Password (2)	Text string containing up to 252 characters. The default value is null.

Although you can configure local Connection profiles to authenticate using name, password, and caller ID, we recommend that you perform this function in RADIUS. To require all callers to authenticate using name, password and caller ID, follow these steps:

1. If you have not done so already, set Id Auth=Prefer in the Ethernet > Answer menu on the MAX.
2. Ensure that the first line of all dial-in RADIUS user profiles has the following format:

   ```
   username Password="password", Caller-Id="phonenum"
   ```

   - `username` is the user name.
   - `password` is the user's password.
   - `phonenum` is the caller ID.

Example using name, password, and caller ID

Here is an example user profile for authentication using name, password, and caller ID:

```
Emma  Password="test", Caller-Id="123456789"
      User-Service=Framed-User,
      Framed-Protocol=PPP,
      Framed-Address=255.255.255.254,
      Framed-Netmask=255.255.255.255,
      Ascend-Assign-IP-Pool=1,
      Ascend-Route-IP=Route-IP-Yes,
      Ascend-Idle-Limit=30
```

Scenario 2: Authentication using a caller ID only

To set up CLID authentication in this scenario, use the attributes listed in Table 3-20.

Table 3-20.CLID authentication attributes: Scenario 2

Attribute	Possible values
Ascend-Require-Auth (201)	Not-Require-Auth (0) Require-Auth (1) In this instance, specify Not-Require-Auth (the default).
User-Name (1)	Text string containing up to 252 characters. The default value is null. In this instance, the user name is the calling party's phone number.
Password (2)	Text string containing up to 252 characters. The default value is null. In this instance, the password is Ascend-CLID.

Although you can configure local Connection profiles to authenticate using a caller ID only, we recommend that you perform this function in RADIUS. To require all callers to authenticate using a caller ID only, follow these steps:

1 If you have not done so already, set Id Auth=Require or Id Auth=Fallback in the Ethernet > Answer menu on the MAX.

2 Verify that the first line of all dial-in RADIUS user profiles has the following format:

phonenum **Password="Ascend-CLID"**

- ***phonenum*** represents the calling party's phone number.
- The Password value specifies that RADIUS authenticates the caller by caller ID only.

3 Set the Ascend-Require-Auth attribute to Not-Require-Auth.

This setting specifies that after CLID authentication, the MAX does not require any additional authentication. If you want to include name and password authentication in addition to CLID authentication, see "Scenario 1: Authentication using name, password, and caller ID" on page 3-35 or "Scenario 3: External authentication after CLID authentication" on page 3-38.

Example using a caller ID only

Here is an example user profile for authentication using a caller ID only:

```
5551212  Password="Ascend-CLID"
         Ascend-Require-Auth=Not-Require-Auth,
         User-Service=Framed-User,
         Framed-Protocol=PPP,
         Framed-Address=255.255.255.254,
         Framed-Netmask=255.255.255.255,
         Ascend-Assign-IP-Pool=1,
         Ascend-Route-IP=Route-IP-Yes,
         Ascend-Idle-Limit=30
```

Scenario 3: External authentication after CLID authentication

This scenario entails using an external authentication server, such as a token-card server, to authenticate callers after CLID authentication. All users must pass caller-ID authentication and token-card authentication. The configuration uses a two-tiered setup.

To set up this two-tiered authentication, use the attributes listed in Table 3-21.

Table 3-21.CLID authentication attributes: Scenario 3

Attribute	Possible values
Ascend-Require-Auth (201)	Not-Require-Auth (0) Require-Auth (1) The default value is Not-Require-Auth. In this instance, specify Require-Auth in the first tier.
User-Name (1)	Text string containing up to 252 characters. The default value is null. In the first tier, the user name is the calling party's phone number. In the second tier, the user name is Default.
Password (2)	Text string containing up to 252 characters. The default value is null. In this instance, the password is Ascend-CLID in the first tier.

To perform external authentication after CLID authentication, follow these steps:

1 If you have not done so already, set Id Auth=Require in the Ethernet > Answer menu on the MAX.

2 Configure the first tier of a two-tiered dial-in setup.

The first-tier dial-in user profile has the following two-line format:

```
phonenum Password="Ascend-CLID"
       Ascend-Require-Auth=Require-Auth
```

– *phonenum* represents the calling party's phone number.

– The Password setting specifies that RADIUS authenticates the caller by caller ID.

– The Ascend-Require-Auth setting specifies that after CLID authentication, the MAX requires additional authentication.

When you set Ascend-Require-Auth=Require-Auth, you should not include any other attributes in the user profile. You must specify the characteristics of the call in the second-tier user profile.

3 Configure the second tier of the two-tiered dial-in setup.

The second-tier user profile has the following format for the first line, with the characteristics of the call specified by the second and succeeding lines:

Default Password="SAFEWORD"

Example using token-card server after CLID authentication

Here is an example of two-tiered user profile entries:

```
5551212   Password="Ascend-CLID"
          Ascend-Require-Auth=Require-Auth
Default   Password="SAFEWORD"
          User-Service=Login-User,
          Login-Host=10.0.4.1,
          ...
```

The first pass checks the caller ID. The second pass checks the name and password through the token-card server. If the caller passes both authentications, the MAX grants access. The Default user profile specifies the characteristics of the call.

Scenario 4: PAP, CHAP, or MS-CHAP after CLID authentication

Following CLID authentication, you can indicate whether the MAX should request Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), or Microsoft CHAP (MS-CHAP) authentication for incoming calls on a PPP or MP+ connection. You specify PAP, CHAP, or MS-CHAP authentication using a two-tiered method with the attributes listed in Table 3-22.

Table 3-22.Attributes for PAP, CHAP, or MS-CHAP after CLID authentication

Attribute	Possible values
Ascend-Require-Auth (201)	Not-Require-Auth (0) Require-Auth (1) The default is Not-Require-Auth. In this instance, specify Require-Auth in the first-tier user profile—the one that sets up CLID authentication.
Caller-Id (31)	A telephone number containing up to 37 characters, limited to the following: **1234567890()[]!z-*#|** The default value is null. In the second-tier profile, specify the same value for Caller-Id as you specified for User-Name in the first-tier profile.

Table 3-22.Attributes for PAP, CHAP, or MS-CHAP after CLID authentication (continued)

Attribute	Possible values
Framed-Protocol (7)	PPP (1) SLIP (2) MPP (256) EURAW (257) EUUI (258) COMB (260) FR (261) ARA (262) FR-CIR (263) By default, the MAX does not restrict the type of protocol a user can access. In this instance, specify PPP in the second-tier profile.
User-Name (1)	Text string containing up to 252 characters. The default value is null. In the first tier, the user name is the calling party's phone number. In the second tier, the user name is the one associated with the user being authenticated.
User-Service (6)	Login-User (1) Framed-User (2) Dialout-Framed-User (5) By default, the MAX does not restrict user access to services. Specify Framed-User in the second-tier profile.
Password (2)	Text string containing up to 252 characters. The default value is null. Set the password to Ascend-CLID in the first tier and to the user's password in the second tier.

To request PAP, CHAP, or MS-CHAP authentication after CLID authentication, you must set up two RADIUS user profiles. Follow these steps:

1 If you have not done so already, set Recv Auth to PAP, CHAP, MS-CHAP, or Either in the Ethernet > Answer > PPP Options menu.

2 In RADIUS, set up a first-tier profile specifying CLID authentication.

– Set the User-Name attribute to the calling party's phone number.

– Set the Password attribute to Ascend-CLID.

– Set the Ascend-Require-Auth attribute to Require-Auth. Calls that have been CLID authenticated undergo no further authentication unless the matching RADIUS profile 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.

For example, the first-tier CLID authentication profile might look like this one:

```
5551212   Password="Ascend-CLID"
          Ascend-Require-Auth=Require-Auth
```

Do not include any other attributes in this profile. You must specify the characteristics of the call in the second-tier user profile.

3 In the first line of the second-tier user profile, specify these attributes:

- user name
- Password
- Caller-Id. The value you specify for the Caller-Id attribute must match the phone number you specified for User-Name in the first-tier user profile.

4 On any succeeding lines of the second-tier user profile, set these attributes:

- User-Service=Framed-User
- Framed-Protocol=PPP

5 Specify any additional attributes in the second-tier user profile.

The characteristics of the call appear in this user profile.

Example using CHAP after CLID authentication

This example shows a two-tiered approach. The first user profile specifies CLID authentication, and indicates that additional CHAP authentication will follow. The second user profile sets up other attributes for the call.

```
5551212   Password="Ascend-CLID"
          Ascend-Require-Auth=Require-Auth
Emma   Password="pwd", Caller-Id="5551212"
       User-Service=Framed-User,
       Framed-Protocol=PPP,
       Framed-Address=200.11.12.10,
       Framed-Netmask=255.255.255.248,
       Ascend-Send-Secret="pwd",
       ...
```

Setting up called-number authentication

Called-number authentication works much like CLID authentication, except that the MAX uses the number called by the remote end to authenticate the connection. The called number appears in an ISDN message as part of the call when Dialed Number Information Service (DNIS) is in use. Called-number authentication is also known as DNIS authentication.

This section describes how to set up a RADIUS user profile for called-number authentication. You can choose from these configurations:

- Authenticate all callers using name, password, and the called number. For details, see "Scenario 1: Authentication using name, password, and called number" on page 3-44.
- Authenticate all callers using the called number only. For details, see "Scenario 2: Authentication using the called number only" on page 3-45.
- Use an external authentication server, such as a token-card authentication server, to authenticate users after called-number authentication. For details, see "Scenario 3: External authentication after called-number authentication" on page 3-46.

Before you begin

Before you set up called-number authentication in RADIUS, you must follow these steps using the MAX configuration interface:

1 Open the Ethernet menu.

2 Open the Answer menu.

3 If you want to authenticate callers by name, password, and called number, set Id Auth=Called Prefer.

This setting specifies that whenever the called number is available, the MAX checks the called number against the value of the Client-Port-DNIS attribute in a RADIUS user profile. If it finds a match, and the profile does not require any further authentication, the MAX accepts the call. If the called number is not available, or if the MAX cannot find a match to the called number, the MAX applies authentication using the Recv Auth parameter in the PPP Options menu.

4 If you want to authenticate callers by called number only, set Id Auth=Called Require

This setting indicates that the called number must match the value of the Client-Port-DNIS attribute before the MAX can answer the call. If the called number is not available, the MAX does not answer the call.

Configuring DNIS numbers in RADIUS

This feature addresses those locations in North America that charge significantly higher rates for digital bearer service than voice bearer service. In addition, this feature can be used by larger ISPs that resell services to smaller ISPs, identifying them by DNIS number. To configure DNIS numbers in RADIUS, follow these steps:

1 Create the first line of a pseudo-user entry using the User-Name and Password attributes.

You create a pseudo-user to store information that the Ascend unit can query—in this case, in order to store DNIS numbers. You can configure pseudo-users for both global and Ascend unit-specific configuration control of DNIS numbers The Ascend unit adds the unit-specific information in addition to the global information.

For a unit-specific DNIS configuration, specify the first line of a pseudo-user entry in this format:

```
dovbs-<unit_name>-<num> Password="ascend"
```

For a global DNIS configuration, specify the first line of a pseudo-user entry in this format:

```
dovbs-<num> Password="ascend"
```

<unit_name> is the system name of the Ascend unit—that is, the name specified by the Name parameter in the System Profile. <num> is a number in a sequential series, starting at 1.

2. For each pseudo-user entry, specify one or more DNIS numbers using the Client-Port-DNIS attribute.

   Specify each DNIS number in this format:

   Client-Port-DNIS="<DNIS number>"

   Client-Port-DNIS specifies the called-party number, indicating the phone number dialed by the user to connect to the Ascend unit. You can specify up to 100 DNIS numbers; if you specify more than 100, the remaining numbers are ignored.

Consider this example:

Five small ISPs connect to a larger ISP using DOVBS with the following numbers:

- 4165551111
- 4165552222
- 4165553333
- 4165554444
- 4165555555

The pseudo-user profile for an Ascend unit named "Toronto" looks like this one:

```
dovbs-Toronto-1 Password = "ascend"
Client-Port-DNIS = "5105551111"
    Client-Port-DNIS = "5105552222"
    Client-Port-DNIS = "5105553333"
    Client-Port-DNIS = "5105554444"
    Client-Port-DNIS = "5105555555"
```

How the Ascend unit learns about DNIS entries

When you have properly configured the pseudo-user profile, RADIUS loads DNIS numbers whenever you power on or reset the Ascend unit, when you select the Upd Rem Cfg command from the Sys Diag menu, or when you use an update command in SNMP. RADIUS loads the numbers in this way:

1. RADIUS looks for entries having the format dovbs-<unit_name>-1, where <unit_name> is the system name.
2. If at least one entry exists, RADIUS loads all existing entries with the format dovbs-<unit_name>-<num>.

   The variable <num> is a number in a sequential series, starting with 1.

3. The Ascend unit queries dovbs-<unit_name>-1, then dovbs-<unit_name>-2, and so on, until it receives an authentication reject from RADIUS.
4. Once the host-specific numbers are loaded, RADIUS loads the global configuration entries; these configurations have the format dovbs-<num>.
5. The Ascend unit queries dovbs-1, then dovbs-2, and so on, until it receives an authentication reject from RADIUS.

   The Ascend unit checks the DNIS number of each incoming call against the phone numbers it has loaded.

Scenario 1: Authentication using name, password, and called number

To set up called-number authentication in this scenario, use the attributes listed in Table 3-23.

Table 3-23.Called-number authentication attributes: Scenario 1

Attribute	Possible values
Client-Port-DNIS	A telephone number containing up to 18 characters, limited to the following: **1234567890()[]!z-*#|** The default value is null. In this instance, specify Client-Port-DNIS on the first line of the user profile.
User-Name (1)	Text string containing up to 252 characters. The default value is null.
Password (2)	Text string containing up to 252 characters. The default value is null.

Although you can configure local Connection profiles to authenticate using a name, password, and called number, we recommend that you perform this function in RADIUS. To require all callers to authenticate using name, password and called number, follow these steps:

1. If you have not done so already, set Id Auth=Called Prefer in the Ethernet > Answer menu on the MAX.
2. Ensure that the first line of all dial-in RADIUS user profiles has the following format:

   ```
   username Password="password", Client-Port-DNIS="phonenum"
   ```

   – *username* is the user name.

   – *password* is the user's password.

   – *phonenum* is the called number.

Example using name, password, and called number

Here is an example user profile for authentication using name, password, and called number:

```
Emma  Password="test", Client-Port-DNIS="123456789"
      User-Service=Framed-User,
```

```
Framed-Protocol=PPP,
Framed-Address=255.255.255.254,
Framed-Netmask=255.255.255.255,
Ascend-Assign-IP-Pool=1,
Ascend-Route-IP=Route-IP-Yes,
Ascend-Idle-Limit=30
```

Scenario 2: Authentication using the called number only

To set up called-number authentication in this scenario, use the attributes listed in Table 3-24.

Table 3-24.Called-number authentication attributes: Scenario 2

Attribute	Possible values
Ascend-Require-Auth (201)	Not-Require-Auth (0) Require-Auth (1) In this instance, specify Not-Require-Auth (the default).
User-Name (1)	Text string containing up to 252 characters. The default value is null. In this instance, the user name is the called number.
Password (2)	Text string containing up to 252 characters. The default value is null. In this instance, the password is Ascend-DNIS.

Although you can configure local Connection profiles to authenticate using the called number only, we recommend that you perform this function in RADIUS. To require all callers to authenticate using the called number only, follow these steps:

1 If you have not done so already, set Id Auth=Called Require in the Ethernet > Answer menu on the MAX.

2 Verify that the first line of all dial-in RADIUS user profiles has the following format:

`phonenum` **`Password="Ascend-DNIS"`**

- *`phonenum`* represents the called number.
- The Password value specifies that RADIUS authenticates the caller by called number only.

3 Set the Ascend-Require-Auth attribute to Not-Require-Auth.

This setting specifies that after called-number authentication, the MAX does not require any additional authentication. If you want to include name and password authentication in addition to called-number authentication, see “Scenario 1: Authentication using name, password, and called number” on page 3-44 or “Scenario 3: External authentication after called-number authentication” on page 3-46.

Example using the called number only

Here is an example user profile for authentication using the called number only:

```
5551212  Password="Ascend-DNIS"
         Ascend-Require-Auth=Not-Require-Auth,
         User-Service=Framed-User,
         Framed-Protocol=PPP,
         Framed-Address=255.255.255.254,
         Framed-Netmask=255.255.255.255,
         Ascend-Assign-IP-Pool=1,
         Ascend-Route-IP=Route-IP-Yes,
         Ascend-Idle-Limit=30
```

Scenario 3: External authentication after called-number authentication

This scenario entails using an external authentication server, such as a token-card server, to authenticate callers after called-number authentication. All users must pass called-number authentication and token-card authentication. The configuration uses a two-tiered setup.

To set up this two-tiered authentication, use the attributes listed in Table 3-25.

Table 3-25.Called-number authentication attributes: Scenario 3

Attribute	Possible values
Ascend-Require-Auth (201)	Not-Require-Auth (0) Require-Auth (1) The default value is Not-Require-Auth. In this instance, specify Require-Auth in the first tier.
User-Name (1)	Text string containing up to 252 characters. The default value is null. In the first tier, the user name is the called number. In the second tier, the user name is Default.
Password (2)	Text string containing up to 252 characters. The default value is null. In this instance, the password is Ascend-DNIS in the first tier.

To perform external authentication after called-number authentication, follow these steps:

1 If you have not done so already, set Id Auth=Called Require in the Ethernet > Answer menu on the MAX.

2 Configure the first tier of a two-tiered dial-in setup.

The first-tier dial-in user profile has the following two-line format:

```
phonenum Password="Ascend-DNIS"
         Ascend-Require-Auth=Require-Auth
```

- ***phonenum*** represents the called number.
- The Password setting specifies that RADIUS authenticates the caller by called number.
- The Ascend-Require-Auth setting specifies that after called-number authentication, the MAX requires additional authentication. When you set Ascend-Require-Auth=Require-Auth, you should not include any other attributes in the user profile. You must specify the characteristics of the call in the second-tier user profile.

3 Configure the second tier of the two-tiered dial-in setup.

The second-tier user profile has the following format for the first line, with the characteristics of the call specified by the second and succeeding lines:

Default Password="SAFEWORD"

Example using token server after called-number authentication

Here is an example of two-tiered user profile entries:

```
5551212   Password="Ascend-DNIS"
          Ascend-Require-Auth=Require-Auth
Default   Password="SAFEWORD"
          User-Service=Login-User,
          Login-Host=10.0.4.1,
          ...
```

The first pass checks the called number. The second pass checks the name and password through the token-card server. If the caller passes both authentications, the MAX grants access. The Default user profile specifies the characteristics of the call.

Putting it all together

This section discusses different ways in which users can dial into the MAX, and the kinds of authentication you can set up.

Analog dial-in with terminal server authentication

If a customer is dialing in over an analog line and will undergo terminal server authentication, you can must carry out these tasks:

1 Set the User-Service attribute in the customer's RADIUS user profile.

If the user will make use of the terminal server interface and then use PPP, set User-Service=Login-User. If the user will bypass the terminal server interface and use PPP, set User-Service=Framed-User.

2 If User-Service=Login-User, set PPP=Yes in the Ethernet > Mod Config > TServ Options menu.

3. If User-Service=Login-User, make sure that your customer’s PPP software has an expect-send script in this format:

   ```
   expect "Login:"
   send $username
   expect "Password:"
   send $password:
   ```

   At the end of the script, the user starts sending PPP packets.

For analog dial-in, these events take place:

1. The client calls with an analog modem, and the MAX answers.
2. The MAX waits for PPP packets, while the client software expects the terminal server login prompt.
3. The MAX times out on PPP, and sends the login prompt.
4. The client software sees the login prompt, enters a user name, and waits, expecting the password prompt.
5. The MAX sends the password prompt, and the client sends a password.
6. The MAX authenticates the user name and password against a RADIUS profile or local Connection profile.
7. If User-Service=Framed-User in the RADIUS user profile, the MAX does not present the `ascend%` prompt, but sends PPP packets.
8. If User-Service=Login-User in the RADIUS user profile, the MAX presents the `ascend%` prompt and then sends PPP packets.
9. The client software and the MAX communicate using PPP over the asynchronous serial analog line.

Digital dial-in using terminal server authentication

If a customer is dialing in using an ISDN terminal adapter (TA) and will undergo terminal server authentication, you must carry out these tasks:

1. Set the User-Service attribute in the customer’s RADIUS user profile.

   If the user will make use of the terminal server interface and then use PPP, set User-Service=Login-User. If the user will bypass the terminal server interface and use PPP, set User-Service=Framed-User.
2. If User-Service=Login-User, set PPP=Yes in the Ethernet > Mod Config > TServ Options menu.
3. In the Answer profile, set V.120=Yes.
4. Make sure that your customer’s TA is configured for V.120 encapsulation.

   You can set most TAs in automatic mode so that the TA looks for a PPP packet from the host. If it finds one, it starts PPP negotiations. If it does not find one, it tries V.120 authentication. Once the call connects, the TA uses asynch/PPP mode for the duration of the call.

For digital dial-in, these events take place:

1. The client calls using an ISDN TA and the MAX answers the call.
2. The MAX waits for PPP packets, while the client software expects the terminal server login prompt.

3 The MAX times out on PPP, and sends the login prompt.

4 The client software sees the login prompt, enters a user name, and waits, expecting the password prompt.

5 The MAX sends the password prompt, and the client sends a password.

6 The MAX authenticates the user name and password against a RADIUS profile or local Connection profile.

7 If User-Service=Framed-User in the RADIUS user profile, the MAX does not present the `ascend%` prompt, but sends PPP packets.

8 If User-Service=Login-User in the RADIUS user profile, the MAX presents the `ascend%` prompt and then sends PPP packets.

9 The client software and the MAX communicate using PPP over an asynchronous line—asynchronous from the workstation to the TA, and asynchronous over V.120 from the TA to the MAX.

In this scenario, you cannot use two channels because the MAX tries to authenticate the second channel using the user name presented at the terminal server login prompt. The client software does not run an expect-send script over V.120 and the second channel, so the second channel cannot connect. Without this connection, MP or MP+ fails.

Most ISDN TAs support either V.120 clear text or asynchronous–to–PPP conversion, but not both. Therefore, if you log into a PPP server in terminal and/or scripted (ASCII text) mode, the TA goes into V.120 mode and should not dial the second B channel. If for some reason the TA does dial the second channel, it will fail to bind the two channels together and will probably drop the first channel.

In order to get the second channel connected, you must use the Authentication area, fill out the `Auth. ID:` field and the `Password:` field, and choose the appropriate authentication method, usually PAP or CHAP. If you want a second channel, you cannot use a script or the terminal.

PPP login with PAP, CHAP, or MS-CHAP authentication

These types of equipment allow a customer to communicate via PPP using PAP, CHAP, or MS-CHAP authentication:

- Analog modems with no expect-send script.

  The customer’s PPP software must support PAP, CHAP, or MS-CHAP. The software must start negotiating PPP once it registers that the modems have connected.

- ISDN TAs using asynchronous-to-synchronous conversion.

  In this scenario, the connection between the client and the TA is asynchronous, and the ISDN connection between the TA and the MAX is synchronous. You must ensure that the customer’s TA is configured for asynchronous-to-synchronous conversion. You do not need V.120 support for clients using ISDN TAs with PAP, CHAP, or MS-CHAP authentication.

- True ISDN routers, such as the Pipeline 50.

These events take place:

1 The client calls and the MAX answers.

2. The MAX waits for PPP packets, based on the RADIUS user profile or a local Connection profile.
3. The client sends PPP packets.
4. The MAX responds with PPP, and LCP negotiation starts.
5. The MAX carries out PAP, CHAP, or MS-CHAP authentication.
6. After authentication, upper layer NCPs (IPCP, IPXCP, CCP) are negotiated.
7. The client device and the MAX communicate using PPP over the ISDN line.

Setting Up WAN Connections in RADIUS

4

This chapter describes how to configure a RADIUS user profile for different types of WAN connections. This chapter contains:

This chapter does not discuss how to set up a frame relay connection. For details on this task, see Chapter 5, “Setting Up Frame Relay in RADIUS.”

Limiting access to services and protocols

To limit the services and protocols that a link can use, you must specify a value for each of the attributes listed in Table 4-1 (except Ascend-Force-56). If you do not specify a value, the MAX does not restrict the services and protocols the link can use.

Table 4-1. Limiting services and protocols

Attribute	Description	Possible values
Ascend-Data-Svc (247)	Specifies the type of data service the link uses for outgoing calls.	For a full list of possible values, see “Ascend-Data-Svc (247)” on page 9-29. The default value is Switched-56K.
Ascend-Force-56 (248)	Indicates whether the MAX uses only the 56-kbps portion of a channel, even when all 64 kbps appear to be available.	Force-56-No (0) Force-56-Yes (1) The default value is Force-56-No.
Framed-Protocol (7)	Specifies the type of protocol the link can use.	PPP (1) SLIP (2) MPP (256) EURAW (257) EUUI (258) COMB (260) FR (261) ARA (262) FR-CIR (263) By default, the MAX does not restrict the type of protocol a link can use.
NAS-Port-Type (61)	Specifies the type of physical port the MAX is using to authenticate the client.	Async Sync ISDN-Sync ISDN-Async-v120 ISDN-Async-v110 Virtual The default value is Async.
Password (2)	Specifies the user’s password.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Name (1)	Specifies the user’s name.	Alphanumeric string containing up to 252 characters. The default value is null.

Table 4-1. Limiting services and protocols (continued)

Attribute	Description	Possible values
User-Service (6)	Indicates whether the link can use framed or unframed services.	Login-User (1) Framed-User (2) Dialout-Framed-User (5) By default, the MAX does not restrict the services that a link can use.

To limit access to services and protocols for a connection, follow these steps:

1 On the first line of the profile, specify the User-Name and Password attributes.

2 To limit the types of services a link can use, set the User-Service attribute on the first line of the profile.

You can specify one of these values:

– Login-User (1): The operator can use an asynchronous Telnet connection to log into the terminal server. The MAX rejects incoming framed calls. The operator cannot use any framed protocol, but can start Telnet or raw TCP sessions.

– Framed-User (2): Incoming calls must use a framed protocol. Otherwise, the MAX rejects them. Asynchronous Telnet sessions are unframed and therefore not allowed when you specify this value.

– Dialout-Framed-User (5): The MAX can use this profile for outgoing calls only. The MAX sends this value to the RADIUS server during an authentication request.

If RADIUS authenticates an incoming call using the User-Name and Password attributes, and the type of call matches the value of the User-Service attribute, the MAX applies the attributes specified in the user profile 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 the User-Service attribute, the MAX does not limit the services the link can access.

For more information on using the User-Service attribute, see “Putting it all together” on page 3-47.

3 To specify the type of framed protocol the link can use, set the Framed-Protocol attribute.

When you set this attribute, the MAX does not allow any other type of framed protocol.

Table 4-2 lists the values you can specify for Framed-Protocol.

Table 4-2. Framed-Protocol settings

Setting	Incoming call	Outgoing call
PPP (1)	A user requesting access can dial in using Multilink Protocol Plus (MP+), Multilink Protocol (MP), or Point-to-Point Protocol (PPP) framing. A user requesting access can also dial in unframed, and then change to PPP framing. If the user dials in using any other type of framing, the MAX rejects the call.	Outgoing calls use PPP framing.
SLIP (2)	A user requesting access can dial in unframed and change to SLIP framing. SLIP requires that a user dial in without using a framed protocol before changing to SLIP.	This value does not apply to outgoing calls.
MPP (256)	This value does not apply to incoming calls.	Outgoing calls request MP+ framing.
EURAW (257)	A user requesting access can dial in using EU-RAW framing. EU-RAW is a type of X.75 encapsulation in which IP packets are HDLC encapsulated with a CRC field. If the user dials in using any other type of framing, the MAX rejects the call.	Outgoing calls use EU-RAW framing.
EUUI (258)	A user requesting access can dial in using EU-UI framing. EU-UI is a type of X.75 encapsulation in which IP packets are HDLC encapsulated with a CRC field and a small header. If the user dials in using any other type of framing, the MAX rejects the call.	Outgoing calls use EU-UI framing.
COMB (260)	A user requesting access can dial in using Combinet framing. If the user dials in using any other type of framing, the MAX rejects the call.	Outgoing calls use Combinet framing.
FR (261)	This value does not apply to incoming calls.	Outgoing calls use frame relay (RFC 1490) framing.

Table 4-2. Framed-Protocol settings (continued)

Setting	**Incoming call**	**Outgoing call**
ARA (262)	A dial-in user can establish an AppleTalk Remote Access (ARA) connection to the Ethernet network. ARA is an asynchronous protocol. It supports V.120, X.75, and modem calls only. It does not support V.110 calls or synchronous connections.	This value does not apply to outgoing calls.
FR-CIR (263)	The call consists of a frame relay circuit.	The call consists of a frame relay circuit.

What Framed-Protocol does depends on how you set User-Service:

– If User-Service=Framed-User or is unspecified, a user requesting access can dial in using the framing specified by Framed-Protocol.

– The MAX rejects other types of framing.

– A user requesting access can also dial in without using a framed protocol, but can then change to the framing specified by the Framed-Protocol attribute.

– If 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 the MAX allows on the outgoing call.

4 To specify the type of data service the link uses for outgoing calls, set the Ascend-Data-Svc attribute.

5 To restrict users to an ISDN or modem connection, set the NAS-Port-Type attribute.

This attribute indicates the type of physical port the MAX is using to authenticate the client. Some ISPs offer different levels of service based on connection type. To prevent a client from using a capability to which he or she has not subscribed, set the NAS-Port-Type attribute to an appropriate value. You can specify one of these settings:

– Async indicates a call routed to a digital modem.

– Sync indicates a non-ISDN synchronous connection, such as a Switched-56K connection.

– ISDN-Sync indicates a synchronous ISDN connection.

– ISDN-Async-v120 indicates an ISDN connection using V.120 asynchronous rate adaptation.

– ISDN-Async-v110 indicates an ISDN connection using V.110 asynchronous rate adaptation.

– Virtual indicates a connection to the MAX using a transport protocol instead of a physical port.

6 Set the Ascend-Force-56 attribute.

This attribute specifies whether the MAX uses only the 56-kbps portion of a channel, even when all 64 kbps appear to be available:

- To use only the 56-kbps portion, set Ascend-Force-56=Force-56-Yes.
- To use the entire 64 kbps (when available), set Ascend-Force-56=Force-56-No.

  The default value is Force-56-No.

Use this feature when you place calls to European or Pacific Rim countries from within North America and the complete path cannot distinguish between the Switched-56 and Switched-64 data services. This feature is not required if you are placing calls only within North America.

Service access example

The dial-in user in this example can use only PPP protocols (PPP, MP+, or MP) and cannot use the terminal server.

```
Ascend Password="Pipeline", User-Service=Framed-User
       Framed-Protocol=PPP,
       Framed-Address=200.250.55.9,
       Framed-Netmask=255.255.255.248,
       Ascend-Link-Compression=Link-Comp-Stac,
       Framed-Compression=Van-Jacobson-TCP-IP,
       Ascend-Route-IP=Route-IP-Yes,
       Ascend-Metric=2
```

Restricting users to specific lines and channels

To restrict the lines and channels that a user can access, set the NAS-Port attribute, as described in Table 4-3.

Table 4-3.NAS-Port attribute

Attribute	Description	Possible settings
NAS-Port (5)	Specifies the network port on which the MAX receives a call.	A bit-encoded, zero-based number in this format: *`FF SSSS LLLLL CCCCC`* to specify the slot, line, and channel to which the dial-in user is restricted. This is the format the MAX TNT recognizes. You can also use the format *`tllcc`* specifying whether the call is digital or analog, and giving the line number and channel number. The default value for the RADIUS daemon appears in the /etc/services/file.

To restrict users to specific lines and channels, make these settings *on the first line of the user profile*:

1 Set the New NASPort ID parameter in the System > Sys Config menu on the MAX.

You can choose one of two settings:

- Yes restricts a dial-in user to a shelf, slot, line, and channel number. This format is the one recognized by the MAX TNT.
- No specifies that the MAX recognizes the five-digit format that specifies the type of service in use, the line number, and the channel number. No is the default.

2 Specify the User-Name and Password attributes.

3 Specify the NAS-Port attribute by doing one of the following:

To restrict the dial-in ISDN user to a shelf, slot, line, and channel number. This is the format the MAX TNT recognizes:

`FF SSSS LLLLL CCCCC`

- ***`FF`*** specifies the shelf number (always 0 in RADIUS, 1 on the MAX)
- ***`SSSS`*** specifies the slot number (0–15)
- ***`LLLLL`*** specifies the line number (0–31)
- ***`CCCCC`*** specifies the channel number (0–31)

For an analog call, the values are the same, except that the line number can be 0-63, and the channel number is always 1.

Because the value you enter is zero-based, you must add 1 to each component to ascertain the actual slot, line, and channel number. The RADIUS daemon converts the NAS-Port number to decimal on most systems.

You can also restrict the dial-in user to a service, line, and channel.

`tlcc`

where

- ***`t`***=digital call or analog call
- ***`ll`***=line number
- ***`cc`***=channel number

Line and channel example

To restrict a dial-in user to analog service on line 1, set up a user profile like this one:

```
Dave Password="password", NAS-Port=20100
      User-Name="Dave",
      User-Service=Framed-User,
      Framed-Protocol=PPP,
      Ascend-Assign-IP-Pool=1,
      Ascend-Route-IP=1,
      Ascend-Idle-Limit=300,
      Framed-Routing=None
```

Setting up a PPP connection

Point-to-Point Protocol (PPP) enables you to set up a single-channel connection to any other device running PPP. A PPP connection can support IP routing, IPX routing, protocol-independent bridging, and password authentication using PAP, CHAP, or MS-CHAP.

A PPP connection is usually a bridged or routed network connection initiated in PPP dialup software. Figure 4-1 shows the MAX with a PPP connection to a remote user running Windows 95 with the TCP/IP stack and PPP dialup software.

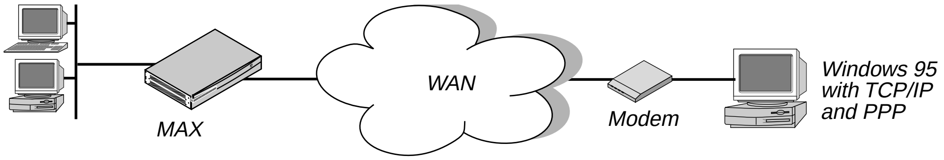

Figure 4-1. A PPP connection

Before you begin

Before configuring the RADIUS user profile for a PPP connection, you must perform the following tasks:

1 Work with the caller to find out what software and modem device exists at the remote end.

2 Determine the appropriate routing, authentication, and compression settings.

3 For the MAX to use the Answer profile as the default when answering a call, set Use Answer as Default=Yes in the Ethernet > Answer menu.

If you accept the default setting of No, the MAX uses the factory defaults.

4 In the Ethernet > Answer > PPP Options menu, set Recv Auth=PAP, CHAP, MS-CHAP, or Either.

If the incoming PPP call does not include a source IP address, the MAX requires PAP, CHAP, or MS-CHAP authentication.

5 To enable PPP encapsulation, set PPP=Yes in the Ethernet > Answer > Encaps menu.

6 Assign a name to the MAX in the System profile.

For information on the tasks specific to the MAX configuration interface, see the MAX *ISP and Telecommuting Configuration Guide*.

Configuring a PPP connection in RADIUS

To configure a PPP connection in RADIUS, use the attributes listed in Table 4-4.

Table 4-4. PPP attributes

Attribute	**Description**	**Possible values**
Ascend-Link-Compression (233)	Turns data compression on or off for a PPP link.	Link-Comp-None (0) Link-Comp-Stac(1) The default value is Link-Comp-None.
Ascend-PPP-Address (253)	Specifies the IP address of the MAX as reported to the calling unit during PPP IPCP negotiations.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0. When you accept this value, IPCP negotiates using the value of the IP Adrs parameter in the Ethernet > Mod Config > Ether Options menu.
Ascend-PPP-Async-Map (212)	Gives the Ascend PPP code the async control character map for the PPP session.	4-byte bitmap to one or more control characters. The default is the standard async control character.

Table 4-4. PPP attributes (continued)

Attribute	Description	Possible values
Ascend-PPP-VJ-1172 (211)	Instructs the Ascend PPP code to use the 0x0037 value for the VJ compression type.	You can specify PPP-VJ-1172 to indicate 0x0037. If you do not specify this value, RADIUS uses the default—VJ compression type 0x002d.
Ascend-PPP-VJ-Slot-Comp (210)	Instructs the Ascend PPP code whether to use slot compression when sending VJ-compressed packets.	VJ-Slot-Comp-No (0) VJ-Slot-Comp-Yes (1) The default value is VJ-Slot-Comp-Yes.
Ascend-Send-Auth (231)	Specifies the authentication protocol that the MAX requests when initiating a connection using PPP or MP+ encapsulation. The answering side of the connection determines which authentication protocol, if any, the connection uses.	Send-Auth-None (0) Send-Auth-PAP (1) Send-Auth-CHAP (2) The default value is Send-Auth-None.
Ascend-Send-Passwd (232)	Specifies the password that the MAX sends to the remote end of a connection on outgoing calls.	Text string containing up to 20 characters. The default value is null.
Ascend-Send-Secret (214)	Specifies that the system encrypts the password when passing it between the RADIUS server and the MAX on outgoing calls.	Text string containing up to 20 characters. The default value is null.
Framed-Compression (13)	Turns on TCP/IP header compression.	You can specify Van-Jacobson-TCP-IP to turn on TCP/IP header compression. If you do not specify this value, RADIUS uses the default of no header compression.
Framed-MTU (12)	Specifies the maximum number of bytes the MAX can receive in a single packet on a PPP link.	Integer between 1 and 1524. The default value is 1524.

Table 4-4. PPP attributes (continued)

Attribute	**Description**	**Possible values**
Framed-Protocol (7)	Specifies the type of protocol the link can use.	PPP (1) SLIP (2) MPP (256) EURAW (257) EUUI (258) COMB (260) FR (261) ARA (262) FR-CIR (263) By default, the MAX does not restrict the type of protocol a link can use.
Password (2)	Specifies the user's password.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Name (1)	Specifies the user's name.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Service (6)	Indicates whether the link can use framed or unframed services.	Login-User (1) Framed-User (2) Dialout-Framed-User (5) By default, the MAX does not restrict the services that a link can use.

To configure a PPP connection in a RADIUS user profile, follow these steps:

1. On the first line of the profile, specify the User-Name and Password attributes, and set User-Service=Framed-User.
2. Set Framed-Protocol=PPP.
3. Set Ascend-Send-Auth=Send-Auth-PAP or Send-Auth-CHAP (outgoing calls only).

   The Ascend-Send-Auth attribute specifies the authentication protocol that the MAX requests when initiating a connection using PPP or MP+ encapsulation. The answering side of the connection determines which authentication protocol, if any, the connection uses. Both sides of the connection must support the specified protocol.

   You can set Ascend-Send-Auth to one of these values:

   – Send-Auth-None (0) specifies that the MAX does not request an authentication protocol for outgoing calls: This setting is the default.

   – Send-Auth-PAP (1) specifies that the MAX requests Password Authentication Protocol (PAP): PAP is a PPP authentication protocol that provides a simple method for the MAX to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment, and does not use encryption. The remote device must support PAP. If you choose this setting, the MAX requests PAP authentication, but uses CHAP authentication if the called unit requires CHAP. Choose this setting for non-token card authentication if you want to send your password unencrypted.

- Send-Auth-CHAP (2) specifies that the MAX requests Challenge Handshake Authentication Protocol (CHAP): CHAP is a PPP authentication protocol that is more secure than PAP. CHAP provides a way for the remote device to periodically verify the identity of the MAX using a three-way handshake and encryption. Authentication takes place upon initial link establishment. A device can repeat the authentication process any time after the connection is made. The remote device must support CHAP. If you choose this setting, the MAX does not bring up the connection using PAP. Choose this setting for non-token card authentication if you do not wish to send your password unencrypted—that is, if you do not wish to use PAP authentication.

4 If you request PAP or CHAP authentication, you must also specify a password using Ascend-Send-Secret or Ascend-Send-Passwd (outgoing calls only).

Both of these attributes specify the password that the MAX sends to the remote end of a connection on outgoing calls. If the value you specify for Ascend-Send-Secret or Ascend-Send-Password does not match the value of the remote end's Ascend-Receive-Secret attribute (in a RADIUS user profile) or the Recv PW parameter (in a Connection profile), the remote system rejects the call.

Use Ascend-Send-Passwd only if your version of the MAX does not support Ascend-Send-Secret.

5 To specify the MAX unit's IP address, set the Ascend-PPP-Address attribute.

If you do not specify a value for this attribute, or if you specify the value 0.0.0.0, IPCP negotiates using the value of the IP Adrs parameter in the Ethernet > Mod Config > Ether Options menu. If you specify a valid IP address, 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 the MAX unit's true IP address, as long as the user requesting access understands that limitation.

6 To specify the async control character map for the PPP session, set the Ascend-PPP-Async-Map attribute.

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 (zero). For example, bit 19 corresponds to Control-S (DC3) or ASCII 19. The control characters pass through the PPP link as data. Only applications running over the link can use these characters.

7 To specify the maximum number of bytes the MAX can receive in a single packet on a PPP link, set the Framed-MTU attribute.

The default value is 1524. You should accept this default unless the device at the remote end of the link cannot support it. If the administrator of the remote network specifies that you must change this value, specify a number between 1 and 1524.

8 To turn data compression on or off for a PPP link, set the Ascend-Link-Compression attribute.

- Link-Comp-None (0) turns off data compression: This value is the default.
- Link-Comp-Stac (1) turns on data compression: The MAX applies the STACKER LZS compression/decompression algorithm.

Both sides of the link must set either the Ascend-Link-Compression attribute (in RADIUS) or the Link Comp parameter (on the MAX) to turn on data compression.

9 To turn on TCP/IP header compression, set Framed-Compression=Van-Jacobson-TCP-IP.

This setting applies only to packets in TCP applications, such as Telnet, and turns on header compression for both sides of the link. Turning on header compression is most effective in reducing overhead when the data portion of the packet is small.

10 To instruct the Ascend PPP code *not to use slot compression* when sending VJ-compressed packets, set Ascend-PPP-VJ-Slot Comp=VJ-Slot-Comp-No.

When you set Framed-Compression=Van-Jacobson-TCP-IP, 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 associates it with the last-used slot ID. This scenario uses slot ID compression, because only the first packet in a stream uses slot compression.

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. This setting specifies that no slot compression take place. If you do not specify a value for Ascend-PPP-VJ-Slot-Comp and Framed-Compression=Van-Jacobson-TCP-IP, slot compression occurs.

11 To instruct the Ascend PPP code to use the 0x0037 value for the VJ compression type, set Ascend-PPP-VJ-1172=PPP-VJ-1172.

The MAX uses the value 0x0037 only during IPNCP negotiation. The MAX accepts incoming 1172 type options without your setting this attribute.

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.

12 Specify routing or bridging attributes for the connection.

For details on specifying that the connection use IP, see “Specifying IP routing and RIP behavior” on page 6-4.

For details on specifying that the connection use IPX, see “Specifying IPX routing” on page 6-26.

For details on specifying protocol-independent bridging, see “Specifying protocol-independent bridging” on page 6-34.

13 Configure the bridging or routing setup in the MAX for the WAN connection.

For details, see Chapter 6, “Setting Up Routing and Bridging Links” in this guide, and the relevant chapters of the MAX *ISP and Telecommuting Configuration Guide*.

PPP connection example

The following is a sample user profile showing a PPP link that requests link compression, TCP/IP header compression, and IP routing:

```
Emma Password="m2dan", User-Service=Framed-User
     Framed-Protocol=PPP,
     Framed-Address=200.250.55.9,
     Framed-Netmask=255.255.255.248,
     Ascend-Link-Compression=Link-Comp-Stac,
     Framed-Compression=Van-Jacobson-TCP-IP,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Metric=2
```

Setting up an MP or MP+ connection

Both Multilink Protocol (MP) and Multilink Protocol Plus (MP+) connections use PPP encapsulation over a multichannel link.

MP supports multichannel links, but not Dynamic Bandwidth Allocation (DBA). The base channel count determines the number of calls to place, and the number of channels does not change. In addition, MP requires that all channels in the connection share the same phone number—that is, the channels on the answering side of the connection must be in a hunt group.

MP+ enables the MAX to support DBA—to increase bandwidth as necessary and to drop bandwidth when a session no longer needs it. An MP+ connection can combine up to 30 channels into a single high-speed connection.

Figure 4-2 shows the MAX connected to a remote Pipeline 25 with an MP+ connection.

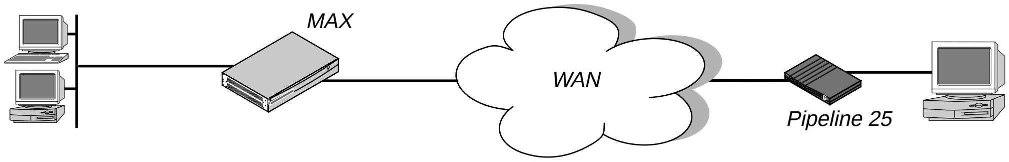

Figure 4-2. An MP+ connection

Other types of units may support MP but not MP+, so if you configure an MP+ connection in RADIUS between the MAX and a non-Ascend unit, the MAX first requests the MP+ protocol. If the remote end refuses MP+, the MAX uses MP instead. If the answering device refuses both MP+ and MP, the MAX sets up a PPP call on a single channel.

Before you begin

Before configuring the RADIUS user profile for an MP or MP+ connection, you must perform the following tasks:

1 Work with the caller to find out about the dial-up software and the Ascend configuration at the remote end.

2 Determine the appropriate routing, bridging, and authentication settings for the caller.

3 For the MAX to use the Answer profile as the default when answering a call, set Use Answer as Default=Yes in the Ethernet > Answer menu.

If you accept the default setting of No, the MAX uses the factory defaults.

4 In the Ethernet > Answer > PPP Options menu, set Recv Auth=PAP, CHAP, MS-CHAP, or Either.

If the incoming PPP call does not include a source IP address, the MAX requires PAP, CHAP, or MS-CHAP authentication.

5 To enable MP encapsulation, set MP=Yes in the Ethernet > Answer > Encaps menu.

6 To enable MP+ encapsulation, set MPP=Yes in the Ethernet > Answer > Encaps menu.

7 Assign a name to the MAX in the System profile.

For information on the tasks specific to the MAX configuration interface, see the MAX *ISP and Telecommuting Configuration Guide*.

Configuring an MP or MP+ connection in RADIUS

To configure an MP or MP+ connection in RADIUS, use the attributes listed in Table 4-5.

Table 4-5. MP and MP+ attributes

Attribute	**Description**	**Possible values**
Ascend-Send-Auth (231)	Specifies the authentication protocol that the MAX requests when initiating a connection using PPP or MP+ encapsulation. The answering side of the connection determines which authentication protocol, if any, the connection uses.	Send-Auth-None (0) Send-Auth-PAP (1) Send-Auth-CHAP (2) The default value is Send-Auth-None.
Ascend-Send-Passwd (232)	Specifies the password that the MAX sends to the remote end of a connection on outgoing calls.	Text string containing up to 20 characters. The default value is null.
Ascend-Send-Secret (214)	Specifies that the system encrypts the password when passing it between the RADIUS server and the MAX on outgoing calls.	Text string containing up to 20 characters. The default value is null.

Table 4-5. MP and MP+ attributes (continued)

Attribute	Description	Possible values
Framed-Compression (13)	Turns on TCP/IP header compression.	You can specify Van-Jacobson-TCP-IP to turn on TCP/IP header compression. If you do not specify this value, RADIUS uses the default of no header compression.
Framed-Protocol (7)	Specifies the type of protocol the link can use.	PPP (1) SLIP (2) MPP (256) EURAW (257) EUUI (258) COMB (260) FR (261) ARA (262) FR-CIR (263) By default, the MAX does not restrict the type of protocol a link can use.
Password (2)	Specifies the user's password.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Name (1)	Specifies the user's name.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Service (6)	Indicates whether the link can use framed or unframed services.	Login-User (1) Framed-User (2) Dialout-Framed-User (5) By default, the MAX does not restrict the services that a link can use.

To configure an MP or MP+ connection in a RADIUS user profile, follow these steps:

1. On the first line of the profile, specify the User-Name and Password attributes, and set User-Service=Framed-User.
2. Set Framed-Protocol=MPP.
3. Set Ascend-Send-Auth=Send-Auth-PAP or Send-Auth-CHAP (outgoing calls only).

   The Ascend-Send-Auth attribute specifies the authentication protocol that the MAX requests when initiating a connection using PPP or MP+ encapsulation. The answering side of the connection determines which authentication protocol, if any, the connection uses. Both sides of the connection must support the specified protocol.

   You can set Ascend-Send-Auth to one of these values:

   – Send-Auth-None (0) specifies that the MAX does not request an authentication protocol for outgoing calls: This setting is the default.

- Send-Auth-PAP (1) specifies that the MAX requests Password Authentication Protocol (PAP): PAP is a PPP authentication protocol that provides a simple method for the MAX to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment, and does not use encryption. The remote device must support PAP. If you choose this setting, the MAX requests PAP authentication, but uses CHAP authentication if the called unit requires CHAP. Choose this setting for non-token card authentication if you want to send your password unencrypted.
- Send-Auth-CHAP (2) specifies that the MAX requests Challenge Handshake Authentication Protocol (CHAP): CHAP is a PPP authentication protocol that is more secure than PAP. CHAP provides a way for the remote device to periodically verify the identity of the MAX using a three-way handshake and encryption. Authentication takes place upon initial link establishment. A device can repeat the authentication process any time after the connection is made. The remote device must support CHAP. If you choose this setting, the MAX does not bring up the connection using PAP. Choose this setting for non-token card authentication if you do not wish to send your password unencrypted—that is, if you do not wish to use PAP authentication.

4 If you request PAP or CHAP authentication, you must also specify a password using Ascend-Send-Secret or Ascend-Send-Passwd (outgoing calls only).

Both of these attributes specify the password that the MAX sends to the remote end of a connection on outgoing calls. If the value you specify for Ascend-Send-Secret or Ascend-Send-Password does not match the value of the remote end’s Ascend-Receive-Secret attribute (in a RADIUS user profile) or the Recv PW parameter (in a Connection profile), the remote system rejects the call.

Use Ascend-Send-Passwd only if your version of the MAX does not support Ascend-Send-Secret.

5 To turn on TCP/IP header compression, set Framed-Compression=Van-Jacobson-TCP-IP.

This setting applies only to packets in TCP applications, such as Telnet, and turns on header compression for both sides of the link. Turning on header compression is most effective in reducing overhead when the data portion of the packet is small.

6 Configure Dynamic Bandwidth Allocation attributes.

For details, see “Setting up Dynamic Bandwidth Allocation (DBA)” on page 4-53.

7 Set call management attributes.

For details, see “Specifying a time limit and idle connection attributes” on page 4-57.

8 Specify routing or bridging attributes for the connection.

For details on specifying that the connection use IP, see “Specifying IP routing and RIP behavior” on page 6-4. For details on specifying that the connection use IPX, see “Specifying IPX routing” on page 6-26. For details on specifying protocol-independent bridging, see “Specifying protocol-independent bridging” on page 6-34.

9 Configure the bridging or routing setup in the MAX for the WAN connection.

For details, see Chapter 6, “Setting Up Routing and Bridging Links” in this guide, and the relevant chapters of the MAX *ISP and Telecommuting Configuration Guide.*

MP+ connection example

This example shows a user profile for an MP+ link that sets DBA attributes and uses IP routing:

```
John  Password="4yr66", User-Service=Framed-User
      Framed-Protocol=MPP,
      Framed-Address=200.0.5.1,
      Framed-Netmask=255.255.255.0,
      Ascend-Target-Util=80,
      Ascend-History-Weigh-Type=History-Constant,
      Ascend-Seconds-Of-History=90,
      Ascend-Add-Seconds=30,
      Ascend-Remove-Seconds=30,
      Ascend-Maximum-Channels=10,
      Ascend-Inc-Channel-Count=2,
      Ascend-Dec-Channel-Count=2,
      Ascend-Route-IP=Route-IP-Yes,
      Ascend-Metric=7,
      Framed-Routing=None,
      Ascend-Idle-Limit=0,
      Ascend-Bridge=Bridge-No
```

Setting up a BACP connection

Bandwidth Allocation Control Protocol (BACP) is the Internet standard protocol equivalent to the Ascend MP+ bandwidth allocation protocol. BACP functions similarly to MP+ and uses the same attributes as MP+. The only additional attribute you must set is listed in Table 4-6.

Table 4-6. BACP attribute

Attribute	Description	Possible values
Ascend-BACP-Enable (134)	Specifies whether BACP is enabled on this link.	BACP-No (0) BACP-Yes (1) The default value is BACP-No.

To set up a BACP connection, follow these steps:

1 To enable incoming BACP calls, set BACP=Yes in the Ethernet > Answer > PPP Options menu.

2 In a RADIUS user profile, set Ascend-BACP-Enable=BACP-Yes.

3 Follow the instructions in “Setting up an MP or MP+ connection” on page 4-14, except for the following:

- You need not set MPP=Yes in the Ethernet > Answer > PPP Options menu.
- You need not set Framed Protocol=MPP.

All other MP+ settings apply to a BACP connection.

Setting up a Nailed/MPP connection

A Nailed/MPP connection is a nailed-up connection that can add switched channels for increased bandwidth. The MAX establishes a Nailed/MPP connection by connecting nailed-up or switched channels end-to-end

The MAX adds or subtracts switched channels as required by the DBA parameters in the Connection profile or RADIUS user profile. If the two sides of a connection disagree on the number of channels necessary for a connection, the side requesting the greater number prevails. Both sides make calculations on the required number of channels based on the traffic each side receives.

The maximum number of channels for the Nailed/MPP connection is the value of the Ascend-Maximum-Channels attribute or the number of nailed-up channels in the specified group, whichever is greater. If a nailed-up channel fails, MAX replaces that channel with a switched channel, even if the call is online with more than the minimum number of channels.

Before you begin

Before configuring the RADIUS user profile for a Nailed/MPP connection, you must perform the following tasks:

1 Work with the caller to find out about the dial-up software and the Ascend configuration at the remote end.

2 Determine the appropriate routing, bridging, and authentication settings for the caller.

3 For the MAX to use the Answer profile as the default when answering a call, set Use Answer as Default=Yes in the Ethernet > Answer menu on the MAX.

If you accept the default setting of No, the MAX uses the factory defaults.

4 In the Ethernet > Answer > PPP Options menu, set Recv Auth=PAP, CHAP, MS-CHAP, or Either.

If the incoming PPP call does not include a source IP address, the MAX requires PAP, CHAP, or MS-CHAP authentication.

5 To enable MP+ encapsulation, set MPP=Yes in the Ethernet > Answer > Encaps menu.

6 Assign a name to the MAX in the System profile.

7 Set up a Line profile in the MAX configuration interface by making these settings:

Action	Example
Specify which channels are nailed up.	For example, if channel 2 is nailed up, specify this setting: **Ch 2=Nailed** Nailed specifies that the channel is permanently connected. No dialout is required, so nailed-up channels do not require a phone number.
For each nailed-up channel, specify a group number from 1 to the maximum number of nailed-up groups that the MAX allows.	For example, to assign channel 2 to group 9, make this specification: **Ch 2 Prt/Grp=9** Each number represents a nailed-up group—that is, a permanent connection across the WAN.

8 On the remote end of the connection, set the AnsOrig and FT1 Caller parameters for answering only.

Note that the DO Hangup command works only from the caller end of the connection.

For complete information on the tasks specific to the MAX configuration interface, see the MAX *ISP and Telecommuting Configuration Guide*.

Configuring a Nailed/MPP connection in RADIUS

To configure a Nailed/MPP connection in RADIUS, you must set the attributes for a regular MP+ connection, and then configure the additional RADIUS attributes listed in Table 4-7.

Table 4-7. Nailed/MPP attributes

Attribute	Description	Possible values
Ascend-Call-Type (177)	Specifies the type of nailed-up connection in use.	Nailed (1) Nailed/Mpp (2) Perm/Switched (3) The default value is Nailed.
Ascend-FT1-Caller (175)	Specifies whether the MAX initiates an FT1-AIM or an FT1-B&O call, or whether it waits for the remote end to initiate these types of calls.	FT1-No (0) FT1-Yes (1) The default value is FT1-No.

Table 4-7. Nailed/MPP attributes (continued)

Attribute	Description	Possible values
Ascend-Group (178)	Points to the nailed-up channels that the WAN link uses.	Single integer, or comma-separated group of integers, between 1 and 60. The default value is 1.

To configure a Nailed/MPP connection in a RADIUS user profile, follow these steps:

1 Configure a regular MP+ connection in RADIUS, as described in "Setting up an MP or MP+ connection" on page 4-14.

2 Set Ascend-Call-Type=Nailed/Mpp.

3 To specify that the MAX is the designated caller for the switched part of the connection, set Ascend-FT1-Caller=FT1-Yes.

When you specify this setting, the MAX dials to bring online any switched circuits that are part of the call. The remote end must have the setting FT1 Caller=No (in a Connection profile) or Ascend-FT1-Caller=FT1-No (in a RADIUS user profile).

4 To specify the nailed-up channels the profile can use, set the Ascend-Group attribute.

This attribute points to the nailed-up channels the WAN link uses. Specify a single number, or specify a list of numbers between 1 and 60, separated by commas. Do not include spaces. The default value is 1. For example, setting the Ascend-Group attribute to "1,3,5,7" assigns four nailed-up groups to the profile.

If a Nailed/MPP connection is down and the nailed-up channels are also down, the connection does not re-establish itself until the nailed-up channels come back up or the switched channels are dialed. (The switched channels are dialed when the calling unit receives a packet whose destination is the unit at the remote end of the Nailed/MPP connection.)

Nailed/MPP connection example

In this example, a Nailed/MPP connection uses the channels in group 2:

```
Permconn-MAX2 Password="Ascend", User-Service=Dialout-Framed-
User
       User-Name="Matt",
       Framed-Protocol=MPP,
       Framed-Address=50.1.1.1,
       Framed-Netmask=255.0.0.0,
       Ascend-Route-IP=Route-IP-Yes,
       Ascend-Metric=7,
       Framed-Routing=None,
       Ascend-Idle-Limit=0,
       Ascend-Bridge=Bridge-No,
       Ascend-Call-Type=Nailed/Mpp,
       Ascend-Group="2",
       Ascend-FT1-Caller=FT1-Yes
```

Setting up a nailed-up connection

A nailed-up connection is a permanent link that is always up as long as the physical connection persists. If the unit or central switch resets or if the link goes down, the MAX attempts to restore the link at ten-second intervals. If the MAX or the remote unit is powered off, the link comes back up when the device is plugged in again. On an ISDN line, a nailed-up connection uses one or more of the line’s channels. A serial WAN link has no channels and is always 100% nailed up.

Before you begin

Before configuring a nailed-up connection in a RADIUS user profile, you must carry out these tasks in the MAX configuration interface:

1 In the Line profile, specify which channels are nailed-up.

For example, if channel 2 is nailed-up, specify this setting:

Ch 2=Nailed

Nailed specifies that the channel is permanently connected. No dialout is required, so nailed-up channels do not require a phone number.

2 For each nailed-up channel, specify a group number from 1 to the maximum number of nailed groups that the MAX allows.

For example, to assign channel 2 to group 9, make this specification:

Ch 2 Prt/Grp=9

Each number represents a nailed-up group—that is, a permanent connection across the WAN.

Configuring a nailed-up connection in RADIUS

To configure a nailed-up connection in RADIUS, use the attributes listed in Table 4-8.

Table 4-8. Nailed-up attributes

Attribute	Description	Possible values
Ascend-backup (176)	Specifies the profile name of a backup profile for a nailed-up link whose physical connection fails.	Text string. The default value is null.
Ascend-Call-Type (177)	Specifies the type of nailed-up connection in use.	Nailed (1) Nailed/Mpp (2) Perm/Switched (3) The default value is Nailed.
Ascend-FT1-Caller (175)	Specifies whether the MAX initiates an FT1-AIM or an FT1-B&O call, or whether it waits for the remote end to initiate these types of calls.	FT1-No (0) FT1-Yes (1) The default value is FT1-No.
Ascend-Group (178)	Points to the nailed-up channels that the WAN link uses.	Single integer, or comma-separated group of integers, between 1 and 60. The default value is 1.
Framed-Protocol (7)	Specifies the type of protocol the link can use.	PPP (1) SLIP (2) MPP (256) EURAW (257) EUUI (258) COMB (260) FR (261) ARA (262) FR-CIR (263) By default, the MAX does not restrict the type of protocol a link can use.
Password (2)	Specifies the user’s password.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Name (1)	Specifies the user’s name.	Alphanumeric string containing up to 252 characters. The default value is null.

Table 4-8. Nailed-up attributes (continued)

Attribute	Description	Possible values
User-Service (6)	Indicates whether the link can use framed or unframed services.	Login-User (1) Framed-User (2) Dialout-Framed-User (5) By default, the MAX does not restrict the services that a link can use.

To configure a nailed-up connection in a RADIUS user profile, follow these steps:

1 On the first line of the RADIUS user profile, specify the User-Name, Password, and User-Service attributes.

- For the User-Name attribute, specify a name that indicates an outgoing nailed-up connection.
- Set Password= “Ascend”.
- Set User-Service=Dialout-Framed-User: This setting ensures that the MAX cannot use the profile for authentication of an incoming call.

For example, you might enter this first line in the profile:

```
Permconn-MAX2 Password="Ascend", User-Service=Dialout-
Framed-User
```

2 On the second line of the user profile, specify the User-Name attribute to indicate the name of the user that can make the nailed-up connection.

3 Set the Framed-Protocol attribute.

4 Set the Ascend-Call-Type attribute to Nailed or Nailed/Mpp.

- Nailed (1) specifies a link that consists entirely of nailed-up channels: This value is the default.
- Nailed/Mpp (2) specifies a link that consists of both nailed-up and switched channels: If you specify this setting, you must also set Framed-Protocol=MPP. For information on setting up a Nailed/MPP connection, see “Setting up a Nailed/MPP connection” on page 4-19.

5 Set the Ascend-FT1-Caller attribute.

This attribute specifies whether the MAX initiates an FT1-AIM or an FT1-B&O call, or whether it waits for the remote end to initiate these types of calls.

- FT1-No (0) specifies that the MAX waits for the remote end to initiate the call. This value is the default.
- FT1-Yes (1) specifies that the MAX initiates the call. If you choose this setting, the MAX dials to bring online any switched circuits that are part of the call.

If the remote end has FT1 Caller=No (in a Connection profile) or Ascend-FT1-Caller=FT1-No (in a RADIUS user profile), set Ascend-FT1-Caller=FT1-Yes in the RADIUS user profile for the local MAX. By the same token, if the remote end has FT1 Caller=Yes (in a Connection profile) or Ascend-FT1-Caller=FT1-Yes (in a RADIUS user profile), set Ascend-FT1-Caller=FT1-No in the RADIUS user profile for the local MAX.

6 To specify the nailed-up channels the profile can use, set the Ascend-Group attribute.

This attribute points to the nailed-up channels that the WAN link uses. Your usage depends upon the value you specify for the Ascend-Call-Type attribute:

– If you set Ascend-Call-Type=Nailed, you can specify a number between 1 and 60 for Ascend-Group. The default value is 1.

– If you set Ascend-Call-Type=Nailed/Mpp, you can use the Ascend-Group attribute to assign multiple nailed-up groups to the profile. Specify a single number, or specify a list of numbers between 1 and 60, separated by commas. Do not include spaces. The default value is 1. For example, setting the Ascend-Group attribute to “1,3,5,7” assigns four nailed-up groups to the profile.

Nailed-up connection example

The pseudo-user profile in this example defines a nailed-up PPP connection using group number 2:

```
Permconn-MAX2 Password="Ascend", User-Service=Dialout-Framed-
User
       User-Name="Matt",
       Framed-Protocol=PPP,
       Framed-Address=50.1.1.1,
       Framed-Netmask=255.0.0.0,
       Ascend-Route-IP=Route-IP-Yes,
       Ascend-Metric=7,
       Framed-Routing=None,
       Ascend-Idle-Limit=0,
       Ascend-Bridge=Bridge-No,
       Ascend-Call-Type=Nailed,
       Ascend-Group="2",
       Ascend-FT1-Caller=FT1-Yes
```

Modifying or deleting nailed-up profiles

To modify or delete nailed-up profiles, follow these steps:

1 Change or delete the profile on the RADIUS server.

2 Choose the Upd Rem Cfg command from the Sys Diag menu.

The Ascend unit closes all the sessions related to all nailed-up profiles, deletes all the profiles from the system, and restarts the process of retrieving profiles from RADIUS.

Setting up a Combinet connection

The MAX supports Combinet bridging to link two LANs as though they were one segment. Figure 4-3 shows a Combinet connection between two networks.

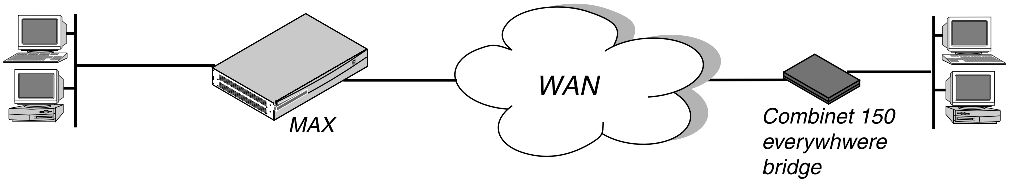

Figure 4-3. A Combinet connection

Before you begin

Before configuring the RADIUS user profile for a Combinet connection, you must perform the following tasks:

1 Work with the caller to find out about the remote device's MAC address and authentication information.

2 For the MAX to use the Answer profile as the default when answering a call, set Use Answer as Default=Yes in the Ethernet > Answer menu.

If you accept the default setting of No, the MAX uses the factory defaults.

3 To disable Guest access via Combinet, set Profile Reqd=Yes in the Ethernet > Answer menu.

Note that Combinet does not support PAP or CHAP authentication.

4 To enable Combinet encapsulation, set COMB=Yes in the Ethernet > Answer > Encaps menu.

5 Set Bridging=Yes in the Ethernet > Mod Config menu.

For information on the tasks specific to the MAX configuration interface, see the MAX *ISP and Telecommuting Configuration Guide.*

Configuring a Combinet connection in RADIUS

To configure a Combinet connection in RADIUS, use the attributes listed in Table 4-9.

Table 4-9. Combinet attributes

Attribute	Description	Possible values
Ascend-Bridge (230)	Enables or disables protocol-independent bridging for the call.	Bridge-No (0) Bridge-Yes (1) The default value is Bridge-No.

Table 4-9. Combinet attributes (continued)

Attribute	Description	Possible values
Ascend-Send-Passwd (232)	Specifies the password that the MAX sends to the remote end of a connection on outgoing calls.	Text string containing up to 20 characters. The default value is null.
Ascend-Send-Secret (214)	Specifies that the system encrypts the password when passing it between the RADIUS server and the MAX on outgoing calls.	Text string containing up to 20 characters. The default value is null.
Framed-Compression (13)	Turns on TCP/IP header compression.	You can specify Van-Jacobson-TCP-IP to turn on TCP/IP header compression. If you do not specify this value, RADIUS uses the default of no header compression.
Framed-Protocol (7)	Specifies the type of protocol the link can use.	PPP (1) SLIP (2) MPP (256) EURAW (257) EUUI (258) COMB (260) FR (261) ARA (262) FR-CIR (263) By default, the MAX does not restrict the type of protocol a link can use.
Password (2)	Specifies the user's password.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Name (1)	Specifies the MAC address of the remote device.	MAC address in standard 12-digit hexadecimal format (yyyyyyyyyyyy) or in colon-separated format (yy:yy:yy:yy:yy:yy). If the leading digit of a colon-separated pair is 0 (zero), you do not need to enter it. That is, **`:y`** is the same as **`:0y`**. The default value is null.

To configure a Combinet connection in a RADIUS user profile, follow these steps:

1. Specify a MAC address using the User-Name attribute, and a password using the Password attribute.

   When Profile Reqd=Yes in the Ethernet > Answer menu, the MAX compares the caller’s MAC address to the value of the User-Name attribute, and the value of the caller’s password to the value of the Password attribute. When Profile Reqd=No, the MAX uses the caller’s MAC address only.

   Note that Combinet bridging cannot use PAP or CHAP authentication. The MAX must use the caller’s MAC address and password to authenticate calls.

2. Set Framed-Protocol=COMB.

3. To turn on bridging for the profile, set Ascend-Bridge=Bridge-Yes.

4. Specify a password using Ascend-Send-Secret or Ascend-Send-Passwd (outgoing calls only).

   Both of these attributes specify the password that the MAX sends to the remote end of a connection on outgoing calls. If the value you specify for Ascend-Send-Secret or Ascend-Send-Password does not match the value of the remote end’s Ascend-Receive-Secret attribute (in a RADIUS user profile) or the Recv PW parameter (in a Connection profile), the remote system rejects the call.

   Use Ascend-Send-Passwd only if your version of the MAX does not support Ascend-Send-Secret.

5. To turn on TCP/IP header compression, set Framed-Compression=Van-Jacobson-TCP-IP.

   This setting applies only to packets in TCP applications, such as Telnet, and turns on header compression for both sides of the link. Turning on header compression is most effective in reducing overhead when the data portion of the packet is small.

6. Configure the bridging setup in the MAX for the WAN connection.

   For details, see Chapter 6, “Setting Up Routing and Bridging Links” in this guide, and the relevant chapters of the MAX *ISP and Telecommuting Configuration Guide.*

Combinet connection example

This user profile sets up a Combinet link:

```
000145CFCF01 Password="m2dan", User-Service=Framed-User
    Framed-Protocol=COMB,
    Ascend-Route-IP=Route-IP-No,
    Ascend-Bridge=Bridge-Yes,
    Ascend-Link-Compression=Link-Comp-Stac,
    Ascend-Idle-Limit=240
```

Setting up an AppleTalk connection

To set up an AppleTalk connection in RADIUS, use the attributes in Table 4-10.

Table 4-10.AppleTalk routing attributes

Attribute	**Description**	**Possible Values**
Ascend-AppleTalk-Peer-Mode (117)	Specifies whether the connection is for a single dial-in station or for a router.	• Appletalk-Peer-Router (0) specifies that the caller is an AppleTalk router, such as an Ascend Pipeline unit. • Appletalk-Peer-Dialin specifies that the caller is a dial-in AppleTalk client, such as a single Macintosh dialing in over a modem.
Ascend-Route-Appletalk (118)	Specifies whether AppleTalk routing is enabled for the connection. When AppleTalk routing is enabled, the connection can forward AppleTalk packets.	• Route-Appletalk-No (0) disables AppleTalk routing for this user profile. • Route-Appletalk-Yes (1) enables AppleTalk routing for this user profile. The default is No (0).
Ascend-Appletalk-Route (116)	Defines a static AppleTalk route in a RADIUS pseudo-user profile.	*net_start* Lower limit of the network range for this network. The default is blank. *net_end* Upper limit of the network range for this network. The default is blank. *zone_name* Name of the AppleTalk zone associated with this network. The default is blank. *profile_name* The outgoing RADIUS user profiles that the route uses. The default is blank.

To configure an AppleTalk connection in RADIUS, follow these steps:

1 Specify whether the calles is an AppleTalk router or a dial-in AppleTalk client in Ascend-AppleTalk Peer-Mode.

2 Enable AppleTalk routing for the connection by specifying Ascend-Route-Appletalk-Yes.

To define a static route for the connection, follow these steps:

1. Create a pseudo-user profile with the first line in the following format:

   ```
   appleroute-num Password="ascend’, user-service=Dialout-
   Framed-User
   Address 1
   Address 2
   ...
   Address n
   ```

   where `num` is a number in a series starting at 1, and `Address n` is the actual route associate with this entry.

2. Enter one or more static AppleTalk route specifications in the following format:

   ```
   Ascend-Appletalk-Route="net_start net_end zone_name
   profile_name"
   ```

   See Table 4-11 for descriptions of the arguments in this line.

Keep in mind the following:

Table 4-11.AppleTalk static route attributes

Argument	**Description**
net_start	The lower limit of the network range for this network. A network range is a range of network numbers set into the port descriptor of the router port and then transmitted through RTMP to the other nodes of the network. Each of the numbers within a network range can represent up to 253 devices. The default is blank.
net_end	The upper limit of the network range for this network. This range defines the networks available for packets routed using the static route. Specify a number between 1 and 65199. If there are other AppleTalk routers on the network, you must configure the network ranges to be identical to the ranges specified on the other routers.
zone_name	The name of the AppleTalk zone associated with this network. A zone is a multicast address containing a subset of the AppleTalk nodes on an internet. Each node belongs to only one zone, but a particular extended network can contain nodes belonging to any number of zones. Zones provide departmental or other groupings of network entities that a user can easily understand. In the Ascend AppleTalk router, zone names are case-insensitive. However, because some routers regard zone names as case-sensitive, the spelling of zone names should be consistent when you configure multiple connections or routers. You can use up to 33 alphanumeric characters. The default is blank.
profile_name	The outgoing RADIUS user profile that the route uses. The default is blank.

- Each static route must appear in a user profile.

- Ascend-Route-AppleTalk must be set to Yes.

Example of AppleTalk connection with static route

An example of a static route with the associated connection profile is:

```
appleroute-1  Password = “ascend” User-Service = Dialout-
Framed-User Ascend-Appletalk-Route = “20 25 testzone1 pipe50”

pipe50  Password = “ascend” User-Service = Dialout-Framed-User,
        User-Service = Framed-User,
        Framed-Protocol = MPP,
        Ascend-Appletalk-Peer-Mode = Appletalk-Peer-Router,
        Ascend-Route-Appletalk = Route-Appletalk-Yes,
        Ascend-Dialout-Allowed = Dialout-Allowed,
        Ascend-Dial-Number = “83272”,
        Ascend-Send-Auth = Send-Auth-PAP,
        Ascend-Send-Passwd = “MAX”
```

Setting up an ARA connection

AppleTalk Remote Access (ARA) connections rely on AppleTalk. The MAX includes a minimal AppleTalk stack for ARA support. The minimal stack includes a Name Binding Protocol (NBP) network-visible entity and an AppleTalk Echo Protocol (AEP) echo responder. You can therefore use standard AppleTalk management and diagnostic tools, such as InterPoll (from Apple Computer), to obtain information.

For a pure AppleTalk connection, a Macintosh user must have ARA Client software and an asynchronous modem. For a TCP/IP connection through ARA, the Macintosh must also be running TCP/IP software such as MacTCP or Open Transport.

ARA is an asynchronous protocol. It supports V.120, X.75, and modem calls only. It does not support V.110 calls or synchronous connections.

Figure 4-4 shows a Macintosh with an internal modem dialing into the MAX. The Macintosh uses the ARA Client software to communicate with an IP host on the Ethernet.

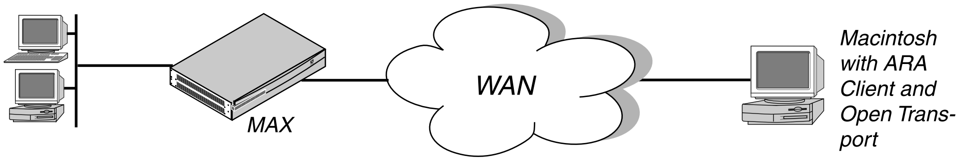

Figure 4-4. An ARA connection

Before you begin

Before configuring a RADIUS user profile for an ARA connection, you must perform the following tasks in the MAX configuration interface:

1 For the MAX to use the Answer profile as the default when answering a call, set Use Answer as Default=Yes in the Ethernet > Answer menu.

If you accept the default setting of No, the MAX uses the factory defaults.

2 To disable Guest access via ARA, set Profile Reqd=Yes in the Ethernet > Answer menu.

Note that ARA does not support PAP or CHAP authentication.

3 To enable ARA encapsulation, set ARA=Yes in the Ethernet > Answer > Encaps menu.

4 Set Appletalk=Yes in the Ethernet > Mod Config menu.

5 Set Auth=RADIUS or Auth=RADIUS/LOGOUT in the Ethernet > Mod Config menu.

6 If the local Ethernet supports an AppleTalk router with configured zones, set the Zone Name parameter in the Ethernet > Mod Config > AppleTalk menu.

For information on the tasks specific to the MAX configuration interface, see the MAX *ISP and Telecommuting Configuration Guide*.

Configuring an ARA connection in RADIUS

To configure an ARA connection in RADIUS, use the attributes listed in Table 4-12.

Table 4-12.ARA attributes

Attribute	Description	Possible values
Ascend-Ara-PW (181)	Indicates the password of the incoming caller over ARA.	Text string containing up to 20 characters. The default value is null.
Ascend-Assign-IP-Pool (218)	Specifies the address pool that incoming calls use.	Integer between 1 and 50. The default value is 1.
Ascend-Route-IP (228)	Specifies whether the MAX allows IP routing for the user profile.	Route-IP-No (0) Route-IP-Yes (1) The default value is Route-IP-Yes.
Framed-Address (8)	Specifies the IP address of the caller.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0. An answering user profile with this setting matches all IP addresses.
Framed-Netmask (9)	Specifies the subnet mask in use for a caller.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0.

Table 4-12.ARA attributes (continued)

Attribute	Description	Possible values
Framed-Protocol (7)	Specifies the type of protocol the link can use.	PPP (1) SLIP (2) MPP (256) EURAW (257) EUUI (258) COMB (260) FR (261) ARA (262) FR-CIR (263) By default, the MAX does not restrict the type of protocol a link can use.
Password (2)	Specifies the user's password.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Name (1)	Specifies the user's name.	Alphanumeric string containing up to 252 characters. The default value is null.

To configure an ARA connection in a RADIUS user profile, follow these steps:

1 Specify a user name using the User-Name attribute, and a password using the Password attribute.

For details on specifying a user name and password for incoming calls, see "Specifying a user name" on page 3-8 and "Specifying a password" on page 3-11. For information on specifying a user name and password for outgoing calls, see "Setting up outgoing calls" on page 4-58.

2 On any line other than the first one, set Framed-Protocol=ARA.

This setting specifies that a dial-in user can establish an ARA connection to the Ethernet network.

3 Set the Ascend-Ara-PW attribute to the same value specified by the Password attribute.

The MAX requires both the Password and the Ascend-Ara-PW attributes. The ARA software in the Ascend unit uses DES to encrypt and decrypt the ARA password.

4 For a TCP/IP connection through ARA, turn on IP routing by setting Ascend-Route-IP=Route-IP-Yes.

Then, carry out one of these tasks:

– If the MAC TCP/IP software has a hard-coded IP address, set the Framed-Address attribute (and, optionally, the Framed-Netmask attribute) to specify the Macintosh user's IP address.

- If the MAC TCP/IP software expects a dynamic IP address assignment, set up dynamic IP addressing as described in “Defining a pool of IP addresses for dynamic assignment” on page 6-8. Then, set the Ascend-Assign-IP-Pool attribute in the user profile to specify the address pool from which RADIUS should assign the user an address.

5 Configure the bridging or routing setup in the MAX for the WAN connection.

For details, see Chapter 6, “Setting Up Routing and Bridging Links” in this guide, and the relevant chapters of the MAX *ISP and Telecommuting Configuration Guide.*

ARA connection example

This example sets up a TCP connection through ARA with dynamic IP address assignment:

```
Emma Password="pwd"
     Framed-Protocol=ARA,
     Ascend-Ara-PW="pwd",
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Assign-IP-Pool=1
```

Setting up a terminal server connection

A terminal server connection is typically an incoming call that uses V.34, V.42, V.110, V.120, or X.75 encapsulation. It can also be an asynchronous data stream, such as a call from an analog modem or a serial connection to the MAX.

When the MAX receives a call that uses V.34, V.42, V.110, V.120, and X.75 encapsulation, it removes the encapsulation and then determines if the call is further encapsulated in PPP. If no PPP encapsulation is present, the MAX establishes a terminal server connection.

Figure 4-5 shows an incoming modem call initiated by a PC running SoftComm, a program that causes the user’s modem to dial into the MAX. The MAX directs the call to its digital modems, and then forwards the calls to its terminal server software. In Figure 4-5, the MAX immediately directs the call to a Telnet host.

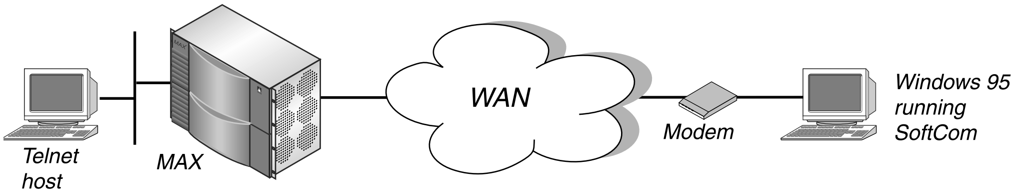

Figure 4-5. A terminal server connection

When the MAX directs the call to the terminal server, the user sees one of the terminal server interfaces (command line or menu), or bypasses the terminal server interface and initiates an immediate Telnet, TCP, or Rlogin connection to a host on the local network.

Note: Most sites restrict dial-in access to the terminal server interface of the MAX, because a user who has logged into the MAX is able to access status and routing information, and may be able to modify routes. See the MAX *Security Supplement* for details.

You can set RADIUS attributes in a user profile to perform these tasks relating to the terminal server interface:

- Enable Telnet, TCP, and Rlogin connections.
- Set the terminal server idle timer
- Configure menu items and an input prompt.
- Configure the banner text and a list of hosts to which users can Telnet.
- Control access to the MAX unit's digital modems on a per-user basis

Before you begin

Before configuring a terminal server connection in a RADIUS user profile, carry out these tasks in the MAX configuration interface:

1 For the MAX to use the Answer profile as the default when answering a call, set Use Answer as Default=Yes in the Ethernet > Answer menu.

If you accept the default setting of No, the MAX uses the factory defaults.

Note: You can restrict a specific user's access to terminal server commands if the user's connection is built in part upon the Answer profile. See the MAX *Security Supplement* for more information.

2 If you give the terminal server operator raw TCP access, makes sure that TCP-Clear=Yes in the Ethernet > Answer > Encaps menu.

3 To allow V.120 calls, set V.120=Yes in the Ethernet > Answer > Encaps menu.

4 To allow X.75 calls, set EU-RAW=Yes and EU-UI=Yes in the Ethernet > Answer > Encaps menu.

5 Navigate to the Ethernet > Mod Config > TServ Options menu.

6 To specify the type of security that the MAX uses for a remote terminal server session, set the Security parameter.

7 To specify whether users can establish Telnet sessions from the terminal server interface, set the Telnet parameter.

8 If you want the RADIUS server to remotely configure a login banner and a list of Telnet hosts, set Remote Conf=Yes.

9 To specify whether the operator uses the command-line interface or the menu-driven interface, set the Initial Scrn parameter, the Toggle Scrn parameter, or both.

The operator has access to a list of Telnet hosts only in the terminal server menu-driven interface.

10 To specify that you want to control the use of the MAX unit's digital modems for outgoing calls on a per-user basis, set Imm. Modem Auth=User.

11 In the Ethernet > Mod Config > Auth menu, set the Auth TS Secure parameter.

For further details on terminal server options in the MAX configuration interface, see the MAX *ISP and Telecommuting Configuration Guide*.

Overview of terminal server attributes

To configure a terminal server connection in RADIUS, use the attributes listed in Table 4-13.

Table 4-13.Terminal server attributes

Attribute	Description	Possible values
Ascend-Dialout-Allowed (131)	Specifies whether the user associated with the RADIUS user profile can dial out using one of the MAX unit's digital modems.	Dialout-Not-Allowed (0) Dialout-Allowed (1) The default value is Dialout-Not Allowed.
Ascend-Host-Info (252)	Specifies the IP address and name of the first, second, third, and fourth hosts to which you can establish a Telnet session, as listed in the terminal server menu-driven interface.	***`IP_address`*** specifies the IP address of each host. ***`text`*** describes each host. The default address is 0.0.0.0/0 and the default description is null.
Ascend-Menu-Item (206)	Defines a single menu item that appears in lieu of the terminal server prompt You can specify up to 20 Ascend-Menu-Item attributes per profile to give the user a custom menu of items from which to choose. The menu items display in the order in which they appear in the RADIUS profile.	***`command`*** is the string sent to the terminal server when the user selects the menu item. ***`text`*** is the text that displays to the user. ***`match`*** is the pattern the user must type to select the item. The first semi-colon (;) that appears acts as the delimiter between ***`command`*** and ***`text`***. The second semi-colon that appears acts as the delimiter between ***`text`*** and ***`match`***. By default, the MAX uses the standard terminal server menu.
Ascend-Menu-Selector (205)	Specifies a string as a prompt for user input in the terminal server menu interface.	Text string containing up to 31 characters. The default is `Enter Selection (1-`*`num`*`, q)`, where *`num`* is the number of items on the menu.
Ascend-TS-Idle-Limit (169)	Specifies the number of seconds that a terminal server connection must be idle before the MAX disconnects the session.	Integer between 0 and 65535.The default value is 120. A setting of 0 (zero) means that the line can be idle indefinitely.
Ascend-TS-Idle-Mode (170)	Specifies whether the MAX uses a terminal server idle timer and, if so, whether both the user and host must be idle before the MAX disconnects the session.	TS-Idle-None (0) TS-Idle-Input (1) TS-Idle-Input-Output (2) The default value is TS-Idle-Input.

Table 4-13.Terminal server attributes (continued)

Attribute	Description	Possible values
Login-Host (14)	Specifies the host to which the automatically connects when you set User-Service=Login-User and specify a value for the Login-Service attribute.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0. This setting specifies that the Login-User does not automatically connect to a particular host.
Login-Service (15)	Specifies the type of terminal service connection to an IP host that occurs immediately after authentication.	Telnet (0) Rlogin (1) TCP-Clear (2) By default, the MAX does not grant immediate access to an IP host.
Login-TCP-Port (16)	Specifies the port number to which a TCP session connects.	Integer between 1 and 65535. The default value is 23.
Password (2)	Specifies the user's password.	Alphanumeric string containing up to 252 characters. The default value is null.
Reply-Message (18)	Specifies text that appears to the terminal server operator using the menu-driven interface. You can specify up to 16 entries per user profile.	Text string containing up to 80 characters. The default value is null.
User-Name (1)	Specifies the user's name.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Service (6)	Indicates whether the link can use framed or unframed services.	Login-User (1) Framed-User (2) Dialout-Framed-User (5) By default, the MAX does not restrict the services that a link can use.

Enabling Telnet, TCP, and Rlogin connections

The terminal server software manages dial-in Telnet, TCP, and BSD-style Rlogin connections. You can set them up as regular terminal server connections, or you can direct them to an IP host immediately so that the dial-in user never sees the terminal server software. Telnet, TCP, and Rlogin connections are TCP/IP based.

To enable Telnet, TCP, and Rlogin connections in a RADIUS user profile, follow these steps:

1 Set User-Service=Login-User on the first line of the user profile, along with the User-Name and Password attributes.

Once the terminal server has authenticated an incoming caller, the operator can use an asynchronous Telnet connection to log into the terminal server, and can start Telnet or raw TCP sessions to an IP host on the local network. The MAX rejects incoming framed calls and the user cannot use any framed protocol.

For details on specifying a user name and password for incoming calls, see “Specifying a user name” on page 3-8 and “Specifying a password” on page 3-11. For information on specifying a user name and password for outgoing calls, see “Setting up outgoing calls” on page 4-58.

2 To specify the type of service that user immediately accesses upon login, set the Login-Service attribute.

When you set the Login-Service attribute, a dial-in terminal server user makes an immediate connection to an IP host on your local network and never sees the terminal server interface. You can specify one of these values:

– Telnet (0). The user immediately establishes a Telnet session with the host specified by the Login-Host attribute.

– Rlogin (1). The user immediately establishes an Rlogin session with the host specified by the Login-Host attribute.

– TCP-Clear (2). This setting specifies a TCP/IP connection with no Telnet protocol. TCP-Clear establishes a TCP session between the MAX and the host specified by Login-Host over which the user can run an application specified by Login-TCP-Port. If you specify this setting, the Ethernet > Answer menu must specify TCP-Clear=Yes.

3 To specify the host to which the Login-User automatically connects, set the Login-Host attribute.

Specify an IP address in dotted decimal notation. Access begins immediately after login. When you specify an IP address, the Login-User never sees the MAX interface, but connects immediately to the specified host via a Telnet, Rlogin, or TCP-Clear connection.

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, he or she can only have access to the hosts listed by the Ascend-Host-Info attribute.

If you specify Login-Service=Telnet or Login-Service=TCP-Clear, and you do not specify a value for the Login-Host attribute, the MAX unit’s response depends on the value of the Auth TS Secure parameter in the Ethernet > Mod Config > Auth menu. If Auth TS Secure=Yes (the default), the MAX drops the call. If Auth TS Secure=No, the MAX allows the caller access to the terminal server interface. For details on the Auth TS Secure parameter, see the MAX *Reference Guide.*

For information on the Ascend-Host-Info attribute, see “Configuring the message text and a list of hosts” on page 4-42.

4 If you set Login-Service=TCP-Clear, set the Login-TCP-Port attribute.

Specify the port number to which a TCP session connects. The default value is 23.

Terminal service access examples

In this example, an Rlogin session starts automatically for anyone using the Userx user name and xyzzy password. When the session terminates, the connection also terminates.

```
# This profile causes an auto-rlogin to 10.0.200.4 upon login.
Userx  Password="xyzzy"
       User-Service=Login-User,
       Login-Service=Rlogin,
       Login-Host=10.0.200.4,
       ...
```

Further, when you specify the following settings, a raw TCP session starts automatically for anyone using the User1 user name 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,
       ...
```

Setting the terminal server idle timer

The terminal server idle timer determines the circumstances under which the MAX disconnects a session. You cannot make terminal server idle timer settings for a frame relay or raw TCP connection.

To set the terminal server idle timer in a user profile, follow these steps:

1. To specify whether the MAX uses a terminal server idle timer and, if so, whether both the user and host must be idle before the MAX disconnects the session, set the Ascend-TS-Idle-Mode attribute.

   You can specify one of these settings:

   – TS-Idle-None (0). This setting indicates that the MAX does not disconnect the session no matter how long the line is idle. This setting disables the idle timer.

   – TS-Idle-Input (1). This setting indicates that the MAX disconnects the session if the user is idle for a length of time greater than the value of the Ascend-TS-Idle-Limit attribute.

     TS-Idle-Input is the default.

   – TS-Idle-Input-Output (2). This setting indicates that the MAX disconnects the session if both the user and the host are idle for a length of time greater than the value of the Ascend-TS-Idle-Limit attribute.

2. To specify the number of seconds that a terminal server connection must be idle before the MAX disconnects the session, set the Ascend-TS-Idle-Limit attribute.

Configuring a custom menu and an input prompt

You can configure the user profile give the operator a custom menu of items from which to choose, along with an input prompt. 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.

To configure a custom menu and an input prompt, follow these steps:

1 Set one or more Ascend-Menu-Item attributes.

Each Ascend-Menu-Item attribute defines a single menu item that appears in lieu of the terminal server prompt. You can specify up to 20 Ascend-Menu-Item attributes per profile. RADIUS ignores additional entries. The menu items display in the order in which they appear in the RADIUS profile.

Enter your specifications using this format:

Ascend-Menu Item="*command***;***text***[;***match***]"**

Table 4-14 lists each argument.

Table 4-14.Ascend-Menu-Item arguments

Argument	Description
command	Specifies 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	Specifies the text that displays to the user. The maximum length for ***text*** is 31 characters.
match	Specifies the pattern the user must type to select the item. The maximum length for ***match*** is 10 characters. Blanks are considered part of the matching pattern.
; (semi-colon)	The first semi-colon (;) that appears acts as the delimiter between ***command*** and ***text***. The second semi-colon that appears acts as the delimiter between ***text*** and ***match***.

If any entry consists of an option containing more that the maximum number of characters allowed, the RADIUS server discards the entry.

2 To specify a string as a prompt for user input in the terminal server menu interface, set the Ascend-Menu-Selector attribute.

By default, when you create a custom menu with the Ascend-Menu-Item attribute, the terminal server displays this string when prompting the user to make a selection:

Enter Selection (1-*num*, q)

The ***num*** argument represents the last number in the list. The terminal server code automatically determines the value of ***num*** by determining the number of items in the menu. The only valid user input is in the range 1 through ***num***, and q to quit.

However, you can specify a different string for prompting the user to make a selection. The Ascend-Menu-Selector attribute enables you to specify a string that the terminal server displays when prompting a user for a menu selection. If you define this attribute, its value overrides the default.

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.

Custom terminal server menu examples

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:
```

Now, suppose you also enter specifications for the ***match*** option, as in this profile:

```
Emma Password="m2dan", User-Service=Login-User
  Ascend-Menu-Item="show ip stats;ip=Display ip stats;ip",
  Ascend-Menu-Item="ping 1.2.3.4;p=Ping server. Ctrl-C stops ping;p",
  Ascend-Menu-Item="telnet 10.2.4.5;t=Telnet to Ken’s machine;t",
  Ascend-Menu-Item="show arp;dsp=Display arp table;dsp ",
  Ascend-Menu-Selector="          Option:",
  ...
```

The terminal server displays this text:

```
ip=Display ip stats          p=Ping server. Ctrl-C stops ping
t=Telnet to Ken's machine    dsp=Display arp table
        Option:
```

Note that you cannot combine numeric menu selections with pattern matching. This example shows what you should *not* do:

```
Emma Password="m2dan", User-Service=Login-User

  Ascend-Menu-Item="show ip stats;ip=Display ip stats",

  Ascend-Menu-Item="ping 1.2.3.4;p=Ping server. Ctrl-C stops ping;p",

  Ascend-Menu-Item="telnet 10.2.4.5;t=Telnet to Ken's machine;t",

  Ascend-Menu-Item="show arp;dsp=Display arp table;dsp ",

  Ascend-Menu-Selector="          Option:",

  ...
```

If you mix numbered selections and pattern matching, the terminal server screen displays the following text:

```
1. ip=Display ip stats             3. t=Telnet to Ken's machine
2. p=Ping server. Ctrl-C stops ping  4. dsp=Display arp table
          Option:
```

Configuring the message text and a list of hosts

For terminal server operators using the standard menu-driven interface, you can specify message text and a list of available Telnet hosts. The message text can contain instructions or other helpful information. The list of hosts consists of each host's IP address and description.

To set up message text and a list of hosts, follow these steps:

1 Create the first line of a pseudo-user profile using the User-Name, Password, and User-Service attributes.

You create a pseudo-user profile to store information that the MAX can query—in this case, in order to store message text and a list of hosts. You can configure pseudo-users for both global and MAX-specific configuration of the message text and list. The terminal server loads the unit-specific information in addition to the global information.

For a unit-specific configuration, specify the first line of a pseudo-user profile in this format:

Initial-Banner-*unit_name* Password="Ascend", User-Service=Dialout-Framed-User

unit_name is the system name of the Ascend unit—that is, the name specified by the Name parameter in the System profile.

For a global configuration, specify the first line of a pseudo-user profile in this format:

Initial-Banner Password="Ascend", User-Service=Dialout-Framed-User

2 To specify message text, set one or more Reply-Message attributes.

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.

An Access-Terminate-Session packet is a RADIUS packet identified by the code number 31. Only RADIUS daemons you customize support this packet code can send an Access-Terminate-Session packet. Neither the Ascend RADIUS daemon nor the Livingston RADIUS daemon supports this packet type. This packet can include only one attribute—the Reply-Message attribute—and this attribute can specify up to 80 characters of text.

When the MAX receives an Access-Terminate-Session packet, it starts a timer, displays any Reply-Message included in the packet, and terminates the session. For example, if a user's bill is past due, the Access-Terminate-Session packet could include the message

```
Emma, you have not paid your connect charges.
```

3 To specify a list of hosts to which a user can establish a Telnet session, set the Ascend-Host-Info attribute.

You can specify up to 10 Ascend-Host-Info entries. Enter your attribute settings in this format:

`Ascend-Host-Info="`*`IP_address text`***`"`**

`IP_address` specifies the IP address of each host, and ***`text`*** describes each host. You can enter up to 31 characters for ***`text`***. The RADIUS server assigns the text a number. When the user selects the number, the terminal server initiates a Telnet session with the host at the specified IP address.

If you specify a value for the Ascend-Host-Info attribute, you must also make these settings in the Ethernet > Mod Config > TServ Options menu:

– Set Initial Scrn=Menu or Toggle Scrn=Yes.

– Set Remote Conf=Yes.

Message text and host list example

Suppose you configure a MAX named Cal to use a RADIUS server. When Cal boots up (or when you enter the Upd Rem Cfg command), it looks into the RADIUS database for a pseudo-user profile named Initial-Banner-Cal. If it does not find this pseudo-user profile, it then looks for a pseudo-user profile named Initial-Banner. If it does not find this pseudo-user profile, it uses the value of the Banner parameter in the Ethernet > Mod Config > TServ Options menu.

Whenever a user logs into the MAX unit's terminal server, the screen displays the appropriate message text and list of hosts. Here is an example for a MAX named Cal:

```
Initial-Banner-Cal Password="Ascend", User-Service=Dialout-
Framed-User
     Reply-Message="Up to 16 lines of up to 80 characters each",
     Reply-Message="will be accepted. Long lines will be
truncated",
     Reply-Message="Additional lines will be ignored.",
     Reply-Message="",
     Ascend-Host-Info="1.2.3.4 Berkeley",
     Ascend-Host-Info="1.2.3.5 Alameda",
     Ascend-Host-Info="1.2.36 San Francisco",
     ...
```

Controlling access to the unit's digital modems on a per-user basis

The immediate modem feature enables a user to Telnet to a MAX in order to access the MAX unit's modems. The user can place outgoing calls without going through MAX terminal server interface. The MAXDial software offers the same outgoing call ability, but through a GUI interface.

You can control access to the modems on a per-user basis. Follow these steps:

1 In the Ethernet > Mod Config > TServ Options menu, set Imm. Modem Auth=User.

When Imm. Modem Auth=User, the MAX requests a login name before allowing any user access to the immediate modem feature. The MAX attempts to find a profile with the name the user provides, looking first for a local Connection profile and then for a RADIUS user profile. If the MAX cannot find a profile matching the name the user provides, the MAX rejects the call and closes the Telnet session. If the MAX finds a matching profile, the MAX prompts the user for the password associated with the profile and verifies that the user enters the correct password.

If the user enters the correct password, the MAX checks the Ascend-Dialout-Allowed attribute in the RADIUS user profile.

2 In a RADIUS user profile, set the Ascend-Dialout-Allowed attribute.

This attribute specifies whether the user associated with the RADIUS user profile can dial out using one of the MAX unit's digital modems. You can specify one of these settings:

- Dialout-Not-Allowed (0) indicates that the RADIUS user profile does not allow modem dialout. The default value is Dialout-Not Allowed.
- Dialout-Allowed (1) indicates that the RADIUS user profile allows modem dialout.

When you configure the MAX to use RADIUS accounting, RADIUS generates the appropriate session Start and Stop records for the immediate modem dialout sessions. In the Stop record, the attribute Ascend-Connect-Progress identifies a modem dialout session. The User-Name attribute contains the user name if Imm. Modem Auth=User. If Imm. Modem Auth=Global or None, the User-Name attribute is null. The Acct-Input-Octets attribute specifies the number of bytes the MAX received from the modem. The Acct-Output-Octets attribute specifies the number of bytes the MAX sent to the modem.

Call accounting does not record outgoing modem calls made through the terminal server interface. It applies only to immediate modem calls.

Digital modem dialout example

This profile enables the user Fred to dial out using the MAX unit's digital modems:

```
Fred Password="scr41"
     User-Service=Framed-User,
     Framed-Protocol=PPP,
     Framed-Address=10.0.1.1,
     Framed-Netmask=255.255.255.0,
     Ascend-Metric=2,
     Framed-Routing=None,
     Ascend-Idle-Limit=30,
Ascend-Dialout-Allowed=Dialout-Allowed
```

An extended terminal server example

In this example, a network administrator needs to set up a terminal server menu giving each user the choice of logging into a BBS or starting PPP, SLIP, or CSLIP. RADIUS is running on a UNIX server. The RADIUS server uses the Default profile to determine the kind of access it grants to users who do not appear in the users file.

Note: You can configure only one Default profile in the users file. Make sure that the Default profile is last in the file. RADIUS ignores any profiles that follow the Default profile.

The first line of the user profile enables a terminal server user to log in using his or her UNIX account name or password. The Reply-Message attribute provides introductory message text. The Ascend-Menu-Selector and Ascend-Menu-Item attributes provide each line of menu text.

```
Default Password="UNIX"
   Ascend-Idle-Limit=1800,
   Framed-Routing=None,
   Framed-Compression=Van-Jacobsen-TCP-IP,
   Ascend-Link-Compression=Link-Comp-None,
   Ascend-PPP-VJ-1172=PPP-VJ-1172,
   Ascend-Assign-IP-Pool=1,
   Ascend-Route-IP=Route-IP-Yes,
   Ascend-Route-IPX=Route-IPX-No,
   Ascend-Bridge=Bridge-No,
   Ascend-Handle-IPX=Handle-IPX-None,
   Ascend-Callback=Callback-No,
   Ascend-Data-Svc=Switched-Voice-Bearer,
   Reply-Message=”Welcome to ABCNet’s Terminal Server.”
   Ascend-Menu-Selector="Press q to Quit>>",
   Ascend-Menu-Item="rlogin bbs.net;BBS",
   Ascend-Menu-Item="ppp;Start PPP",
   Ascend-Menu-Item="slip;Start SLIP",
   Ascend-Menu-Item="cslip;Start CSLIP"
```

This text displays on the terminal server screen:

```
Welcome to ABCNet’s Terminal Server
1. BBS           3. Start SLIP
2. Start PPP     4. Start CSLIP
Press q to Quit>>
```

Notice that pressing the first option causes the MAX to establish an Rlogin session with the BBS at bbs.net.

Instead of using the Default profile, you can configure individual profiles to restrict users from certain services. For example, if you want the user Emma to immediately establish an Rlogin session with bbs.net upon authentication, you might use this user profile:

```
Emma Password="UNIX"
   User-Service=Login-User,
   Login-Host=bbs.net,
   Login-Service=Rlogin
```

To let new users sign up, you might use a profile like this one:

```
Guest Password="UNIX"
   User-Service=Login-User,
   Login-Host=unix.bbs.net,
   Login-Service=Rlogin
```

When a user dials in as Guest, he or she immediately logs into the UNIX machine. The UNIX machine has a shell /usr/local/bin/guest like this one:

```
#!/bin/sh
echo Welcome to BBS.NET.
signup
```

The signup line refers to an interactive shell script you can write in order to gather introductory information, set up a temporary account for verification, or perform any other relevant tasks.

Setting up a TCP connection between two MAX units

The MAX unit’s Dialed Number Information Service (DNIS) support enables ISPs to receive TCP connections instead of switched calls. Using DNIS, a MAX unit at a central switch creates a TCP connection to port 150 on a second MAX at an ISP. The MAX at the ISP treats the connection like a modem connection, routing the call to the terminal server interface or handling it as an asynchronous PPP session. The user appears to be connected to the second MAX.

This type of setup bypasses the Public Switched Telephone Network (PTSN). It also has the advantage of concentrating phone calls. For example, if the central switch receives two asynchronous calls, each of which use 32K of bandwidth, the MAX can handle both calls on one T1 PRI channel.

Figure 4-6 shows a TCP connection between MAX units.

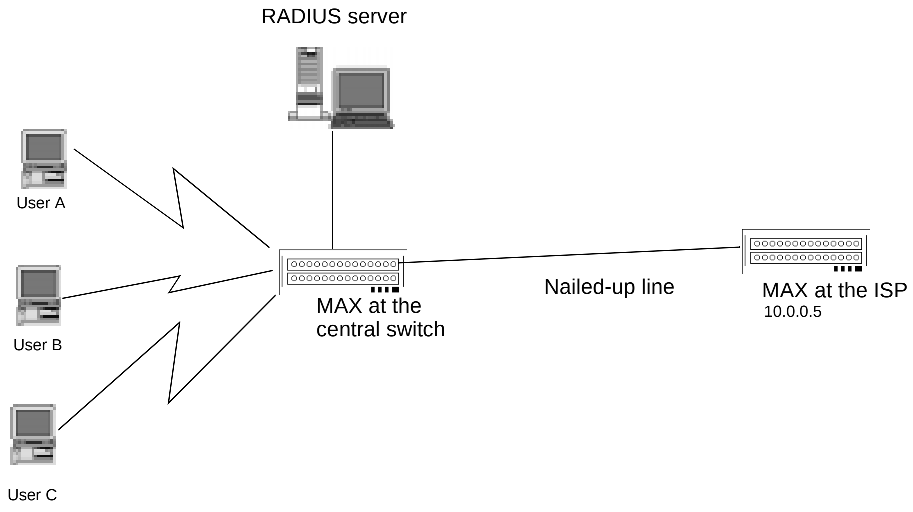

Figure 4-6. Sample TCP connection between MAX units

Before you begin

Before you set up the TCP connection in RADIUS, you must set Id Auth=Called Require in the Answer profile for the MAX at the central switch. This setting indicates that the called number must match the value of the called number in the user profile before the MAX can answer the call. For details, see the MAX *Reference Guide*.

Overview of TCP connection attributes

To set up the connection, you use the attributes in Table 4-15.

Table 4-15.TCP connection attributes

Attribute	Description	Possible values
Login-Host (14)	Specifies the host to which the user automatically connects when you set User-Service=Login-User and specify a value for the Login-Service attribute.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0. This setting specifies that the Login-User does not automatically connect to a particular host.

Table 4-15.TCP connection attributes (continued)

Attribute	**Description**	**Possible values**
Login-Service (15)	Specifies the type of terminal service connection to an IP host that occurs immediately after authentication.	Telnet (0) Rlogin (1) TCP-Clear (2) By default, the MAX does not grant immediate access to an IP host.
Login-TCP-Port (16)	Specifies the port number to which a TCP session connects.	Integer between 1 and 65535. The default value is 23.
Password (2)	Specifies the user's password.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Name (1)	Specifies the user's name.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Service (6)	Indicates whether the link can use framed or unframed services.	Login-User (1) Framed-User (2) Dialout-Framed-User (5) By default, the MAX does not restrict the services that a link can use.

Configuring the MAX at the central switch

To configure the MAX at the central switch, follow these steps:

1 Verify that the first line of all dial-in RADIUS user profiles has the following format:

```
phonenum Password="Ascend-DNIS"
```

– `phonenum` represents the called number.

– The Password value specifies that RADIUS authenticates the caller by called number only.

2 Set User-Service=Login-User.

3 Set Login-Service=TCP-Clear.

4 Set Login-Host to the IP address of the MAX at the ISP.

5 Set Login-TCP-Port=50.

Configuring the MAX at the ISP

To configure the MAX at the ISP, follow these steps:

1 Set User-Service=Login-User on the first line of the user profile, along with the User-Name and Password attributes.

Once the terminal server has authenticated an incoming caller, the operator can use an asynchronous Telnet connection to log into the terminal server, and can start Telnet or raw TCP sessions to an IP host on the local network. The MAX rejects incoming framed calls and the user cannot use any framed protocol.

2 To specify the type of service that a user immediately accesses upon login, set the Login-Service attribute.

When you set the Login-Service attribute, a dial-in terminal server user makes an immediate connection to an IP host on your local network and never sees the terminal server interface. You can specify one of these values:

– Telnet (0). The user immediately establishes a Telnet session with the host specified by the Login-Host attribute.

– Rlogin (1). The user immediately establishes an Rlogin session with the host specified by the Login-Host attribute.

– TCP-Clear (2). This setting specifies a TCP/IP connection with no Telnet protocol. TCP-Clear establishes a TCP session between the MAX and the host specified by Login-Host over which the user can run an application specified by Login-TCP-Port.

3 To specify the host to which the Login-User automatically connects, set the Login-Host attribute.

Specify an IP address in dotted decimal notation. Access begins immediately after login. When you specify an IP address, the Login-User never sees the MAX interface, but connects immediately to the specified host via a Telnet, Rlogin, or TCP-Clear connection.

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 by the Ascend-Host-Info attribute.

For information on the Ascend-Host-Info attribute, see “Configuring the message text and a list of hosts” on page 4-42.

4 If you set Login-Service=TCP-Clear, set the Login-TCP-Port attribute.

Specify the port number to which a TCP session connects. The default value is 23.

TCP connection example

Suppose the MAX at the central switch has this RADIUS user profile:

```
555-1212 Password="Ascend-DNIS"
         User-Service=Login-User,
         Login-Service=TCP-Clear,
         Login-Host=10.0.0.5,
         Login-TCP-Port=150
```

When the MAX receives a connection from a device at 555-1212, it opens a TCP connection to the specified IP address. The MAX at the ISP receives an incoming TCP connection on port

150 and treats that connection like a modem connection. The second MAX routes the call to the terminal server interface using a RADIUS user profile like this one:

```
UserA  Password="Test1"
       User-Service=Login-User,
       Login-Service=TCP-Clear,
       Login-Host=10.0.0.6,
       Login-TCP-Port=9
```

Managing bandwidth

You can manage bandwidth in one of the following ways:

- Use Dynamic Bandwidth Allocation (DBA).

  DBA is a way to automatically add or subtract channels on demand. When traffic levels expand, the MAX adds switched channels to the call. When traffic levels subside, it removes the channels and frees up the bandwidth for re-allocation.
- Specify a time limit for a session and the MAX unit's response to an idle connection.

To manage bandwidth in RADIUS, use the attributes listed in Table 4-16.

Table 4-16.Bandwidth management attributes

Attribute	Description	Possible values
Ascend-Add-Seconds (240)	Specifies the number of seconds that average line utilization (ALU) for transmitted data must exceed the threshold indicated by the Ascend-Target-Util attribute before the MAX begins adding bandwidth to a session.	Integer between 1 and 300. The default value is 5.
Ascend-Base-Channel-Count (172)	Specifies the initial number of channels the MAX sets up when originating calls for a PPP, MP+, MP, or Combinet multichannel link.	For a PPP link, the maximum number of channels is always 1. For an MP+ or MP link, you can specify any value up to the number of channels available, but the device at the remote end of the link must also support MP+ or MP. For a Combinet link, you can specify up to two channels. The default value is 1.

Table 4-16.Bandwidth management attributes (continued)

Attribute	**Description**	**Possible values**
Ascend-DBA-Monitor (171)	Specifies how the MAX monitors traffic on an MP+ call.	DBA-Transmit (0) DBA-Transmit-Recv (1) DBA-None (2) The default value is DBA-Transmit.
Ascend-Dec-Channel-Count (237)	Specifies the number of channels the MAX removes when bandwidth changes either manually or automatically during a call.	Integer between 1 and 32. The default value is 1.
Ascend-History-Weigh-Type (239)	Specifies which Dynamic Bandwidth Allocation (DBA) algorithm to use for calculating average line utilization (ALU) of transmitted data.	History-Constant (0) History-Linear (1) History-Quadratic (2) The default value is History-Quadratic.
Ascend-Idle-Limit (244)	Specifies the number of seconds the MAX waits before clearing a call when a session is inactive.	Integer between 0 and 65535. The default value is 120. If you accept the default and the Answer profile specifies a value for the analogous Idle parameter on the MAX, the MAX ignores the Idle value uses the Ascend-Idle-Limit default.
Ascend-Inc-Channel-Count (236)	Specifies the number of channels the MAX adds when bandwidth changes either manually or automatically during a call.	Integer between 1 and 32. The default value is 1.
Ascend-Maximum-Call-Duration (125)	Specifies the maximum number of minutes an incoming call can remain connected.	Integer between 0 and 1440. The default value is 0 (zero).
Ascend-Maximum-Channels (235)	Specifies the maximum number of channels the MAX allows on an MP+ call.	Integer between 1 and the maximum number of channels your system supports. The default value is 1.

Table 4-16.Bandwidth management attributes (continued)

Attribute	Description	Possible values
Ascend-Maximum-Time (194)	Specifies the maximum length of time in seconds that any session can remain online. Once a session reaches the time limit, the MAX takes its connection offline.	Integer between 0 and 4,294,967,295. The default value is 0 (zero). When you accept the default, the MAX does not enforce a time limit.
Ascend-Minimum-Channels (173)	Specifies the minimum number of channels an MP+ call maintains.	The default value is 1.
Ascend-MPP-Idle-Percent (254)	Specifies a percentage of bandwidth utilization below which the MAX clears a single-channel MP+ call.	Integer between 0 and 99. The default value is 0 (zero).
Ascend-Preempt-Limit (245)	Specifies the number of idle seconds the MAX waits before using one of the channels of an idle link for a new call.	Integer between 0 and 65535. The default value is 60.
Ascend-Remove-Seconds (241)	Specifies the number of seconds that average line utilization (ALU) for transmitted data must fall below the threshold indicated by the Ascend-Target-Util attribute before the MAX begins removing bandwidth from a session.	Integer between 1 and 300. The default value is 10.
Ascend-Seconds-Of-History (238)	Specifies the number of seconds the MAX uses as a sample for calculating average line utilization (ALU) of transmitted data.	Integer between 1 and 300. The default value is 15.
Ascend-Target-Util (234)	Specifies the percent bandwidth utilization at which the MAX adds or subtracts bandwidth dynamically.	Integer between 0 and 100. The default value is 70.

Setting up Dynamic Bandwidth Allocation (DBA)

How DBA works

The MAX uses the historical time period specified by the Ascend-Seconds-Of-History attribute as the basis for calculating average line utilization (ALU), and uses the algorithm specified by the Ascend-History-Weigh-Type attribute for calculating ALU.

The MAX then compares ALU to the amount specified by the Ascend-Target-Util attribute. When ALU exceeds the threshold defined by Ascend-Target-Util for a period of time greater than the value of the Ascend-Add-Seconds attribute, the MAX attempts to add the number of channels specified by the Ascend-Inc-Channel-Count attribute. When ALU falls below the threshold defined by Ascend-Target-Util for a period of time greater than the value of the Ascend-Remove-Seconds attribute, the MAX attempts to remove the number of channels specified by the Ascend-Dec-Channel-Count attribute.

The MAX compares the calculated ALU to the percentage specified in the Ascend-Target-Util attribute. It uses this logic to decide when to add channels:

If ALU > Ascend-Target-Util for > Ascend-Add-Seconds seconds, add Ascend-Inc-Channel-Count channels.

The MAX uses this logic to decide when to subtract channels:

If ALU < Ascend-Target-Util for > Ascend-Remove-Seconds seconds, subtract Ascend-Dec-Channel-Count channels.

How RADIUS authenticates multiple channels

When the system adds additional channels, the MAX must authenticate each one. You can secure each circuit using one of methods described in the following sections.

Static passwords

Before the MAX dials a new circuit, it prompts the user to enter a static, reusable password as specified in the RADIUS user profile. To prevent intruders from capturing the password as it travels across the WAN, you can specify that the MAX use the Challenge Handshake Authentication Protocol (CHAP). This protocol uses encryption to protect the password and verify the identity of the caller.

For information on specifying a static password, see “Setting the Password attribute” on page 3-11. For information on requiring CHAP authentication, see “Requiring PAP, CHAP, or MS-CHAP for PPP, MP, and MP+ calls” on page 3-20.

Dynamic passwords

Using PAP-TOKEN authentication, RADIUS can require a user to specify a one-time-only password from a security-card server for each additional channel. For information, see “Configuring PAP-TOKEN authentication” on page 3-29.

Combination of static and dynamic passwords

In RADIUS, you can indicate that the user need only specify a dynamic password for the initial channel, and that CHAP will authenticate all additional channels. Whenever the MAX adds channels to a PPP or MP+ call using PAP-TOKEN-CHAP authentication, the calling unit sends the encrypted value of Aux Send PW (in the Connection profile at the remote end), and the answering unit checks this password against the value of Ascend-Receive-Secret in the RADIUS user profile. The answering unit receives Ascend-Receive-Secret from the RADIUS server when the first channel of the call connects.

For details, see “Configuring PAP-TOKEN-CHAP authentication” on page 3-32.

Cached passwords

You can configure RADIUS to reuse a password dynamically generated during session initiation. In this case, both the user and the MAX cache the password. Then, when the MAX needs to add bandwidth, the user provides the CHAP-encrypted password automatically and the MAX uses an internal key to authenticate the additional channels. You can specify a timeout value for the cached password, or configure RADIUS to maintain the password throughout the session.

For details on setting up RADIUS for cached passwords, see “Configuring CACHE-TOKEN authentication” on page 3-30.

Configuring DBA in RADIUS

To configure DBA for a RADIUS user profile, follow the steps described below. For guidelines on how to set up DBA for optimal performance, see “Guidelines for optimal use of DBA” on page 4-56.

1 Configure an MP+ connection, as described in “Configuring an MP or MP+ connection in RADIUS” on page 4-15.

2 To specify the percentage of bandwidth use at which the MAX should add or subtract bandwidth, set the Ascend-Target-Util attribute.

3 To select the algorithm to use for calculating ALU, set the Ascend-History-Weigh-Type attribute.

Figure 4-7 illustrates the differences among the algorithms you can choose.

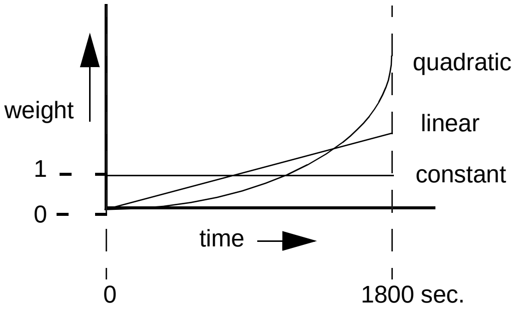

Figure 4-7. Bandwidth algorithms for MP+ calls

– History-Constant (0) gives equal weight to all samples taken during the historical time period specified by Ascend-Seconds-Of History. When you select this option, older historical samples have as much impact on the decision to change bandwidth allocation as do more recent samples.

- History-Linear (1) gives more weight to recent samples of bandwidth usage than to older samples taken during the historical period specified by Ascend-Seconds-Of-History. The weighting grows at a linear rate.
- History-Quadratic (2) gives more weight to recent samples of bandwidth usage than to older samples taken during the historical period specified by Ascend-Seconds-Of-History. The weighting grows at a quadratic rate. History-Quadratic is the default.

4 To specify the number of seconds that the MAX uses as a sample for calculating ALU, set the Ascend-Seconds-of-History attribute.

5 To specify the number of seconds that ALU must exceed the threshold indicated by the Ascend-Target-Util attribute before the MAX begins adding bandwidth to a session, set the Ascend-Add-Seconds attribute. Once the MAX adds bandwidth, there is typically a minimum usage charge. Thereafter, billing is time sensitive.

6 To specify the number of seconds that ALU must fall below the threshold indicated by the Ascend-Target-Util attribute before the MAX begins removing bandwidth from a session, set the Ascend-Remote-Seconds attribute.

The Ascend-Remove-Seconds value should be at least equal to the minimum duration charge plus one or two billing time increments. Typically, billing is done to the next multiple of six seconds, with a minimum charge for the first thirty seconds. Your carrier representative can help you understand the billing structure of the switched tariffs.

7 To specify the initial number of channels the MAX sets up when originating calls for the link, specify the Ascend-Base-Channel-Count attribute.

8 To specify the maximum number of channels the MAX allows on a call, set the Ascend-Maximum-Channels attribute.

9 To specify the minimum number of channels the call maintains, set the Ascend-Minimum-Channels attribute.

10 To specify the number of channels to add to a call when increasing bandwidth, set the Ascend-Inc-Channel-Count attribute.

11 To specify the number of channels to remove from a call when decreasing bandwidth, set the Ascend-Dec-Channel-Count attribute.

12 To specify how the MAX monitors traffic on an MP+ call, set the Ascend-DBA-Monitor attribute.

You can specify one of these values:

- DBA-Transmit (0). This setting specifies that the MAX adds or subtracts bandwidth based on the amount of data it transmits. DBA-Transmit is the default.
- DBA-Transmit-Recv (1). This setting specifies that the MAX adds or subtracts bandwidth based on the amount of data it transmits *and* receives.
- DBA-None (2). This setting specifies that the MAX does not monitor traffic over the link, and disables DBA.

Guidelines for optimal use of DBA

For optimum MP+ performance, set these values to the same number on both sides of a connection:

- The base channel count, as specified by Base Ch Count (in the Connection profile) or Ascend-Base-Channel-Count (in RADIUS)
- The minimum channel count, as specified by Min Ch Count (in the Answer profile or Connection profile) or Ascend-Minimum-Channels (in RADIUS)
- The maximum channel count, as specified by Max Ch Count (in the Answer profile or Connection profile) or Ascend-Maximum-Channels (in RADIUS)

The values for the Ascend-Seconds-Of-History, Ascend-Add-Seconds, and Ascend-Remove-Seconds attributes should smooth out spikes in bandwidth utilization that last for a shorter time than it takes to add capacity. Over T1 lines, the MAX can add bandwidth in less than ten seconds. Over ISDN lines, the MAX can add bandwidth in less than five seconds.

If you specify a small value for the Ascend-Seconds-Of-History attribute, and increase the values of the Ascend-Add-Seconds attribute and the Ascend-Remove-Seconds attribute relative to the value of Ascend-Seconds-Of-History, the system becomes less responsive to quick spikes. The easiest way to determine the proper values for all these attributes is to observe usage patterns. If the system is not responsive enough, the value of Ascend-Seconds-Of-History is too high.

Avoid adding or subtracting channels too quickly (less than 10-20 seconds apart). This leads to many short duration calls, each of which incur the carrier's minimum charge. In addition, adding or subtracting channels too quickly can affect link efficiency, since the devices on either end have to retransmit data when the link speed changes.

When selecting a target utilization value, monitor how the application behaves when using different bandwidths and different loads. For example, an application might be able to use 88% of a 64-kbps link, but only 70% of a 256-kbps link.

DBA example

This RADIUS user profile contains all the RADIUS attributes necessary for configuring DBA.

```
John  Password="4yr66", User-Service=Framed-User
      Framed-Protocol=MPP,
      Framed-Address=200.0.5.1,
      Framed-Netmask=255.255.255.0,
      Ascend-Target-Util=80,
      Ascend-History-Weigh-Type=History-Constant,
      Ascend-Seconds-Of-History=90,
      Ascend-Add-Seconds=30,
      Ascend-Remove-Seconds=30,
      Ascend-Maximum-Channels=10,
      Ascend-Inc-Channel-Count=2,
      Ascend-Dec-Channel-Count=2,
      Ascend-DBA-Monitor=DBA-Transmit-Recv,
      ...
```

Specifying a time limit and idle connection attributes

To specify the time limit for a session and the action the MAX should take when a connection is idle, follow these steps:

1 Configure an MP+ connection, as described in “Setting up an MP or MP+ connection” on page 4-14.

2 To specify the maximum number of minutes an incoming call can remain connected, set the Ascend-Maximum-Call-Duration attribute.

You can specify an integer between 0 and 1440. The MAX checks the connection once per minute, so the actual time the call remains connected is slightly longer than the actual time you set.

The default value is 0 (zero). If you accept the default, the MAX does not set a limit on the duration of an incoming call.

3 To specify the maximum length of time in seconds that the MAX allows any session to stay online, set the Ascend-Maximum-Time attribute.

Once a session reaches the time limit, the MAX takes its connection offline.

4 To indicate the number of seconds the MAX waits before clearing a call when a session is inactive, set the Ascend-Idle-Limit attribute.

Specify a number between 0 and 65535. If you specify 0 (zero), the MAX always clears a call when a session is inactive. The default value is 120 seconds.

The Ascend-Idle-Limit attribute does not apply to nailed-up links.

5 To specify a percentage of bandwidth utilization below which the MAX clears a single-channel MP+ call, set the Ascend-MPP-Idle-Percent attribute.

Specify an integer between 0 and 99. The default value is 0 (zero). This setting causes the MAX to ignore bandwidth utilization when determining whether to clear a call.Bandwidth utilization must fall below this percentage *on both sides of the connection* before the MAX clears the call.

If the device at the remote end of the link enters an Ascend-MPP-Idle-Percent value (in RADIUS) or an Idle Pct setting (on the MAX) lower than the value you specify, the MAX does not clear the call until bandwidth utilization falls below the lower percentage.

If the time set by the Ascend-Idle-Limit expires, the call disconnects whether or not bandwidth utilization falls below the Ascend-MPP-Idle-Percent setting. When bandwidth utilization falls below the Ascend-MPP-Idle-Percent setting, the call disconnects regardless of whether the time specified by the Ascend-Idle-Limit attribute has expired.

Because the Ascend-MPP-Idle-Percent attribute is dependent on traffic levels on both sides of the connection, we recommend that you use the Ascend-Idle-Limit attribute in preference to it.

6 To indicate the number of idle seconds the MAX waits before using one of the channels of an idle link for a new call, set the Ascend-Preempt-Limit attribute.

Specify a number between 0 and 65535. The MAX never preempts a call if you enter 0 (zero). The default value is 60.

The Ascend-Preempt-Limit attribute does not apply to nailed-up links.

Setting up outgoing calls

To configure outgoing calls in RADIUS, use the attributes listed in Table 4-17

Table 4-17.Outgoing call attributes

Attribute	Description	Possible values
Ascend-Billing-Number (249)	Specifies a billing number for charges incurred on the line. If you do not enter a billing number, the telephone company assigns charges to the telephone number associated with the line.	Up to ten characters, and limited to the following: **1234567890()[]!z-*# |** The default value is null.
Ascend-Call-By-Call (250)	Specifies the T1 PRI service that the MAX uses when placing a PPP call.	Integer corresponding to services provided by AT&T, MCI, and Sprint. By default, the MAX uses ACCUNET Switched Digital Services from AT&T (6).
Ascend-Data-Svc (247)	Specifies the type of data service the link uses for outgoing calls.	For a full list of possible values, see “Ascend-Data-Svc (247)” on page 9-29. The default value is Switched-56K.
Ascend-Dial-Number (227)	Specifies the phone number the MAX dials to reach the bridge, router, or node at the remote end of the link.	Up to 21 characters, limited to the following: **1234567890()[]!z-*#|** The default value is null.
Ascend-Expect-Callback (149)	Specifies whether the outgoing caller should expect the remote end to call back.	Expect-Callback-No (0) Expect-Callback-Yes (1) The default value is Expect-Callback-No.
Ascend-PRI-Number-Type (226)	Specifies the type of phone number the MAX dials.	Unknown-Number (0) Intl-Number (1) National-Number (2) Local-Number (4) Abbrev-Number (5) The default value is National-Number.

Table 4-17.Outgoing call attributes (continued)

Attribute	**Description**	**Possible values**
Ascend-Transit-Number (251)	Specifies the U.S Interexchange Carrier (IEC) you use for long distance calls over a T1 PRI line.	Integer corresponding to an IEC. The default value is null.
Framed-Address (8)	Specifies the IP address of the caller.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0. An answering user profile with this setting matches all IP addresses.
Framed-Netmask (9)	Specifies the subnet mask in use for a caller.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0.
Password (2)	Specifies the user's password.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Name (1)	Specifies the user's name.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Service (6)	Indicates whether the link can use framed or unframed services.	Login-User (1) Framed-User (2) Dialout-Framed-User (5) By default, the MAX does not restrict the services that a link can use.

To configure outgoing calls in a RADIUS user profile, follow these steps:

1 On the first line of the user profile, specify the User-Name, Password, and User-Service attributes.

- For the User-Name attribute, specify the name of the user, appending **`-Out`** to the user name.
- Set Password = "Ascend".
- Set User-Service=Dialout-Framed-User. This setting ensures that the MAX cannot use the profile for authentication of an incoming call.

For example, you might enter this first line in the profile for the user Homer:

Homer-Out Password="Ascend", User-Service=Dialout-Framed-User

2 On the second line of the user profile, specify the name of the user that can make outgoing calls by indicating a value for the User-Name attribute.

3 If the receiving end requires an IP address, and does not assign one dynamically, specify the caller's IP address using the Framed-Address attribute (and, optionally, the Framed-Netmask attribute).

The values of the Framed-Address and Framed-Netmask attributes for the local MAX must match the NAS-Identifier attribute (in RADIUS) or the IP Adrs parameter (in a Connection profile) on the Ascend unit at the remote end of the link. If there is no match, the remote end clears the call.

If you specify an IP address, you must also enable IP routing for the profile by setting Ascend-Route-IP=Route-IP-Yes. For more information, see "Setting up a system-based IP routing connection" on page 6-1.

4 To indicate the phone number the MAX dials to reach the bridge, router, or node at the remote end of the link, set the Ascend-Dial-Number attribute.

Specify a telephone number. You can enter up to 21 characters, and you must limit those characters to the following:

1234567890()[]!z-*#|

The MAX sends only the numeric characters to place a call. The default value is null.

If Use Trunk Grps=Yes in the System profile, the first digits in the Ascend-Dial-Number attribute have the meanings listed in Table 4-18.

Table 4-18.Ascend-Dial-Number digits

Digit	**Explanation**
First digit is between 4 and 9.	The MAX places the call over the corresponding trunk group listed in the Ch *n* Trnk Grp, B1 Trnk Grp, or B2 Trnk Grp parameters in the Line profile. If Dial Plan=Trunk Grp, the digits following the first digit constitute an ordinary phone number. If Dial Plan=Extended, the next two digits specify the Dial Plan profile containing the parameters the MAX uses when making the call. These parameters constitute the extended dial plan. An ordinary phone number follows these two digits.
First digit is 3.	The MAX places the call to a destination listed in a Destination profile. In this case, the second and third digits indicate the number of the Destination profile.

Table 4-18.Ascend-Dial-Number digits (continued)

Digit	Explanation
First digit is 2.	The MAX places the call between host ports on the same MAX, or between Terminal Equipment (TEs) on a local ISDN BRI line on the same MAX. The first type of call is a port-to-port call. The latter type of call is a TE-to-TE call. In a port-to-port call, the second digit indicates the slot of an AIM/6 card. In a TE-to-TE call, the second digit indicates the slot of a Host/BRI module. If you enter 0 (zero) for the second digit, the call connects to any available AIM port and ignores the third digit. If you enter a nonzero value for the second digit, the third digit selects the AIM port (for a port-to-port call) or a local ISDN BRI port (for a TE-to-TE call). If you enter 0 (zero) for the third digit, the call connects to any available AIM port or local ISDN BRI line in the module selected by the second digit.

5 To specify the data service the link uses for outgoing calls, set the Ascend-Data-Svc attribute.

6 To indicate a billing number for charges incurred on the line, set Ascend-Billing-Number.

Specify a telephone number. You can specify up to ten characters, and you must limit those characters to the following:

1234567890()[]!z-*# |

If you do not enter a billing number, the telephone company assigns charges to the telephone number associated with the line. Your carrier determines the billing number, and uses it to sort your bill. If you have several departments, and each department has its own billing number, your carrier can separate and tally each department's usage.

The MAX uses the Ascend-Billing-Number differently depending on the type of line you use:

- For a T1 line, the MAX appends the value specified in the Ascend-Billing-Number attribute to the end of each phone number it dials for the call.
- Ascend-Billing-Number for outgoing calls on an ISDN BRI line applies only to installations in Australia.
- For a T1 PRI line, the MAX uses the Ascend-Billing-Number attribute, rather than the phone number ID to identify itself to the answering party.

7 To specify the T1 PRI service that the MAX uses when placing a PPP call, specify the Ascend-Call-By-Call attribute.

Specify a number corresponding to the type of service the MAX uses. The default value is 6. Table 4-19 lists the services available for each service provider.

Table 4-19.Ascend-Call-By-Call settings

Number	AT&T	Sprint	MCI
0	Disable call-by-call service.	Reserved	N/A
1	SDN (including GSDN)	Private	VNET/Vision
2	Megacom 800	Inwatts	800
3	Megacom	Outwatts	PRISM1, PRISM II, WATS
4	N/A	FX	900
5	N/A	Tie Trunk	DAL
6	ACCUNET Switched Digital Services	N/A	N/A
7	Long Distance Service (including AT&T World Connect)	N/A	N/A
8	International 800 (I800)	N/A	N/A
16	AT&T MultiQuest	N/A	N/A

8 To specify the type of phone number the MAX dials, set the Ascend-PRI-Number-Type attribute.

You can specify one of these settings:

– Unknown-Number (0). This setting indicates that the MAX can dial any type of number.

– Intl-Number (1). This setting indicates that the MAX dials a number outside the U.S.

– National-Number (2). This setting indicates that the MAX dials a number inside the U.S. The National-Number value is the default.

– Local-Number (4). This setting indicates that the MAX dials a number within your Centrex group.

– Abbrev-Number (5). This setting indicates that the MAX dials an abbreviated phone number.

9 To specify the U.S Interexchange Carrier (IEC) you use for long distance calls over a T1 PRI line, set the Ascend-Transit-Number attribute.

Specify the same digits you use to prefix a phone number you dial over an ISDN BRI line, T1 access line, or voice interface:

– 288 selects AT&T.

– 222 selects MCI.

– 333 selects Sprint.

The default value is null. If you accept the default, the MAX uses any available IEC for long-distance calls.

10 To specify whether the caller expects the remote device to call back, set the Ascend-Expect-Callback attribute.

When the remote device is set to call back (Ascend-Callback=Callback-Yes in RADIUS or Callback=Yes on the MAX) and CLID authentication is not required, the remote device answers the call, verifies a name and password against a user profile, hangs up, and dials back to the caller.

If the remote end is set up for callback *and* requires CLID-only authentication (Id Auth=Require), the remote device never answers the call. The caller can therefore avoid billing charges. However, a problem can also occur. To the caller, it appears as though the call never got through at all. This is a special problem for Ping and Telnet, because these processes continuously try to open a connection and reject any callback.

When you set Ascend-Expect-Callback=Expect-Callback-Yes, calls that dial out and do not connect (for any reason) appear on a list that disallows any further calls to that destination for 90 seconds. This delay gives the remote device an opportunity to complete the callback.

You can specify one of these values:

– Expect-Callback-No (0) indicates that the caller does not wait for a callback after placing a call that does not connect.

– Expect-Callback-Yes (1) indicates that the caller waits 90 seconds after placing a call that does not connect before attempting to place another call to the same number.

Outgoing call example

This example shows a user profile for dialing calls from the MAX. This profile uses Destination Profile 1 to dial a number in the United States:

```
Homer-Out Password="Ascend", User-Service=Dialout-Framed-User
     User-Name="Homer",
     Ascend-Dial-Number=31,
     Framed-Protocol=PPP,
     Framed-Address=10.0.100.1,
     Framed-Netmask=255.255.255.0,
     Ascend-Metric=2,
     Framed-Routing=None,
     Ascend-Idle-Limit=30,
     Ascend-PRI-Number-Type=National-Number,
     Ascend-Send-Auth=Send-Auth-PAP,
     Ascend-Send-Secret="password1"
```

Setting up packet filters

You can set up two types of filters on a per-user basis:

- generic filter

  A generic filters examine the byte- or bit-level contents of a packet. It focuses on certain bytes or bits and compare them with a value defined in the filter. To use generic filters effectively, you need to know the contents of certain bytes in the packets you wish to filter. Protocol specifications are usually the best source of such information

  Use the Ascend-Data-Filter attribute to define the data filter in a RADIUS user profile.

  Refer to a data filter defined in a local profile using the Filter-Id attribute.

  Note: You can also refer to a firewall defined by SAM.For more information see "How firewalls work with the Filter-Id RADIUS attribute" on page 4-75

- IP filter

  An IP filter examines higher level fields specific to IP packets. It focuses on known fields, such as source or destination address, protocol number, and so forth. An IP filter operates on logical information that is relatively easy to obtain.

  Use the Ascend-Call-Filter attribute to define a call filter

How packet filters work

You can specify several filters in a RADIUS user profile. Filter entries apply on a first-match basis. Therefore, the order in which you specify filter entries is significant. When you define a filter in a RADIUS user profile, it applies to data the user sends or receives. If you make changes to a filter, the changes do not take affect until a call uses that profile.

A match occurs at the first successful comparison between a filter and the packet being examined. When a comparison succeeds, the filtering process stops and the MAX TNT applies the forward or drop action to the packet.

If no comparisons succeed, the packet does not match the filter. However, the MAX TNT does not forward the packet. When no filter is in use, the MAX TNT forwards all packets. However, once you apply a filter to a connection, this default is *reversed*. For security purposes, the MAX TNT does not automatically forward non-matching packets. It requires a rule that explicitly allows those packets to pass.

In a generic filter, all settings work together to specify a location in a packet and a number that the MAX TNT compares to the value in that location. In an IP filter, the MAX TNT makes a set of distinct comparisons in order. When a comparison fails, the packet goes on to the next comparison. When a comparison succeeds, the filtering process stops and the MAX TNT applies the forward or drop action to the packet. The IP filter tests proceed in the following order:

1. Compare the source address specified by the filter to the source address of the packet. If they are not equal, the comparison fails.
2. Compare the destination address specified by the filter to the destination address in the packet. If they are not equal, the comparison fails.
3. If the protocol specified by the filter is zero (which matches any protocol), the comparison succeeds. If it is non-zero and not equal to the protocol field in the packet, the comparison fails.

4 If the source port specified by the filter does not compare to the source port of the packet as the filter indicates, the comparison fails.

5 If the destination port specified by the filter does not compare to the destination port of the packet as the filter indicates, the comparison fails.

6 If the filter specifies a match only if a TCP session is already established, and a TCP session is up, the comparison succeeds.

Filter entries apply on a first-match basis. Therefore, the order in which you specify filter entries is significant. When a comparison succeeds, the filtering process stops and the MAX applies the forward or drop action to the packet.

If no comparisons succeed, the packet does not match the filter and the MAX does not forward the packet. When no filter is in use the MAX forwards all packets. Once you apply a filter to a connection, this default is reversed. For security purposes, the MAX does not automatically forward non-matching packets. It requires a rule that explicitly allows these packets to pass.

When you define a filter in a user profile, it applies to data the user sends or receives. If you make changes to a filter in a RADIUS user profile, the changes do not take effect until a call uses that profile. For complete information about how filters work, see the MAX *Security Supplement*, and the chapter on using filters in the MAX *ISP and Telecommuting Configuration Guide*.

For more information on filtering, refer to the *Telecommuting and ISP Guide* that came with your MAX unit.

An Ascend unit can also accept RADIUS requests from clients to change filters for a particular session, for a particular user, or for a particular IP address. For details, see“Configuring filter changes” on page 4-77.

Ways to apply packet filters

You can apply a generic or IP filter as either a data filter of a call filter. The sections that follow describe each method.

Data filters for dropping or forwarding certain packets

A data filter defines which packets the MAX TNT can transmit on a connection. Many sites use data filters for security purposes, but you can apply data filters to any purpose that requires the MAX TNT to drop or forward only specific packets. For example, you can use data filters to drop packets addressed to particular hosts or to prevent broadcasts from going across the WAN. You can also use data filters to allow users to access only specific devices across the WAN.

When you apply a data filter, its forward or drop action affects the actual data stream by preventing certain packets from reaching the Ethernet from the WAN, or vice versa (Figure 4-8).

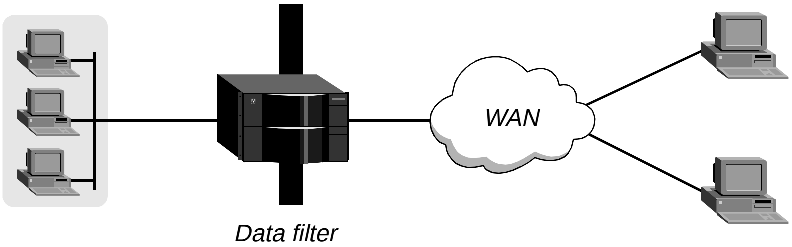

Figure 4-8. Data filters can drop or forward certain packets

Data filters do not affect the idle timer, and a data filter applied to a RADIUS user profile does not affect the answering process.

Call filters for managing connections

A call filter defines which packets can or cannot bring up a connection or reset the idle timer for an established link (Figure 4-9).

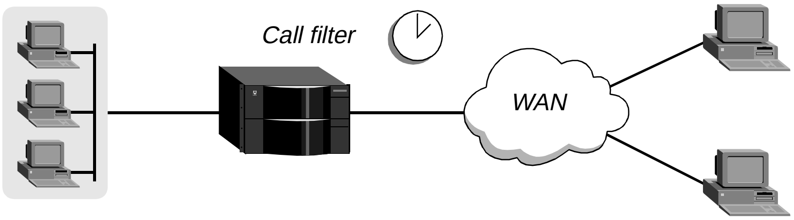

Figure 4-9. Call filters can prevent certain packets from resetting the timer

A call filter prevents unnecessary connections and helps the MAX TNT distinguish active traffic from “noise.” By default, any traffic to a remote site triggers a call, and any traffic across an active connection resets the connection’s idle timer.

When you apply a call filter, its forwarding action does not affect which packets are sent across an active connection. The forwarding action of a call filter determines which packets can initiate a connection or reset a session’s timer. When a session’s idle timer expires, the MAX TNT terminates the session. The idle timer is set to 120 seconds by default, so if a connection is inactive for two minutes, the MAX TNT terminates the connection.

Overview of filter configuration tasks

When you set up filters, you can:

- Set up an IP filter, as described in “Overview of filter configuration tasks” on page 4-66.
- Set up a generic filter, as described in “Configuring a generic filter” on page 4-72.
- Set up a client to request filter changes, as described in “Configuring filter changes” on page 4-77.

Configuring IP filters

Use the following format for an IP data filter entry:

```
Ascend-Data-Filter="ip dir action
[dstip dest_ipaddr\subnet_mask][srcip src_ipaddr\subnet_mask]
[proto [dstport cmp value] [srcport cmp value] [est]]"
```

Use this format for an IP call filter entry:

```
Ascend-Call-Filter="ip dir action
[dstip dest_ipaddr\subnet_mask][srcip src_ipaddr\subnet_mask]
[proto [dstport cmp value] [srcport cmp value] [est]]"
```

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

Table 4-20 describes each element of the syntax. None of the keywords are case sensitive.

Table 4-20.IP filter syntax elements

Keyword or argument	Description
ip	Indicates an IP filter.
dir	Indicates filter direction. You can specify **`in`** (to filter packets coming into the MAX) or **`out`** (to filter packets going out of the MAX).
action	Indicates what action the MAX should take with a packet that matches the filter. You can specify either **`forward`** or **`drop`**.
dstip *dest_ipaddr*	**`dstip`** is a keyword indicating *destination IP address*. The filter applies to packets whose destination address matches the value of ***`dest_ipaddr`***. If a subnet mask portion of the address is present, the MAX compares only the masked bits. If you set ***`dest_ipaddr`*** to 0.0.0.0, or if this keyword and its IP address specification are not present, the filter matches all IP packets.
srcip *src_ipaddr*	**`srcip`** is a keyword indicating *source IP address*. The filter applies to packets whose source address matches the value of ***`src_ipaddr`***. If a subnet mask portion of the address is present, the MAX compares only the masked bits. If you set ***`src_ipaddr`*** to 0.0.0.0, or if this keyword and its IP address specification are not present, the filter matches all IP packets.

Table 4-20.IP filter syntax elements (continued)

Keyword or argument	Description
proto	Indicates a protocol that you can specify as a name or a number. The filter applies to packets whose protocol field matches this value.The supported names and numbers are icmp (1), tcp (6), udp (17), and ospf (89). If you set ***proto*** to 0 (zero), the filter matches any protocol.
dstport *cmp value*	**dstport** is a keyword indicating *destination port*. This argument is valid only when the protocol is tcp (6) or udp (17). If you do not specify a destination port, the filter matches any port. ***cmp*** is an argument indicating how to compare the specified value to the actual destination port. It can have the value <, =, >, or !=. ***value*** can be a number or a name. Supported names and numbers are ftp-data (20), ftp (21), telnet (23), smtp (25), nameserver (42), domain (53), tftp (69), gopher (70), finger (79), www (80), kerberos (88), hostname (101), nntp (119), ntp (123), exec (512), login (513), cmd (514), and talk (517).
srcport *cmp value*	**srcport** is a keyword indicating *source port*. It is valid only when the protocol is tcp (6) or udp (17). If you do not specify a source port, the filter matches any port. ***cmp*** is an argument indicating how to compare the specified value to the actual source port. It can have the value <, =, >, or !=. ***value*** can be a number or a name. Supported names and numbers are ftp-data (20), ftp (21), telnet (23), smtp (25), nameserver (42), domain (53), tftp (69), gopher (70), finger (79), www (80), kerberos (88), hostname (101), nntp (119), ntp (123), exec (512), login (513), cmd (514), and talk (517).
est	If you set this argument to 1, the filter matches a packet only if a TCP session is already established. It is valid only when the ***proto*** specification is tcp (6).

IP filter example

The following profile shows one IP data filter and two generic data filters. Together, these filters specify that the MAX sends out IP and ARP packets, but drops all other packets.

```
Ascend1 Password="Ascend", User-Service=Dialout-Framed-User
     User-Name="Greg",
     Ascend-Dial-Number=555-1234,
     Framed-Address=10.0.200.1,
     Framed-Netmask=255.255.255.0,
     Ascend-Metric=1,
     Framed-Routing=None,
     Ascend-Idle-Limit=20,
     Ascend-Send-Auth=Send-Auth-CHAP,
     Ascend-Send-Secret="kuro",
     Ascend-Data-Filter="ip out forward",
     Ascend-Data-Filter="generic out forward 12 ffff 0806",
     Ascend-Data-Filter="generic out drop 0 0 0"
```

Configuring IPX filters

Use the following format for an IPX data filter entry:

```
Ascend-Data-Filter="ipx <dir> <action>
   [srcipxnet <srcipxnet> srcipxnode <srcipxnode>
   [srcipxsoc <cmp> <value> ]]
   [dstipxnet <dstipxnet> dstipxnode <dstipxnode>
   [dstipxsoc <cmp> <value> ]]
```

Use the following format for an IPX call filter entry:

```
Ascend-Call-Filter="ipx <dir> <action>
   [srcipxnet <srcipxnet> srcipxnode <srcipxnode>
   [srcipxsoc <cmp> <value> ]]
   [dstipxnet <dstipxnet> dstipxnode <dstipxnode>
   [dstipxsoc <cmp> <value> ]]
```

Note: A filter definition cannot contain newlines. The syntax is shown on multiple lines for documentation purposes only.

Table 4-21 lists each keyword and argument.

Table 4-21.IPX filter syntax elements

Syntax element	Description
ipx	Designates an IPX filter.
<dir>	Indicates filter direction. You can specify “in” (to filter packets coming into the MAX) or “out” (to filter packets going out of the MAX).
<action>	Indicates the action the MAX should take with a packet that matches the filter. You can specify either “forward” or “drop”.
srcipxnet	Designates that a source IPX network number appears after this keyword.
<srcipxnet>	Specifies the source IPX network number—the unique internal network number assigned to the NetWare server. You must specify the network number in hexadecimal format. Specifying 0x or 0X is optional.
srcipxnode	Designates that a source IPX node number appears after this keyword.
<srcipxnode>	Specifies the source IPX node number—the node number of the NetWare server. A valid IPX node number must accompany the IPX network number. You must specify the node number in hexadecimal format. Specifying 0x or 0X is optional. The IPX node number 0xffffffffffff is allowed and matches all IPX packets with the same node number.
srcipxsoc	Designates that a source IPX socket number specification appears after this keyword.
<cmp>	Indicates how to compare the socket number specified by <value> to the actual socket number in the packet. The <cmp> argument can have the value <, =, >, or !=.
<value>	Specifies the socket number of the NetWare server. Following the srcipxsoc keyword, the <value> argument specifies the source socket number; following the dstipxsoc keyword, the <value> argument specifies the destination socket number. You must specify the socket number in hexadecimal format. Specifying 0x or 0X is optional.
dstipxnet	Designates that a destination IPX network number appears after this keyword.
<dstipxnet>	Specifies the destination IPX network number—the unique internal network number assigned to the NetWare server. You must specify the network number in hexadecimal format. Specifying 0x or 0X is optional.

Table 4-21.IPX filter syntax elements (continued)

Syntax element	Description
dstipxnode	Designates that a destination IPX node number appears after this keyword.
<dstipxnode>	Specifies the destination IPX node number—the node number of the NetWare server. A valid IPX node number must accompany the IPX network number. You must specify the node number in hexadecimal format. Specifying 0x or 0X is optional. The IPX node number 0xffffffffffff is allowed and matches all IPX packets with the same node number.
dstipxsoc	Designates that a source IPX socket number specification appears after this keyword.

Two IPX filter examples

Dropping outbound IPX packets with specific destination network

The IPX filter specified in the following RADIUS user profile drops all outbound IPX packets with a destination IPX network number of 0x00003823, regardless of the node or socket number. The generic filter that appears after the IPX filter forwards all other packets.

```
st1 Password="st1"
    Ascend-Idle-Limit=300,
    Ascend-Route-IPX=Route-IPX-Yes,
    Ascend-Route-IP =Route-IP-Yes,
    Ascend-IPX-Peer-Mode=IPX-Peer-Router,
    Ascend-Data-Filter="ipx out drop dstipxnet 0x00003823
dstipxnode 0xffffffffffff",
    Ascend-Data-Filter="generic out forward 0 0 0"
```

You should specify a default filter for packets that do not match the filter criteria. In this example, if the specification Ascend-Data-Filter ="generic out forward 0 0 0" did not appear in the profile, the MAX would drop all other IPX, IP, and generic packets.

Dropping outbound IPX packets with specific source network

The IPX filter specified in the following RADIUS user profile drops all outbound IPX packets with a source network number of 0x00000005, a source node number of 00abcde12345, and a source socket number of 0x4002. The generic filter that appears after the IPX filter forwards all other packets.

```
st1 Password = "st1"
    Ascend-Idle-Limit=300,
    Ascend-Route-IPX=Route-IPX-Yes,
    Ascend-Route-IP =Route-IP-Yes,
    Ascend-IPX-Peer-Mode=IPX-Peer-Router,
    Ascend-Data-Filter="ipx in drop srcipxnet 0x00000005
srcipxnode 0x00abcde12345
    00a024cd5807 srcipxsock=0x4002",
    Ascend-Data-Filter="generic out forward 0 0 0"
```

Note: A filter definition cannot contain newlines. The syntax is shown on multiple lines for documentation only.

Configuring a generic filter

Use the following format for a generic data filter entry:

Ascend-Data-Filter="generic *dir action offset mask value compare* **[***more***]"**

Use this format for a generic call filter entry:

Ascend-Call-Filter="generic *dir action offset mask value compare* **[***more***]"**

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

Table 4-22 describes each element of the syntax. None of the keywords are case sensitive.

Table 4-22.Generic filter syntax elements

Keyword or argument	Description
generic	Indicates a generic filter.
dir	Indicates filter direction. You can specify **in** (to filter packets coming into the MAX) or **out** (to filter packets going out of the MAX).
action	Indicates what action the MAX should take with a packet that matches the filter. You can specify either **forward** or **drop**.

Table 4-22.Generic filter syntax elements (continued)

Keyword or argument	**Description**
offset	Indicates the number of bytes masked from the start of the packet. The byte position specified by ***offset*** is called the byte-offset. Starting at the position specified by ***offset***, the MAX applies the value of the ***mask*** argument. A mask hides the part of a number that appears behind the binary zeroes in the mask. For example, if you set ***mask*** to ffff0000 in hexadecimal format, the filter uses only the first 16 binary digits in the comparison, since f=1111 in binary format. The unit then compares the unmasked portion of the packet with the value specified by the ***value*** argument.
mask	Indicates which bits to compare in a segment of the packet. The mask cannot exceed 6 bytes (12 hexadecimal digits). A one-bit in the mask indicates a bit to compare. A zero-bit indicates a bit to ignore. The length of the mask specifies the length of the comparison.
value	Indicates the value to compare to the packet contents at the specified offset in the packet. The length of the value must be the same as the length of the mask. Otherwise, the MAX ignores the filter.
compare	Indicates how the MAX compares a packet's contents to the value specified by ***value***. You can specify == (for Equal) or != (for NotEqual). The default value is Equal.
more	If present, specifies whether the MAX applies the next filter definition in the profile to the current packet before deciding whether to forward or drop the packet. The ***dir*** and ***action*** values for the next entry must be the same as the ***dir*** and ***action*** values for the current entry. Otherwise, the MAX ignores the ***more*** flag.

Generic filter example

In this example, several Macintosh workstations are running Open Transport on the local LAN, and you want only IP traffic destined for the WAN to bring up a connection. To ensure that AppleTalk packets with destinations on the local LAN do not bring up a connection, you must specify several generic call filters.

You must configure a filter to carry out each of the following tasks. Create the filters in the order specified.

1 Drop AppleTalk Address Resolution Protocol (AARP) packets.

This filter specification keeps AARP packets (protocol ID 80f3) from bringing up a connection:

Ascend-Call-Filter="generic out drop 14 ffffffffffffffff aaaa0300000080f3"

2 Forward non-AppleTalk traffic.

AppleTalk has the protocol 809b. This filter specification forwards all non-AppleTalk packets:

Ascend-Call-Filter="generic out forward 14 ffffffffffffffff aaaa03080007809b !="

From this point on, any additional filters deal only with AppleTalk traffic.

3 Drop AppleTalk Echo Protocol (AEP) packets.

This filter specification keeps AEP packets from bringing up a connection.

Ascend-Call-Filter="generic out drop 32 ffffff0000000000 0404040000000000 !="

4 Forward all traffic not destined for an AppleTalk multicast address.

AppleTalk uses a multicast address, rather than a broadcast address. This filter specification forwards all packets not destined for that multicast address:

Ascend-Call-Filter="generic out forward 32 ffffffffffff0000 090007ffffff0000 !="

5 Forward Name Binding Protocol (NBP) lookup packets, but only those that the Chooser makes use of—that is, only those with a wildcard entity name.

This filter specification indicates that the filter forwards NBP packets:

Ascend-Call-Filter="generic out forward 32 ff00fff000000000 0200022000000000 more"

The `more` value in the specification indicates that the MAX must examine the next specification before making the decision to forward a packet. The next specification indicates that the MAX should forward only those packets with a wildcard entity name:

Ascend-Call-Filter="generic out forward 42 ffff000000000000 013d000000000000"

Configuring a RADIUS user profile to use a filter defined on the MAX

If you use Ascend-Data-Filter to define the complete filter policy in a user profile, you must change the filter definition when the filter policy changes. This process can be time-consuming if you must redefine the filters in a number of user profiles. To avoid having to redefine filters, you can set up a filter on the MAX itself, and then refer to that filter in the RADIUS user profile.

The RADIUS attribute Filter-Id (11) in the RADIUS user profile specifies the locally defined data filter or data firewall applied for a user. To assign the same filter or firewall policy to a number of users, you only need to assign the same values to Filter-Id in their RADIUS profiles. If the filter policy changes, you only need to change the reference in the user profile, instead of the entire filter definition.

You can specify several filters in a RADIUS user profile, using the Filter-Id attribute in addition to Ascend-Data-Filter and Ascend-Call-Filter. The way in which filtering works is the same as described in “Setting up packet filters” on page 4-64.

Note: The usage and syntax for Ascend-Data-Filter (and Ascend-Call-Filter) are not modified by Filter-Id.

How firewalls work with the Filter-Id RADIUS attribute

If you specify more than one firewall definition using Filter-Id, only the first firewall definition is applied. If the RADIUS user profile contains a mixture of firewall and filter definitions for Filter-Id, the firewall is applied before any of the filters. The filters are applied after the firewall is applied in the sequence described in "Local filter use example."

If you specify a firewall ID for an undefined firewall, a default firewall definition is loaded that allows Telnet packets but not pings.

Ascend-Data-Filter (and Ascend-Call-Filter) do not provide a way to describe a firewall policy. Their usage and syntax are not modified by Filter-Id.

Filter ID numbering

When you create a data filter, you assign it a number between 0 and 199. The number you enter depends on the whether you are applying a filter you created using the VT100 interface, or a firewall you created using Secure Access Manager (SAM).

If you are applying a filter created using the VT100 interface, enter the filter number as it appears in the Filters menu.

If you are applying a firewall created with SAM, add 100 to the last 2 digits of the firewall number as it appears in the Firewalls menu. For example, if the number of your firewall is 90-601, enter `101`. Refer to your SAM documentation for information on creating firewalls and downloading them to the MAX. The numbering scheme for filters and firewalls is:

- 0 indicates that no filtering is being used (this is the default)
- 1-99 indicates that a filter created using the vt100 interface is being used
- 100-199 indicates that a filter created using SAM is being used.

Local filter use example

After you have created a filter on the MAX, you can refer to it in a RADIUS user profile. The following is an example of two data filter profiles and a RADIUS-defined filter applied to a RADIUS user profile

Assume the following two filter profiles are already set up on the MAX are:

```
Filter-id=6
Name=DisAllowPing
Out filter 01...Valid=Yes
Out filter 01...Type=IP
Out filter 01...Ip...Forward=No
Out filter 01...Ip...Protoco1=6
```

```
Filter-id=9
Name=DisAllowTelnet
Out filter 01...Valid=Yes
Out filter 01...Type=IP
Out filter 01...Ip...Forward=No
Out filter 01...Ip...Protocol=6
Out filter 01...Ip...Src Port Cmp-Eql
Out filter 01...Ip...Src Port #=23
```

The RADIUS user profile is:

```
someuser   Password="ascend"
           User-Service=Framed-User,
           Filter-Id="6",
           Filter-Id="9",
           Ascend-Data-Filter="ip out forward",
           Framed-Protocol=PPP,
           Framed-Address=10.11.1.1,
           Framed-Netmask=255.255.255.0,
           State="p"
```

The first filter is applied, disallowing pings. The second filter disallows Telnet packets. The Ascend-Data-Filter entry allows all IP packets to be forwarded. All pings and Telnet packets will be blocked, but other IP data packets are allowed.

Note: A Telnet directed to another port should be allowed with this configuration.

Firewall example

The following is an example of how Filter-Id can be used to specify a firewall defined in SAM:

1 Create a firewall in the SAM program.

The firewall must block all traffic (including Telnets) except ping traffic.

2 Download the firewall to the MAX and assign a number, for example,

`menu-item 90-101.`

3 Add the following line to the RADIUS profile in the first example:

```
Filter-Id="101"
```

so that the entry reads:

```
someuser   Password="ascend"
           User-Service=Framed-User,
           Filter-Id="101",
           Framed-Protocol=PPP,
           Framed-Address=10.11.1.1,
           Framed-Netmask=255.255.255.0,
          State="p"
```

The user should be able to ping into the MAX, but other packets are dropped, since the firewall is applied before the filters are applied.

Configuring filter changes

An Ascend unit can accept RADIUS requests from clients to change filters for a particular session, for a particular user, or for a particular IP address.

Before you begin

Before you set up RADIUS to accept filter change requests, you must carry out these tasks in the MAX configuration interface:

1 Open the Ethernet menu.

2 Open the Mod Config menu.

3 Open the RADIUS Server menu.

4 Set Server=Yes.

5 To specify the IP address or range of addresses corresponding to devices the MAX permits to make RADIUS requests, set the Client #*n* parameters.

Specify each IP address or range in dotted decimal notation. You designate a range of addresses by entering a subnet specification. The default value is 0.0.0.0. A value of 0.0.0.0 disables the associated client field. At least one of the fields must contain an IP address other than 0.0.0.0 for client support to be active.

For example, can specify values like these:

- Client #1= 125.65.5.0/24. This setting specifies any addresses from the 125.65.5 subnet.
- Client #2= 125.5.0.0/16. This setting specifies any addresses from the 125.5 subnet.
- Client #3= 135.50.248.76/32. This setting specifies the single address of 138.50.248.76.
- Client #4= 198.5.248.76/29. This setting specifies a single address from 198.5.248.72 subnet.
- Client #5= 255.255.255.255. This setting specifies that the RADIUS server can accept requests from any client.

Note: Past releases of the MAX allowed up to three specified clients, with a single server key for all three clients. When you restore configurations with the previous client list, the MAX will assign the default subnet mask of the specified address type to each client, and not the previous 32-bit (single host) address. For example, the MAX will assign the address 128.50.1.1 a subnet mask of 16. In addition, the MAX will not automatically set the Server Key. You must manually set the Server Key for each client.

6 To specify the shared secret between clients and RADIUS, set the Server Key #*n* parameter.

RADIUS uses this key to validate the authenticator on requests and to generate the authenticator on responses. You can enter up to 20 characters. Client #1 and Client #2 share the same key. You can specify a different key for each additional Client #*n* specification.

7 To indicate the UDP port number on which the RADIUS server receives client requests, set the Server Port parameter.

You can enter a number between 1 and 65535. The default value is 1700. Although the value can match the port setting for RADIUS authentication or accounting, we recommend that you specify a different port.

8 To specify whether the client sends a session key to the RADIUS server, set the Session Key parameter.

The session key associates the client request with the user session. You can specify one of these values:

- Yes indicates that the client sends a session key using the Ascend-Session-Svr-Key attribute.
- No indicates that the client does not send a session key. The default value is No.

9 To specify the attributes required to identify a user session when Session Key=Yes, set the Attributes parameter.

You can specify one of these settings:

– Any indicates that the RADIUS server can use any attribute to identify the user session. If the user sends multiple attributes, the RADIUS checks them in this order: Ascend-Session-Svr-Key (session key), Acct-Session-Id (session ID), User-Name (user name), and Framed-IP-Address (IP address).

– Session indicates that the RADIUS server uses only the server key (the value of Ascend-Session-Svr-Key) to identify the session.

– All indicates that all applicable attributes must be sent and pass validation before the client can perform any operation on the connection. For example, if a session has a user name, IP address, session ID, and session key specified, all four attributes must be sent to the RADIUS server and pass validation. However, if a session has a user name, session ID and session key, only these attributes must be sent. The MAX does not require the IP address.

10 Save your changes.

Specifying filter changes in RADIUS

In the RADIUS user profile for the client at the IP address specified by a Client #*n* parameter on the MAX, specify the attributes that the MAX uses to control filter changes. In a RADIUS Change-Filter-Request packet (code 43), the attributes listed in Table 4-23 control filter changes.

Table 4-23.Filter change attributes

Attribute	**Purpose in a Change-Filter-Request packet**
User-Name (1)	The MAX changes the filters for all routing or bridging sessions associated with this user name. If you specify Framed-Address as well, the MAX changes filters only for routing/bridging sessions associated with both attributes. The User-Name attribute can contain up to 252 characters. The default value is null. The string need not be null terminated.
Framed-Address (8)	The MAX changes the filters for all routing or bridging sessions associated with this address. If you specify User-Name as well, the MAX changes filters only for routing/bridging sessions associated with both attributes. The MAX ignores the default address of 0.0.0.0.

Table 4-23.Filter change attributes (continued)

Attribute	Purpose in a Change-Filter-Request packet
Acct-Session-Id (44)	The Acct-Session-Id attribute consists of an ASCII string representing a number between 1 and 2,147,483,647. Each number represents a separate session. The number 1 represents the first session. The MAX ignores numbers outside the valid range. The number you specify must match the session reference number used in SNMP accounting or RADIUS accounting.
Ascend-Data-Filter (242)	Specifies the data filter to use.
Ascend-Call-Filter (243)	Specifies the call filter to use.
Ascend-Session-Svr-Key (151)	Specifies the session key that identifies the user session. You can specify up to 16 characters. The default value is null.

How RADIUS uses Change-Filter-Request packet attributes

The client must supply a session specifier when making a filter change request. This specifier can be the session key specified by Ascend-Session-Svr-Key, the session reference number found in Acct-Session-Id, a user name, or an IP address.

The MAX sends the session key and session reference number on all RADIUS authentication requests. You can also obtain the session key, session reference number, and user name through RADIUS accounting, or from the accounting MIB (for systems that support SNMP accounting). If the MAX assigns the IP address from a pool, you can obtain the address through RADIUS accounting or the accounting MIB as well.

Only Ascend-Data-Filter and Ascend-Call-Filter can appear multiple times.

The MAX silently discards a Change-Filter-Request packet if one of these conditions is true:

- The packet is badly formatted.
- The client is not on the list of clients allowed to send RADIUS requests to the server.
- The authenticator field is incorrect.
- The packet contains invalid attribute values.

If RADIUS found at least one routing/bridging session whose filters it could change, the response code is 44 (Change-Filter-Request-ACK). Otherwise, the code is 45 (Change-Filter-Request-NAK). RADIUS does not return any attributes in the response.

Setting up disconnects

An Ascend unit can accept RADIUS requests from clients to disconnect for a particular session, for a particular user, or for a particular IP address.

Before you begin

Before you set up RADIUS to accept disconnect requests, you must specify settings using the MAX configuration interface. You specify the same basic settings for both filter change requests and disconnect requests. For information on how to carry out this task, see “Before you begin” on page 4-77.

Configuring disconnects in RADIUS

In the RADIUS user profile for the client at the IP address specified by a Client #*n* parameter on the MAX, specify the attributes that the MAX uses for disconnect requests.

When the MAX receives a Disconnect-Request packet (code 40), it disconnects the associated user. The attributes User-Name, Framed-Address, Acct-Session-Id, or Ascend-Session-Svr-Key can identify the user. (For details on these attributes, see Table 4-23 on page 79.) RADIUS ignores all other attributes. In addition, none of the attributes may appear more than once. That is, the client should not specify two different user names with a single request.

How RADIUS uses Disconnect-Request packet attributes

The MAX sends the session key and session reference number on all RADIUS authentication requests. You can also obtain the session key, session reference number, and user name through RADIUS accounting or from the accounting MIB (for systems that support SNMP accounting). If the MAX assigns the IP address from a pool, you can obtain the address through RADIUS accounting or the accounting MIB as well.

The MAX silently discards a Disconnect-Request packet if one of these conditions is true:

- The packet is badly formatted.
- The client is not on the list of clients allowed to send RADIUS requests to the server.
- The authenticator field is incorrect.
- The packet contains invalid attribute values.

If RADIUS found at least one session it could disconnect, the response code is 41 (Disconnect-Request-ACK). Otherwise, the code is 42 (Disconnect-Request-NAK). RADIUS does not return any attributes in the response.

Disconnect example

If two users with the name Steve are logged into the terminal server, a request specifying the name Steve disconnects both. A request specifying the session reference number of the first user disconnects only that user.

If there is a four-channel MP session for user Steve at IP address 11.0.0.1, a request specifying IP address 11.0.0.1 and/or the name Steve disconnects all four channels. A request specifying the session reference number associated with one of the four channels disconnects all channels in the MP session. If the request specifies Steve and an address of 11.0.0.2, the MAX returns a NAK because there is no session Steve with that address.

If there is also a terminal server session for Steve in addition to the four-channel MP session, a request specifying Steve disconnects both. A request specifying Steve and 11.0.0.1 disconnects only the MP session. Likewise, a request specifying 11.0.0.1 disconnects only the MP session.

Setting up multicast forwarding

The MAX implements Internet Group Membership Protocol (IGMP) version-1 and version-2, along with configuration options that enable the MAX to communicate with multicast backbone (MBONE) routers and forward multicast traffic.

The MBONE is a multicast network that provides real-time, two-way audio and video functionality to the Internet. A multicast network is a network in which a router sends packets to all addresses on a subscriber list. This type of network is different from both a unicast network (in which the router sends packets to one user at a time) and a broadcast network (in which the router sends packets to all users, whether they appear on subscription lists or not). The MBONE is a virtual network that actually consists of groups of networks called *islands*. These islands are connected by tunnels and support IP.

Figure 4-10 shows a MAX acting as an MBONE client. The MAX accesses an MBONE network and starts receiving the MBONE multicasts. It resends these multicast packets to all of the clients connected to the MAX for MBONE service. The clients wishing MBONE service must implement IGMP.

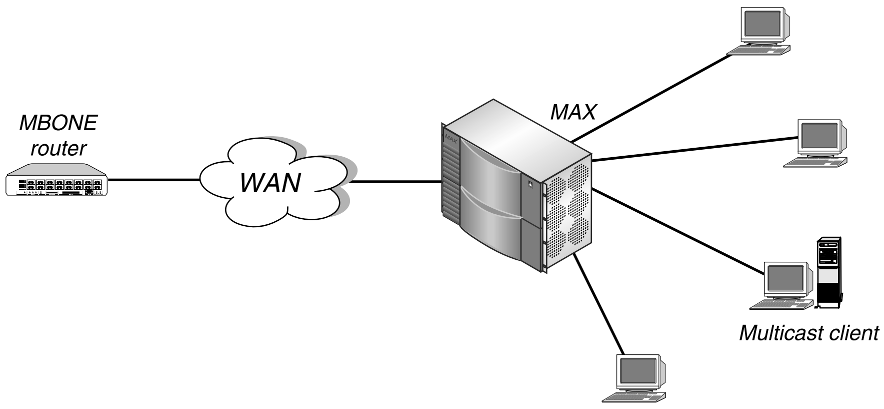

Figure 4-10. The MAX interacting with an MBONE router and multicast clients

To the MBONE network, the MAX appears to be a client, implementing IGMP. To its own clients, the MAX looks like a multicast router, although in fact the MAX simply forwards multicast packets based on group memberships. Each client tells the MAX the multicast address it wants to listen to. To communicate with multicast clients, the MAX sends the clients IGMP queries every 60 seconds, receives responses, and forwards multicast traffic.

The MBONE router can reside on the MAX unit’s Ethernet interface or across a WAN link. If the router resides across a WAN link, the MAX can respond to multicast clients on its Ethernet interface as well as across the WAN.

For complete information on multicast forwarding, see the MAX *ISP and Telecommuting Configuration Guide*.

Before you begin

Before configuring the RADIUS user profile for multicast forwarding, you must set multicast parameters in the Ethernet profile of the MAX configuration interface. For details, see the MAX *ISP and Telecommuting Configuration Guide*.

Configuring multicast forwarding in RADIUS

To configure multicast forwarding in RADIUS, use the attributes listed in Table 4-24.

Table 4-24.Multicast forwarding attributes

Attribute	Description	Possible values
Ascend-Multicast-Client (152)	Specifies whether the user is a multicast client of the MAX.	Multicast-No (0) Multicast-Yes (1) The default value is Multicast-No.
Ascend-Multicast-Rate-Limit (153)	Specifies how many seconds the MAX waits before accepting another packet from the multicast client.	The default value is 100.

To configure a multicast forwarding in a RADIUS user profile, follow these steps:

1. To specify that the user is a multicast client of the MAX, set Ascend-Multicast-Client=Multicast-Yes.
2. To specify how many seconds the MAX waits before accepting another packet from the multicast client, specify a value for Ascend-Multicast-Rate-Limit.

   To prevent multicast clients from creating response storms to multicast transmissions, you configure the user profile to limit the rate at which the MAX accepts packets from clients. Specify an integer. If you set the attribute to 0 (zero), the MAX does not apply rate limiting. The default value is 100. The MAX discards any subsequent packets it receives in the window you configure.

Configuring T-Online for Deutsche Telekom

T-Online is a customized application designed for Deutsche Telekom. You can configure the MAX to work with a ZGR (a piece of older equipment that Deutsche Telekom uses to give clients access to X.25 services) in two ways :

- as a special RADIUS bootup server to load the subaddresses and answer numbers the MAX needs for redirecting calls to a Deutsche Telekom ZGR. The MAX does not use this special server for authentication. See “Setting up a RADIUS bootup server to support a Deutsche Telekom ZGR” on page 4-85.
- as a network switch, redirecting calls to a ZGR that handles T-Online services. (T-Online is Deutsche Telekom’s online service.) See “Setting up a MAX to redirect calls to a ZGR” on page 4-86.

Setting up a RADIUS bootup server to support a Deutsche Telekom ZGR

RADIUS loads ZGR subaddresses by means of a pseudo-user profile. For a unit-specific configuration, the first line has the following format:

```
DirdoSub-unit_name-num Password="Ascend", User-Service=Dialout-
Framed-User
```

where `unit_name` is the system name of the MAX TNT (the name specified by the Name parameter in the System profile) and *num is a* number in a sequential series starting at 1. For a global configuration, the first line has the following format:

```
DirdoSub-num Password="Ascend", User-Service=Dialout-Framed-
User
```

After the first line, you specify one or more ZGR subaddresses by setting the Client-Port-DNIS attribute as many times as necessary.

For example, suppose that a MAX connects to a ZGR, and that you want the MAX to pass to the ZGR ports all calls that provide the subaddresses 1111, 1234, and 1982. For a MAX named Munich1, you would create the following pseudo-user profile:

```
DirdoSub-Munich1-1 Password="Ascend", User-Service=Dialout-
Framed-User
        Client-Port-DNIS="1111",
        Client-Port-DNIS="1234",
        Client-Port-DNIS="1982"
```

Loading ZGR answer numbers

RADIUS loads ZGR answer numbers by means of a pseudo-user profile. For a unit-specific configuration, the first line has the following format:

```
DirdoNum-unit_name-num Password="Ascend", User-Service=Dialout-
Framed-User
```

where `unit_name` is the system name of the MAX TNT (the name specified by the Name parameter in the System profile) and *num is a* number in a sequential series starting at 1.

For a global configuration, the first line has the following format:

```
DirdoNum-num Password="Ascend", User-Service=Dialout-Framed-User
```

After the first line, you specify one or more ZGR answer numbers by setting the Client-Port-DNIS attribute as many times as necessary.

For example, suppose that a MAX connects to a ZGR, and that you want the MAX to pass to the ZGR ports all calls that provide the answer numbers 1111, 1234, and 1982. For a MAX named Munich1, you would create the following pseudo-user profile:

```
DirdoNum-Munich1-1 Password="Ascend", User-Service=Dialout-Framed-User
        Client-Port-DNIS="1111",
        Client-Port-DNIS="1234",
        Client-Port-DNIS="1982"
```

Setting up a MAX to redirect calls to a ZGR

The MAX can act as a network switch, redirecting calls to a ZGR that handles online services. A ZGR is a piece of older equipment that Deutsche Telekom uses to give clients access to X.25 services. You can configure RADIUS to provide the MAX with the necessary ZGR answer numbers and ZGR subaddresses.

Configuring RADIUS with ZGR answer numbers

The MAX uses an answer number to determine whether it should forward a call to a ZGR. If the incoming number matches the answer number, the MAX forwards the call. To specify the ZGR answer numbers in RADIUS, follow these steps:

1. Create the first line of a pseudo-user profile using the User-Name, Password, and User-Service attributes.

   You create a pseudo-user profile to store information that the MAX TNT can query—in this case, to store ZGR answer numbers. You can configure pseudo-users for both global and MAX TNT-specific configuration control of ZGR answer numbers. The MAX TNT adds the unit-specific numbers in addition to the global numbers.

   For a unit-specific configuration, specify the first line of a pseudo-user profile in this format:

   ```
   DirdoNum-unit_name-num Password="Ascend", User-Service=Dialout-Framed-User
   ```

   For a global configuration, specify the first line of a pseudo-user profile in this format:

   ```
   DirdoNum-num Password="Ascend", User-Service=Dialout-Framed-User
   ```

   `unit_name` is the system name of the MAX TNT—that is, the name specified by the name parameter in the System profile. *num* is a number in a sequential series, starting at 1.

2. For each pseudo-user profile, specify one or more ZGR answer numbers using the Client-Port-DNIS attribute.

   The combined total of all the answer numbers you define in pseudo-user profiles cannot exceed 100. This configuration constitutes a new use of Client-Port-DNIS, an attribute generally used for called number authentication.

For example, suppose that a MAX connects to a ZGR, and that you want the MAX to pass all calls that provide the answer numbers 1111, 1234, and 1982 to the ZGR ports. The pseudo-user profile for a MAX named Munich1 looks like this one:

```
DirdoNum-Munich1-1 Password="Ascend", User-Service=Dialout-
Framed-User
        Client-Port-DNIS="1111",
        Client-Port-DNIS="1234",
        Client-Port-DNIS="1982"
```

How the MAX obtains ZGR answer numbers

Whenever you power on the MAX, reset the unit, update the RADIUS configuration with the Upd Rem Cfg command, or update RADIUS from SNMP, the MAX queries RADIUS for the ZGR answer numbers. RADIUS provides the answer numbers in this way:

1. RADIUS looks for profiles having the format DirdoNum-*unit_name*-1, where *unit_name* is the system name.
2. If at least one profile exists, RADIUS loads all existing profiles with the format DirdoNum-*unit_name-num*.

   The variable *num* is a number in a sequential series, starting with 1.
3. The MAX TNT queries for DirdoNum-*unit_name*-1, then DirdoNum-*unit_name*-2, and so on, until it receives an authentication reject from RADIUS.
4. RADIUS loads the global configuration profiles having the form DirdoNum-*num*.
5. The MAX TNT queries DirdoNum-1, then DirdoNum-2, and so on, until it receives an authentication reject from RADIUS.

The MAX caches the answer numbers locally, and uses them to check against the answer numbers of incoming calls. Note that ports 3 and 4 are reserved for outbound connections to the ZGR device.

Configuring RADIUS with ZGR subaddresses

You can configure RADIUS to provide the MAX with the necessary ZGR subaddresses. To specify the ZGR subaddresses in RADIUS, you create a pseudo-user profile to store information that the MAX can query—in this case, to store ZGR subaddresses. You can configure a pseudo-user either for global configuration control of ZGR subaddresses, or for local control of the subaddresses specific to a MAX unit. The MAX adds both the unit-specific configuration and the global subaddresses to its routing table.

To configure the pseudo-user profile, follow these steps:

1. Create the first line using the User-Name, Password, and User-Service attributes.

   For a unit-specific configuration, specify the attributes in this format:

   ```
   DirdoSub-unit_name-num Password="Ascend", User-Service=Dialout-
   Framed-User
   ```

   where *unit_name* is the system name of the MAX (the name specified by the Name parameter in the System profile) and *num* is a number in a sequential series, starting at 1.

   For a global configuration, specify the attributes in this format:

   ```
   DirdoSub-num Password="Ascend", User-Service=Dialout-Framed-User
   ```

2. For each pseudo-user profile, specify one or more ZGR subaddresses by setting the Client-Port-DNIS attribute as many times as necessary.

   The combined total of all the subaddresses you define in pseudo-user profiles must not exceed 100. This configuration constitutes a new use of Client-Port-DNIS, an attribute generally used for called-number authentication.

For example, suppose that a MAX connects to a ZGR, and that you want the MAX to pass all calls that provide the subaddresses 1111, 1234, and 1982 to the ZGR ports. The pseudo-user profile for a MAX named Munich1 would look like this one:

```
DirdoSub-Munich1-1 Password="Ascend", User-Service=Dialout-Framed-User

       Client-Port-DNIS="1111",
       Client-Port-DNIS="1234",
       Client-Port-DNIS="1982"
```

How the MAX obtains ZGR subaddresses

Whenever you power on the MAX, reset the unit, update the RADIUS configuration with the Upd Rem Cfg command, or update RADIUS from SNMP, the MAX queries RADIUS for the ZGR subaddresses. RADIUS provides the subaddresses in the following way:

1. RADIUS looks for profiles having the format DirdoSub-*unit_name*-1, where *unit_name* is the system name.
2. If at least one such profile exists, RADIUS loads all existing profiles that have the format DirdoSub-*unit_name*-*num*. The variable *num* is a number in a sequential series starting with 1.
3. The MAX queries for DirdoSub-*unit_name*-1, then DirdoSub-*unit_name*-2, and so on, until it receives an authentication reject from RADIUS.
4. RADIUS loads the global configuration profiles that have the form DirdoSub-*num*.
5. The MAX queries DirdoSub-1, then DirdoSub-2, and so on, until it receives an authentication reject from RADIUS.

The MAX caches the subaddresses locally, and uses them to check against the subaddresses of incoming calls. Note that ports 3 and 4 are reserved for outbound connections to the ZGR device.

Setting Up Frame Relay in RADIUS

5

This chapter contains:

Using the MAX as a Frame Relay concentrator

In a Frame Relay backbone, every access line must connect directly to a Frame Relay switch. In the past, most connections to the Frame Relay network were relatively high speed, such as full T1 lines at 1.5 Mbps. With recent changes in Frame Relay pricing, you may now want to run low-speed Frame Relay connections rather than analog or ISDN dial-up connections. When you configure the MAX as a Frame Relay concentrator, the MAX concentrates low-speed 56K and 64K connections into one or more high-speed connections to a Frame Relay switch. (Figure 5-1).

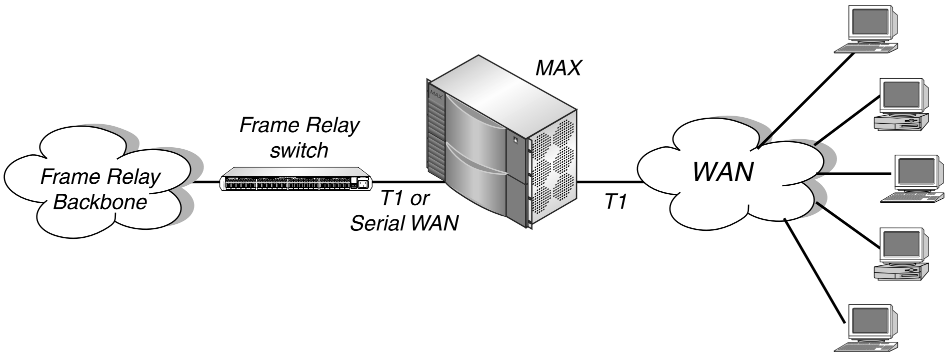

Figure 5-1. The MAX operating as a Frame Relay concentrator

The MAX uses the 8 Mbps serial interface, the T1 PRI line, or the E1 PRI line. Each B-channel on a T1 PRI or E1 PRI line can be a separate Frame Relay connection from a low-speed Frame Relay user. In North America and Japan, a single MAX can concentrate up to 96 low-speed connections. In Europe, the MAX can concentrate up to 120 low-speed connections. If all of the Frame Relay connections are concentrated onto the single 8-Mbps serial interface, the MAX turns a single high-cost Frame Relay port on a traditional Frame Relay switch into approximately 100 operational ports.

For the MAX to operate as a Frame Relay concentrator, it must appear as a Frame Relay switch to both MAX users and other Frame Relay switches (such as those from Cascade or Stratacom). To set up the MAX as a Frame Relay concentrator, you must carry out these tasks:

1. Configure a physical interface to the Frame Relay switch (usually T1 PRI, E1 PRI, or serial WAN).

   For information, see the *MAX ISP and Telecommuting Configuration Guide*.

2. Set up a logical link between the MAX and the Frame Relay switch.

   A RADIUS Frame Relay profile defines each logical link. For information on the basic kinds of links you can configure, see “Types of logical links between the MAX and a Frame Relay switch” on page 5-2. For details on setting up each logical interface, see “Setting up the logical link to a Frame Relay switch” on page 5-7.

3. Create one or more Frame Relay user connections.

   A RADIUS user profile specifies a Data Link Connection Indicator (DLCI) for each user connection. A DLCI is a number between 16 and 991 that the Frame Relay administrator assigns. A DLCI is not an address, but a local label that identifies a logical link between a device and a Frame Relay switch. The switch uses the DLCI to route frames through the network. The DLCI may change as frames pass through multiple switches.

   For information on the types of user connections you can configure, see “Types of Frame Relay user connections” on page 5-4. For details on setting up each user connection, see “Setting up Frame Relay user connections” on page 5-13.

Types of logical links between the MAX and a Frame Relay switch

In a Frame Relay configuration, the MAX can operate as a Customer Premise Equipment (CPE) device, as a Frame Relay switch, or both. Figure 5-2 shows the types of Frame Relay interfaces the MAX supports. All the devices can be Ascend units. The Frame Relay switches can be third-party products as well.

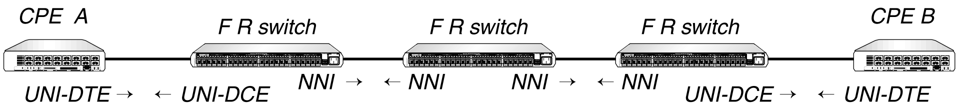

Figure 5-2. Types of logical interfaces to Frame Relay switches

The MAX supports these types of interfaces to the Frame Relay network:

- Network-to-Network Interface (NNI)
- User-to-Network Interface–Data Circuit-Terminating Equipment (UNI-DCE)
- User-to-Network Interface–Data Terminal Equipment (UNI-DTE)

The sections that follow describe each type of interface.

NNI interfaces

An NNI configuration consists of a Frame Relay switch's interface to another Frame Relay switch. This configuration enables separate Frame Relay networks to connect via a common protocol (Figure 5-3).

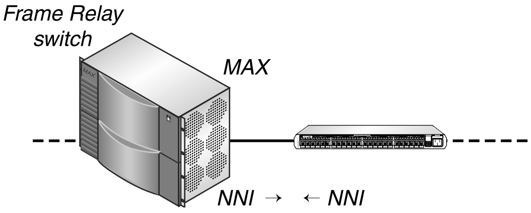

Figure 5-3. NNI interfaces

In this configuration, the MAX acts as a Frame Relay switch, and can perform both DTE and DCE link management.

When it performs DTE link management, the MAX regularly requests updates on the status of the link. The Frame Relay unit at the other end of the link must respond to these requests. Otherwise, the MAX considers the link inactive. Furthermore, if the response to these requests indicates a DLCI failure, the MAX considers the link inactive.

When it performs DCE link management, the MAX expects to get regular requests for the status of the link. If the MAX does not receive these requests within the expected interval, it considers the link inactive. The MAX responds to these requests with the status of the link identified by the DLCI.

For information on setting up a RADIUS Frame Relay profile for an NNI interface, see "Specifying an NNI interface" on page 5-11.

UNI-DCE interfaces

UNI is the interface between a user's CPE and a router or switch on the Frame Relay network. In this configuration, the user equipment is a DTE, and the MAX operates as a DCE. To the DTE, the MAX appears as a Frame Relay network endpoint (Figure 5-4).

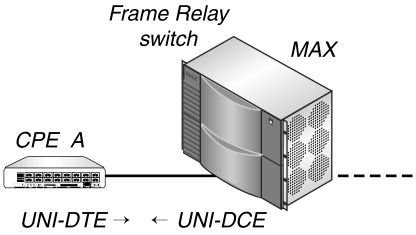

Figure 5-4. UNI-DCE interface

When you set up a MAX in this configuration, it can perform DCE link management functions. For information on setting up a RADIUS Frame Relay profile for a UNI-DCE interface, see "Specifying a UNI-DCE interface" on page 5-12.

UNI-DTE interfaces

In a UNI-DTE connection, the MAX is a DTE communicating with a Frame Relay switch. It acts as a Frame Relay feeder and can perform the DTE functions specified for link management (Figure 5-5).

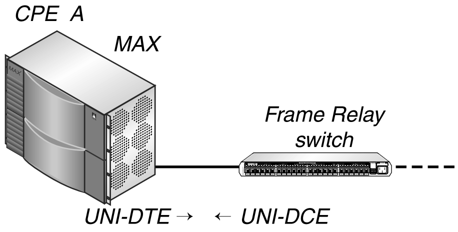

Figure 5-5. UNI-DTE interface

For information on setting up a RADIUS Frame Relay profile for a UNI-DTE interface, see “Specifying a UNI-DTE interface” on page 5-12.

Note: For NNI or UNI-DTE connections, the MAX can query the device at the other end of the link about the status of the DLCIs in the connection. If any of the DLCIs become unusable and the DLCI’s RADIUS user profile specifies a backup connection, the MAX dials the connection. For information on setting up a backup connection, see “Setting up a backup profile for a Frame Relay link” on page 5-22.

Types of Frame Relay user connections

The MAX supports three kinds of Frame Relay user connections:

- Gateway
- Circuit
- Redirect

The sections that follow describe each type of user connection.

Gateway connections

A gateway connection is a bridging or routing link between an endpoint on the Frame Relay network and one of these locations:

- The local network
- A distant network reachable through another Frame Relay switch

Figure 5-6 illustrates a gateway connection.

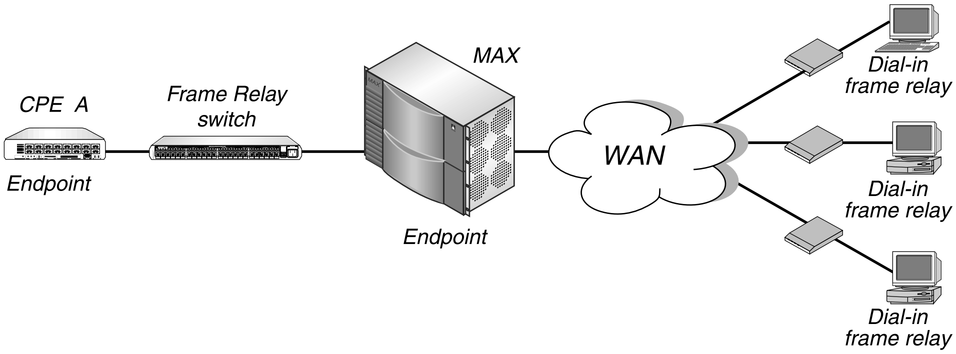

Figure 5-6. Gateway connections

The user endpoint (DTE) sees the MAX as a Frame Relay switch (DCE). The MAX routes a gateway connection to the local network or out to another endpoint on the Frame Relay network.

If the destination address is on a local interface, the MAX routes the packets normally. If the destination address is a remote network reachable through a Frame Relay switch, the MAX encapsulates the packets in Frame Relay (RFC 1490) and forwards the data stream out to the Frame Relay switch using the specified DLCI. The Frame Relay switch uses that DLCI to route the frames to the right destination.

For information on setting up a RADIUS user profile for a gateway connection, see “Configuring a Frame Relay gateway connection” on page 5-15.

Circuit connections

A circuit is a connection that follows a specified path through the Frame Relay switch, as shown in Figure 5-7.

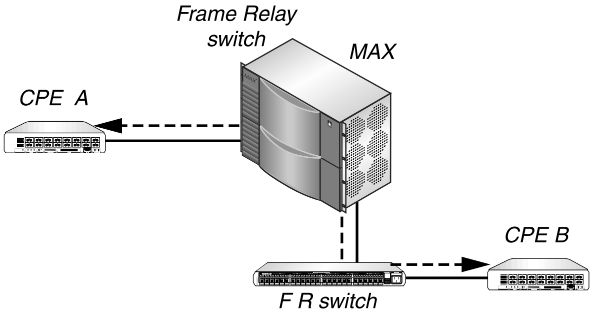

Figure 5-7. Circuit connections

A Permanent Virtual Circuit (PVC) consists of two DLCI endpoints. The MAX switches data coming in one DLCI to the other DLCI. There may be another Frame Relay switch in between, as shown in Figure 5-7, or both endpoints might be able to reach each other directly through the MAX. Bear in mind that circuit connections are switched, not routed.

For information on setting up a RADIUS user profile for a circuit connection, see “Configuring a Frame Relay circuit connection” on page 5-16.

Redirect connections

A redirect connection forwards incoming switched calls that use IP routing, such as regular PPP or MP+ calls, to a Frame Relay switch. (Figure 5-8).

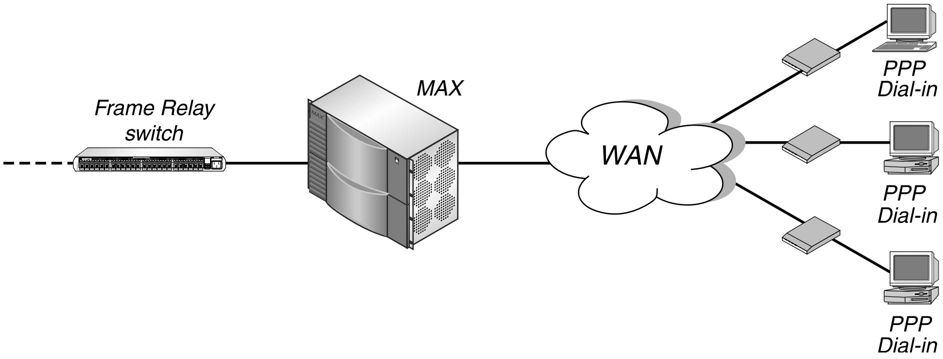

Figure 5-8. Redirect connections

Many redirect connections can use the same DLCI. For that reason, especially when the incoming switched calls are MP+ encapsulated, you must make sure that the nailed-up connection to the Frame Relay switch has sufficient bandwidth to handle multiple concurrent connections.

When the MAX receives IP packets from a caller that has a redirect specified in its local Connection profile or RADIUS user profile, it simply forwards the data stream out to the Frame Relay switch using the specified DLCI, effectively passing on the responsibility of routing those packets to a later hop on the Frame Relay network. The MAX never examines the destination address of redirect packets. This feature enables you to accept traffic from one link and send all traffic to a predetermined destination, eliminating any user concerns over security.

Redirection is not designed for calls that use Frame Relay encapsulation. The redirected call must use IP routing because the MAX must have a way to route data back to the caller. Its method is to use the destination IP address. For the inbound data stream, any type of connection would suffice, because the MAX doesn’t pass the data to its bridge/router. But for the data stream coming back from the Frame Relay network to the caller, the MAX must use the caller’s IP address to distinguish between the multiple connections using the same DLCI.

For information on setting up a redirect connection in a Frame Relay user profile, see “Configuring a Frame Relay redirect connection” on page 5-17.

Setting up the logical link to a Frame Relay switch

You define the link between the MAX and a Frame Relay switch in a RADIUS Frame Relay profile. The MAX accesses the profile at system startup or when you select the Upd Rem Cfg from the Sys Diag menu.

Overview of RADIUS attributes for a Frame Relay profile

To configure a Frame Relay profile in RADIUS, you use the attributes listed in Table 5-1.

Table 5-1. Frame Relay profile attributes

Attribute	Description	Possible values
Ascend-Call-Type (177)	Specifies the type of nailed-up connection in use.	Nailed (1) Nailed/Mpp (2) Perm/Switched (3) The default value is Nailed.
Ascend-Data-Svc (247)	Specifies the type of data service the link uses for outgoing calls.	Switched-Voice-Bearer (0) Switched-56KR (1) Switched-64K (2) Switched-64KR (3) Switched-56K (4) Nailed-56KR (1) Nailed-64K (2) The default value is Switched-56K.
Ascend-FR-DCE-N392 (162)	Specifies the number of errors during Ascend-FR-DCE-N393-monitored events that cause the network side to declare the user side's procedures inactive.	Integer between 1 and 10. The default value is 3.
Ascend-FR-DCE-N393 (164)	Specifies the DCE-monitored event count.	Integer between 1 and 10. The default value is 4.
Ascend-FR-DTE-N392 (163)	Specifies the number of errors during Ascend-FR-DTE-N393-monitored events that cause the network side to declare the user side's procedures inactive.	Integer between 1 and 10. The default value is 3.
Ascend-FR-DTE-N393 (165)	Specifies the DTE-monitored event count.	Integer between 1 and 10. The default value is 4.
Ascend-FR-Link-Mgt (160)	Specifies the type of Frame Relay link management in use for the profile.	Ascend-FR-No-Link-Mgt (0) Ascend-FR-T1-617D (1) Ascend-FR-Q-933A (2) The default value is Ascend-FR-No-Link-Mgt.

Table 5-1. Frame Relay profile attributes (continued)

Attribute	Description	Possible values
Ascend-FR-LinkUp (157)	Indicates whether a link comes up automatically.	Ascend-LinkUp-Default (0) Ascend-LinkUp-AlwaysUp (1) The default value is Ascend-LinkUp-Default.
Ascend-FR-N391 (161)	Specifies the interval at which the MAX requests a Full Status Report.	Integer between 1 and 255. The default is 6.
Ascend-FR-Nailed-Grp (158)	Associates a group of nailed-up channels with the Frame Relay profile.	Integer between 1 and the maximum number of nailed-up channels that your MAX allows. The default value is 1.
Ascend-FR-T391 (166)	Sets up the Link Integrity Verification polling timer.	An integer between 5 and 30. The default value is 10.
Ascend-FR-T392 (167)	Sets up the timer for the verification of the polling cycle— the length of time the unit should wait between Status Enquiry messages. An error results if the MAX does not receive a Status Enquiry message within the number of seconds this attribute specifies.	An integer between 5 and 30. The default value is 15.
Ascend-FR-Type (159)	Specifies the type of Frame Relay connection.	Ascend-FR-DTE (0) Ascend-FR-DCE (1) Ascend-FR-NNI (2) The default is Ascend-FR-DTE.
Framed-MTU (12)	Specifies the maximum number of bytes the MAX can receive in a single packet.	Integer between 128 and 1600. The default value is 1524.
Password (2)	Specifies the password.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Name (1)	Specifies the name of the RADIUS Frame Relay profile.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Service (6)	Indicates whether the link can use framed or unframed services.	Login-User (1) Framed-User (2) Dialout-Framed-User (5) By default, the MAX does not restrict the services that a link can use.

Configuring a RADIUS Frame Relay profile

To set up a Frame Relay profile in RADIUS, follow these steps:

1 Create the first line of a pseudo-user profile using the User-Name, Password, and User-Service attributes.

You create a pseudo-user to store information that the MAX can query—in this case, to store Frame Relay profile information. Specify the first line of a pseudo-user profile in this format:

```
Frdlink-unit_name-unit_id Password="Ascend", User-Service=
Dialout-Framed-User
```

unit_name is the system name of the Ascend unit—that is, the name specified by the Name parameter in the System profile. ***unit_id*** is a unique string identifying this profile.

You must assign IDs in sequence, starting with 1, with no missing numbers. If the numbers are not in sequence, the MAX cannot retrieve them correctly.

2 On the second line, specify the User-Name attribute to indicate the name of the Frame Relay profile.

User connections link up with the Frame Relay profile by indicating the profile name. The name must be unique and cannot exceed 15 characters.

3 To specify that the link consists entirely of nailed-up channels, set Ascend-Call-Type=Nailed.

You can specify Perm/Switched if the Frame Relay switch allows dial-in. However, Frame Relay networks currently have no dial-out connection capability.

4 To specify the group number of the nailed-up channels (or the serial WAN port) to use, set the Ascend-FR-Nailed-Grp attribute.

5 To specify the type of Frame Relay link in use for the profile, set the Ascend-FR-Type attribute.

You can specify one of these values:

– Ascend-FR-DTE (0). This setting indicates a UNI-DTE interface (the default). When you specify this value, the MAX acts as a DTE that can connect to a Frame Relay switch.

– Ascend-FR-DCE (1). This setting indicates a UNI-DCE interface. When you specify this value, the MAX acts as a DCE that can connect to a Frame Relay DTE unit—that is, to the user’s CPE.

– Ascend-FR-NNI (2). This setting indicates an NNI interface. When you specify this value, the MAX can connect to another NNI unit (a Frame Relay switch).

6 To specify whether the link comes up automatically, set the Ascend-FR-LinkUp attribute.

You can specify one of these values:

– Ascend-LinkUp-Default (0). This setting indicates that the link does not come up unless a DLCI brings it up, and that the link shuts down after the last DLCI becomes inactive. This value is the default.

– Ascend-LinkUp-AlwaysUp (1). This setting indicates that the link comes up automatically and stays up even when the last DLCI becomes inactive.

Note: You can start Frame Relay connections using the DO DIAL command. You can drop connections using the DO HANGUP command. DO DIAL brings up a connection. DO HANGUP closes the link and any DLCIs on it. If Ascend-FR-LinkUp=Ascend-LinkUp-AlwaysUp, DO HANGUP brings the link down, but the link automatically restarts. A restart also occurs if a DLCI brings up the link.

7 To specify a data service, set the Ascend-Data-Svc attribute.

8 To specify the link management protocol in use between the MAX and the Frame Relay switch, set the Ascend-FR-Link-Mgt attribute.

You can specify one of these values:

– Ascend-FR-No-Link-Mgt (0). This setting indicates no link management, and is the default. The MAX always considers a link active if no link management functions take place.

– Ascend-FR-T1-617D (1). This setting indicates T1.617 Annex D link management.

– Ascend-FR-Q-933A (2). This setting indicates Q.933 Annex A link management.

If you specify link management for a MAX with a UNI-DTE interface, the MAX regularly requests updates on the status of the link. The Frame Relay unit at the other end of the link must respond to these requests. Otherwise, the MAX considers the link inactive. Furthermore, if the response to these requests indicates a DLCI failure, the MAX considers the link inactive.

If you specify link management for a MAX with a UNI-DCE interface, the MAX expects to get regular requests for the status of the link. If the MAX does not receive these requests within the expected interval, it considers the link inactive. The MAX responds to these status requests with the status of the link identified by the DLCI.

If you specify link management for a MAX with an NNI interface, the MAX regularly requests updates on the status of the link and expects to get regular requests for updates as well. In other words, the MAX performs both DTE and DCE link management functions.

9 If Ascend-FR-Type=Ascend-FR-DCE or Ascend-FR-NNI, set these attributes:

– Ascend-FR-DCE-N392. This attribute specifies the number of errors during Ascend-FR-DCE-N393-monitored events that cause the network side to declare the user side’s procedures inactive. Specify an integer between 1 and 10. The default value is 3. Set this attribute to a value less than Ascend-FR-DCE-N393.

– Ascend-FR-DCE-N393. This attribute indicates the DCE-monitored event count. Specify a number between 1 and 10. The default value is 4. The MAX always considers a link active if the event count does not reach the value of Ascend-FR-DCE-N393.

– Ascend-FR-T392. This attribute indicates the timer for the verification of the polling cycle—the length of time the unit should wait between Status Enquiry messages. Specify a number of seconds between 5 and 30. The default value is 10. The MAX records an error if it does not receive a Status Enquiry within the number seconds this attribute specifies.

None of these attributes apply if Ascend-FR-Type=Ascend-FR-DTE.

10 If Ascend-FR-Type=Ascend-FR-DTE or Ascend-FR-NNI, set these attributes:

– Ascend-FR-N391. This attribute specifies the Full Status polling cycle. It is the interval at which the MAX requests a Full Status Report. Specify an integer between 1 and 255. The default value is 6.

- Ascend-FR-DTE-N392. This attribute specifies the number of errors during Ascend-FR-DTE-N393-monitored events that cause the user side to declare the network side's procedures inactive. Specify an integer between 1 and 10. The default value is 3. Set this attribute to a value less than Ascend-FR-DTE-N393.
- Ascend-FR-DTE -N393. This attribute indicates the DTE-monitored event count. Specify a number between 1 and 10. The default value is 4. The MAX always considers a link active if the event count does not reach the value of Ascend-FR-DTE-N393.
- Ascend-FR-T391. This attribute indicates the Link Integrity Verification polling timer. You can specify a number of seconds between 5 and 30. The default value is 10.

None of these attributes apply if Ascend-FR-Type=Ascend-FR-DCE.

11 To set the maximum data size, set the Framed-MTU attribute.

Sample RADIUS Frame Relay profile configurations

This section shows a sample RADIUS Frame Relay profile configuration for each type of Frame Relay interface—NNI, UNI-DCE, and UNI-DTE.

Specifying an NNI interface

In this example, the MAX has a nailed-up T1 connection to another Frame Relay switch and an NNI interface to that switch. Figure 5-9 shows the sample connection.

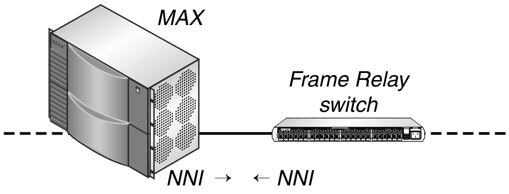

Figure 5-9. NNI interface to another switch

To set up a Frame Relay profile called FR Prof 1 with an NNI interface, enter these specifications:

```
Frdlink-Dial-1 Password="Ascend", User-Service=Dialout-Framed-User
      User-Name="FR Prof 1",
      Ascend-FR-Type=Ascend-FR-NNI,
      Ascend-FR-Nailed-Grp=1,
      Ascend-Data-Svc=Nailed-64K,
      Ascend-FR-LinkUp=Ascend-LinkUp-AlwaysUp,
      Ascend-FR-Link-Mgt=Ascend-FR-T1-617D
```

Specifying a UNI-DCE interface

In this example, the MAX acts as a Frame Relay switch with a UNI-DCE interface to CPE A. Figure 5-10 shows the sample network connection.

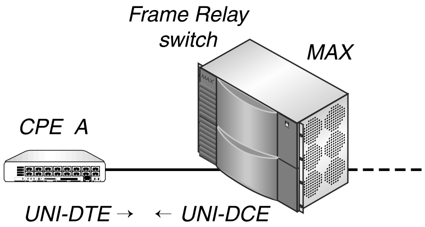

Figure 5-10. UNI-DCE interface to an endpoint (DTE)

To set up a Frame Relay profile called FR Prof 2 with a UNI-DCE interface, enter these specifications:

```
Frdlink-Dial-2 Password="Ascend", User-Service=Dialout-Framed-User
     User-Name="FR Prof 2",
     Ascend-FR-Type=Ascend-FR-DCE,
     Ascend-FR-Nailed-Grp=1,
     Ascend-Data-Svc=Nailed-64K,
     Ascend-FR-LinkUp=Ascend-LinkUp-AlwaysUp,
     Ascend-FR-Link-Mgt=Ascend-FR-T1-617D
```

Specifying a UNI-DTE interface

In this example, the MAX has a nailed-up connection to a Frame Relay switch. The Frame Relay switch has a UNI-DCE interface, and the MAX has a UNI-DTE interface to that switch. Figure 5-11 shows the sample network connection.

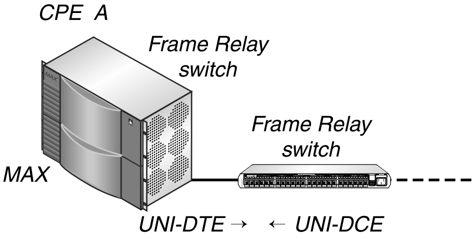

Figure 5-11. UNI-DTE interface to a Frame Relay switch

To set up a Frame Relay profile called FR Prof 3 with a UNI-DTE interface, enter these specifications:

```
Frdlink-Dial-3 Password="Ascend", User-Service=Dialout-Framed-User
     User-Name="FR Prof 3",
     Ascend-FR-Type=Ascend-FR-DTE,
     Ascend-FR-Nailed-Grp=1,
     Ascend-Data-Svc=Nailed-64K,
     Ascend-FR-Link-Mgt=Ascend-FR-T1-617D,
     Ascend-FR-N391=20
```

Setting up Frame Relay user connections

This section describes how to configure each type of Frame Relay user connection—gateway, circuit, and redirect.

Before you begin

Before configuring a RADIUS user profile for a Frame Relay connection, you must perform the following tasks:

1. Make sure there are nailed-up channels available for the link to the Frame Relay switch.
2. Work with the Frame Relay administrator to obtain the DLCIs you need.

   Each gateway connection requires its own DLCI. Several redirect connections can use the same DLCI.
3. For a gateway connection, work with the remote site to find out the required routing/bridging and authentication information.
4. Set Profile Reqd=Yes in the Ethernet > Answer menu.
5. Make sure that the Answer profile enables FR and PPP encapsulation (FR=Yes and PPP=Yes in the Ethernet > Answer > Encaps menu).
6. Configure a Frame Relay profile in RADIUS, following the instructions in “Setting up the logical link to a Frame Relay switch” on page 5-7.

For information on the tasks specific to the MAX configuration interface, see the MAX *ISP and Telecommuting Configuration Guide.*

Overview of RADIUS attributes for a Frame Relay connection

To configure the Frame Relay user connection in RADIUS, use the attributes listed in Table 5-2.

Table 5-2. Frame Relay user profile attributes

Attribute	Description	Possible values
Ascend-FR-Circuit-Name (156)	Indicates the PVC for which this profile is an endpoint.	Text string containing up to 15 characters. The default value is null.
Ascend-FR-Direct (219)	Specifies whether the Ascend unit creates a redirect connection to the Frame Relay switch.	FR-Direct-No (0) FR-Direct-Yes (1) The default value is FR-Direct-No.
Ascend-FR-Direct-DLCI (221)	Specifies the Data Link Connection Indicator (DLCI) for a redirect connection.	Integer between 16 and 991. The default value is 16.
Ascend-FR-Direct-Profile (220)	Specifies the name of the Frame Relay profile that carries the redirect connection to the Frame Relay switch.	Text string containing up to 15 alphanumeric characters. The default value is null.
Ascend-FR-DLCI (179)	Specifies the Data Link Connection Indicator (DLCI) for a gateway or circuit connection.	Integer between 16 and 991. The default value is 16.
Ascend-FR-Profile-Name (180)	Specifies the name of the Frame Relay profile to use in building a gateway or circuit connection.	Text string containing up to 15 alphanumeric characters. The default value is null.
Framed-Protocol (7)	Specifies the type of protocol the link can use.	PPP (1) SLIP (2) MPP (256) EURAW (257) EUUI (258) COMB (260) FR (261) ARA (262) FR-CIR (263) By default, the MAX does not restrict the type of protocol a link can use.
Password (2)	Specifies the user’s password.	Alphanumeric string containing up to 252 characters. The default value is null.

Table 5-2. Frame Relay user profile attributes (continued)

Attribute	**Description**	**Possible values**
User-Name (1)	Specifies the user's name.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Service (6)	Indicates whether the link can use framed or unframed services.	Login-User (1) Framed-User (2) Dialout-Framed-User (5) By default, the MAX does not restrict the services that a link can use.

Configuring a Frame Relay gateway connection

To configure a Frame Relay gateway connection in a RADIUS user profile, follow these steps:

1 Create the first line of a pseudo-user profile using the User-Name, Password, and User-Service attributes.

You create a pseudo-user to store information that the MAX can query—in this case, to store Frame Relay connection information. Specify the first line of a pseudo-user profile in this format:

`Permconn-`*`unit_name`***`-`***`unit_id`* **`Password="Ascend", User-Service=`**
`Dialout-Framed-User`

`unit_name` is the system name of the Ascend unit—that is, the name specified by the Name parameter in the System profile. ***`unit_id`*** is a unique string identifying this profile.

You must assign IDs in sequence, starting with 1, with no missing numbers. If the numbers are not in sequence, the MAX cannot retrieve them correctly.

For example, you might enter this first line in the profile:

Permconn-MAX-1 Password="Ascend", User-Service=Dialout-Framed-User

2 On the second line of the user profile, specify the User-Name attribute to indicate the name of the user that can make the Frame Relay connection.

3 To specify that the MAX uses a gateway link, set Ascend-FR-Direct=FR-Direct-No.

4 To specify the name of the Frame Relay profile that the MAX uses when building the connection, set the Ascend-FR-Profile-Name attribute.

Indicate the name of a Frame Relay profile that connects to the Frame Relay switch handling the DLCI. You can specify up to 15 alphanumeric characters. The default value is null. Make sure that you enter the name exactly as it appears in User-Name attribute on the second line of the Frame Relay profile.

5 To specify the DLCI that identifies the user profile to the Frame Relay switch, set the Ascend-FR-DLCI attribute.

You can specify an integer between 16 and 991. The default value is 16. Enter the DLCI value given to you by your Frame Relay network administrator. Each user profile that specifies a gateway connection is a separate logical link and must have a separate DLCI.

6 Set Framed-Protocol=FR.

This setting indicates Frame Relay encapsulation as specified in RFC 1490, and enables the user to send and receive packets between the MAX unit's bridge/router and a Frame Relay network. The bridge/router is the endpoint of the Frame Relay connection, and processes all packets going to or coming from the Frame Relay link.

7 Configure the routing or bridging setup in the MAX for the WAN connection.

For details, see Chapter 6, "Setting Up Routing and Bridging Links" in this guide, and the relevant chapters of the MAX *ISP and Telecommuting Configuration Guide*.

Configuring a Frame Relay circuit connection

To set up a Frame Relay circuit connection in a RADIUS user profile, follow these steps:

1 Create the first line of a pseudo-user profile using the User-Name, Password, and User-Service attributes.

You create a pseudo-user to store information that the MAX can query—in this case, to store Frame Relay connection information. Specify the first line of a pseudo-user profile in this format:

Permconn-*unit_name-unit_id* **Password="Ascend", User-Service=Dialout-Framed-User**

unit_name is the system name of the Ascend unit—that is, the name specified by the Name parameter in the System profile. ***unit_id*** is a unique string identifying this profile.

You must assign IDs in sequence, starting with 1, with no missing numbers. If the numbers are not in sequence, the MAX cannot retrieve them correctly.

For example, you might enter this first line in the profile:

Permconn-MAX-1 Password="Ascend", User-Service=Dialout-Framed-User

2 On the second line of the user profile, specify the User-Name attribute to indicate the name of the user that can make the Frame Relay connection.

3 To specify the name of the Frame Relay profile that the MAX uses when building the connection, set the Ascend-FR-Profile-Name attribute.

Indicate the name of a Frame Relay profile that connects to the Frame Relay switch handling the DLCI. You can specify up to 15 alphanumeric characters. The default value is null. Make sure that you enter the name exactly as it appears in User-Name attribute on the second line of the Frame Relay profile.

4 To specify the DLCI that identifies the user profile to the Frame Relay switch, set the Ascend-FR-DLCI attribute.

You can specify an integer between 16 and 991. The default value is 16. Enter the DLCI value given to you by your Frame Relay network administrator.

5 Set Framed-Protocol=FR-CIR.

This setting indicates that the Frame Relay link connects to another Frame Relay link handled by the MAX. By linking two DLCI endpoints, the connection creates a Permanent Virtual Circuit (PVC). When you combine them as a circuit, the two DLCI endpoints act as a tunnel—data coming in on one DLCI bypasses the Ascend router and goes out on the other DLCI.

If any one of the DLCIs in a PVC becomes inactive because of disconnect or failure, the PVC using that DLCI becomes inactive. A physical line can carry multiple DLCIs, and the failure of the line causes the failure of all DLCIs it carries.

6 Set Ascend-FR-Circuit-Name to a text string identifying the PVC.

A circuit specification defines two DLCI endpoints of a PVC, with one endpoint specified in each RADIUS user profile (or Connection profile). The MAX requires two profiles for a single PVC. You can use two RADIUS user profiles, two Connection profiles, or one RADIUS user profile and one Connection profile. The two DLCIs can use the same Frame Relay profile or different ones. The two DLCIs must be different.

The MAX connects pairs of links with matching Ascend-FR-Circuit-Name attributes. Therefore, make sure that you specify the exact same name for Ascend-FR-Circuit-Name in each profile.

7 Configure the routing or bridging setup in the MAX for the WAN connection.

For details, see Chapter 6, “Setting Up Routing and Bridging Links” in this guide, and the relevant chapters of the MAX *ISP and Telecommuting Configuration Guide.*

Configuring a Frame Relay redirect connection

To configure a Frame Relay redirect connection in a RADIUS user profile, follow these steps:

1 Create the first line of a pseudo-user profile using the User-Name, Password, and User-Service attributes.

You create a pseudo-user to store information that the MAX can query—in this case, to store Frame Relay connection information. Specify the first line of a pseudo-user profile in this format:

```
Permconn-unit_name-unit_id Password="Ascend", User-Service=
Dialout-Framed-User
```

unit_name is the system name of the Ascend unit—that is, the name specified by the Name parameter in the System profile. ***unit_id*** is a unique string identifying this profile.

You must assign IDs in sequence, starting with 1, with no missing numbers. If the numbers are not in sequence, the MAX cannot retrieve them correctly.

For example, you might enter this first line in the profile:

Permconn-MAX-1 Password="Ascend", User-Service=Dialout-Framed-User

2 On the second line of the user profile, specify the User-Name attribute to indicate the name of the user that can make the Frame Relay connection.

3 To specify that the MAX uses a redirect link, set Ascend-FR-Direct=FR-Direct-Yes.

4 To indicate the name of the Frame Relay profile the MAX uses when building the connection, set the Ascend-FR-Direct-Profile attribute.

Indicate the name of a Frame Relay profile that connects to the Frame Relay switch handling the DLCI. You can specify up to 15 alphanumeric characters. The default value is null. Make sure that you enter the name exactly as it appears in the User-Name attribute on the second line of the Frame Relay profile.

5 To indicate the DLCI that identifies the user profile to the Frame Relay switch, set the Ascend-FR-Direct-DLCI attribute.

You can specify an integer between 16 and 991. The default value is 16. Many redirect connections can use the same DLCI.

6 Set Framed-Protocol=PPP, MP, or MPP.

7 Configure the incoming PPP or MP+ connection as described in “Setting up a PPP connection” on page 4-8 and “Setting up an MP or MP+ connection” on page 4-14.

8 Configure the routing or bridging setup in the MAX for the WAN connection.

For details, see Chapter 6, “Setting Up Routing and Bridging Links” in this guide, and the relevant chapters of the MAX *ISP and Telecommuting Configuration Guide.*

Sample RADIUS Frame Relay user profile configurations

This section shows a Frame Relay user profile for each type of user connection—gateway, circuit, and redirect.

Specifying a gateway connection

Figure 5-12 shows a MAX with three gateway connections to CPEs at remote sites across the Frame Relay network.

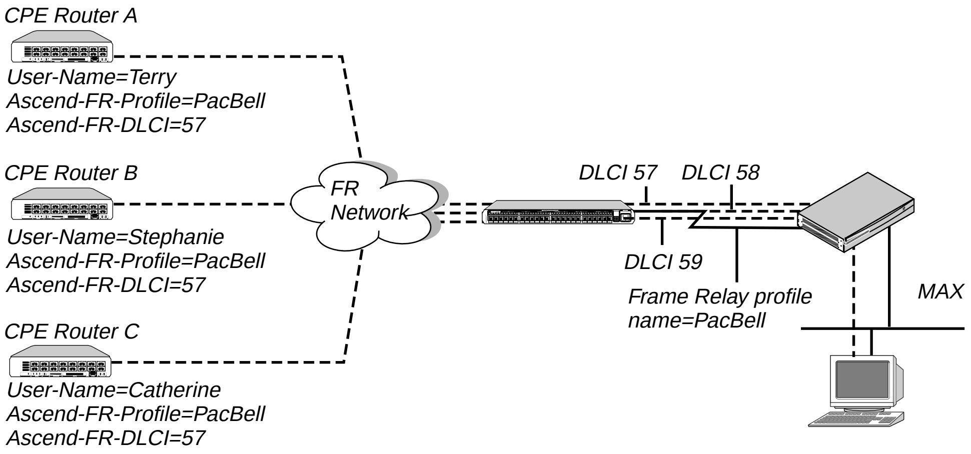

Figure 5-12. Gateway connections to the Frame Relay network

Each connection uses the Frame Relay profile called PacBell with the MAX as a DTE:

```
Frdlink-Dial-1 Password="Ascend", User-Service=Dialout-Framed-
User
   User-Name="PacBell",
   Ascend-FR-Type=Ascend-FR-DTE,
   Ascend-FR-Nailed-Grp=1,
   Ascend-FR-Link-Mgt=Ascend-FR-T1-617D,
   Ascend-FR-N391=20
```

To configure the user profiles, make these settings:

```
Permconn-MAX-1 Password="Ascend", User-Service=Dialout-Framed-
User
   Framed-Protocol=FR,
   User-Name="Terry",
   Ascend-FR-Profile-Name="PacBell",
   Ascend-FR-DLCI=57
```

```
Permconn-MAX-2 Password="Ascend", User-Service=Dialout-Framed-
User
   Framed-Protocol=FR,
   User-Name="Stephanie",
   Ascend-FR-Profile-Name="PacBell",
   Ascend-FR-DLCI=57
Permconn-MAX-3 Password="Ascend", User-Service=Dialout-Framed-
User
   Framed-Protocol=FR,
   User-Name="Catherine",
   Ascend-FR-Profile-Name="PacBell",
   Ascend-FR-DLCI=57
```

Specifying a circuit connection

This example shows the MAX with both a UNI-DCE and an NNI interface. The UNI-DCE interface supports a Frame Relay link to a CPE (a user's workstation). Acting as a Frame Relay switch, the MAX has an NNI interface that supports a link to another Frame Relay switch. Figure 5-13 shows this configuration.

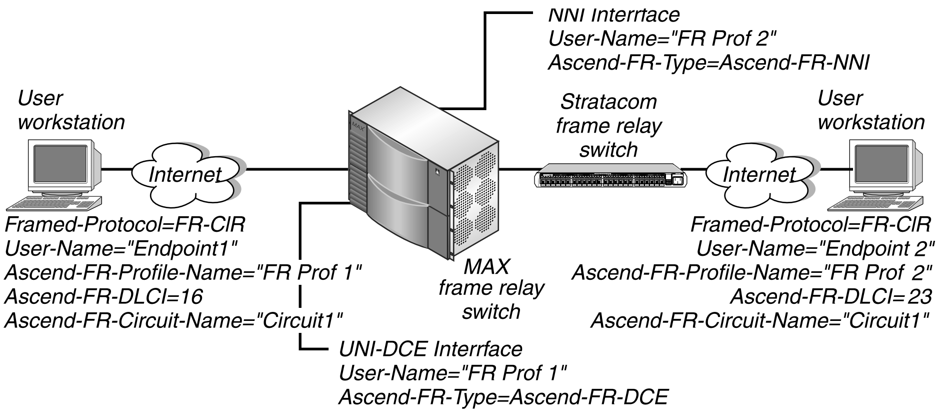

Figure 5-13. The MAX with UNI-DCE and NNI interfaces

This example makes use of two Frame Relay profiles and two Frame Relay user profiles.

One Frame Relay profile specifies the UNI-DCE interface, and the other specifies the NNI interface:

```
Frdlink-Dial-1 Password="Ascend", User-Service=Dialout-Framed-
User
   User-Name="FR Prof 1",
   Ascend-FR-Type=Ascend-FR-DCE,
   Ascend-FR-Nailed-Grp=1,
   Ascend-FR-LinkUp=Ascend-LinkUp-AlwaysUp,
   Ascend-FR-Link-Mgt=Ascend-FR-T1-617D
```

```
Frdlink-Dial-2 Password="Ascend", User-Service=Dialout-Framed-
User
   User-Name="FR Prof 2",
   Ascend-FR-Type=Ascend-FR-NNI,
   Ascend-FR-Nailed-Grp=2,
   Ascend-FR-LinkUp=Ascend-LinkUp-AlwaysUp,
   Ascend-FR-Link-Mgt=Ascend-FR-T1-617D
```

The two Frame Relay user profiles are called Endpoint1 and Endpoint2. The EndPoint1 user profile uses FR Prof 1, and the Endpoint2 user profile uses FR Prof 2:

```
Permconn-MAX-1 Password="Ascend", User-Service=Dialout-Framed-
User
   Framed-Protocol=FR-CIR,
   User-Name="EndPoint1",
   Ascend-FR-Profile-Name="FR Prof 1",
   Ascend-FR-DLCI=16,
   Ascend-FR-Circuit-Name="Circuit1"
Permconn-MAX-2 Password="Ascend", User-Service=Dialout-Framed-
User,
   Framed-Protocol=FR-CIR,
   User-Name="EndPoint2",
   Ascend-FR-Profile-Name="FR Prof 2",
   Ascend-FR-DLCI=23,
   Ascend-FR-Circuit-Name="Circuit1"
```

Setting Framed-Protocol=FR-CIR specifies that the packets the MAX transmits and receives over the link do not go through the MAX unit's bridge/router. Setting the Ascend-FR-Circuit-Name attribute to the same value in both user profiles tells the MAX to pass packets transparently between FR Prof 1 (DLCI 16) and FR Prof 2 (DLCI 23).

Specifying a redirect connection

Figure 5-14 shows two Frame Relay redirect connections. The incoming calls are PPP-encapsulated IP routing connections.

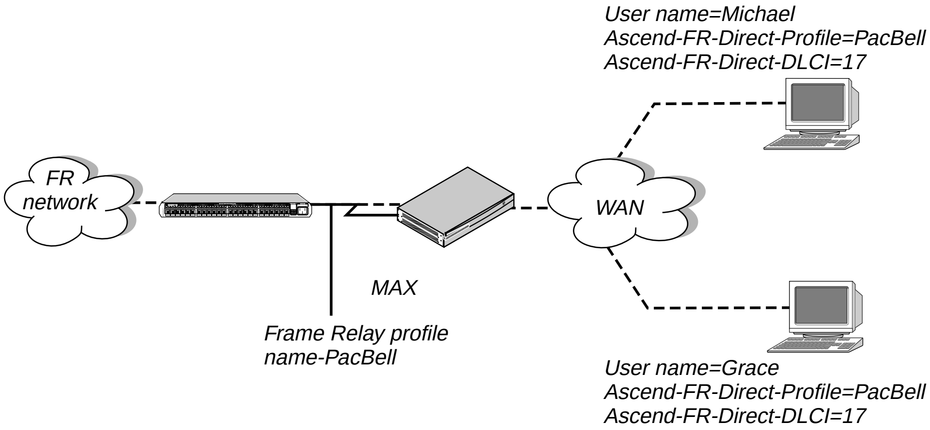
User name=Michael
Ascend-FR-Direct-Profile=PacBell
Ascend-FR-Direct-DLCI=17
FR network
WAN
MAX
Frame Relay profile name-PacBell
User name=Grace
Ascend-FR-Direct-Profile=PacBell
Ascend-FR-Direct-DLCI=17

Figure 5-14. Frame Relay redirect connections

When the MAX receives packets, it doesn't examine the destination address in the packets. The MAX simply forwards the data stream out to the Frame Relay switch on DLCI 17.

Each connection uses the Frame Relay profile called PacBell:

```
Frdlink-Dial-1 Password="Ascend", User-Service=Dialout-Framed-
User
   User-Name="PacBell",
   Ascend-FR-Type=Ascend-FR-NNI,
   Ascend-FR-Nailed-Grp=1,
   Ascend-FR-Link-Mgt=Ascend-FR-T1-617D,
   Ascend-FR-N391=20
```

To set up the user profiles for the redirect connection, enter these specifications:

```
Permconn-MAX-1 Password="Ascend", User-Service=Dialout-Framed-
User
   Framed-Protocol=PPP,
   User-Name="Michael",
   Ascend-FR-Direct-Profile="PacBell",
   Ascend-FR-DLCI=17
Permconn-MAX-2 Password="Ascend", User-Service=Dialout-Framed-
User
   Framed-Protocol=PPP,
   User-Name="Grace",
   Ascend-FR-Direct-Profile="PacBell",
   Ascend-FR-DLCI=17
```

Setting up a backup profile for a Frame Relay link

You can set the Ascend-backup attribute in a Frame Relay user profile to bring up a backup connection when any of the DLCIs become unusable.

For example, consider the Frame Relay configuration in Figure 5-15. The MAX connects to two remote routers, DTE 1 and DTE 2, through the Frame Relay switch. The PVC to DTE 1 consists of DLCIs 34 and 38, while the PVC to DTE 2 consists of DLCIs 33 and 39.

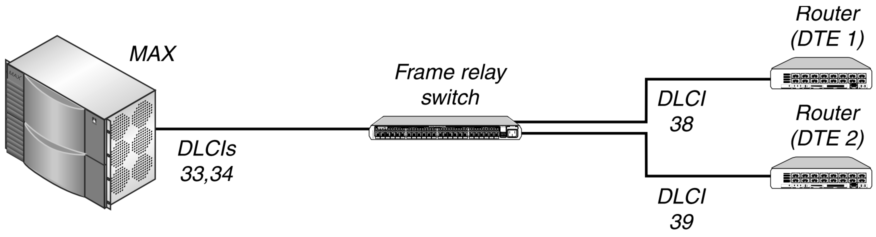

Figure 5-15. Configuring a backup profile for a Frame Relay link

Suppose DTE 2 suddenly becomes unreachable, either because the link between the Frame Relay switch and DTE 2 fails, or because the link between the Ascend unit and the Frame Relay switch fails. In either case, the Ascend unit brings up the backup for DTE 2 (specifically, the backup for the user profile using DLCI 33 or 39).

To set up a backup profile for a Frame Relay link, use the attributes listed in Table 5-3.

Table 5-3. Backup attributes

Attribute	**Description**	**Possible values**
Ascend-backup (176)	Specifies the name of a backup profile for a nailed-up link whose physical connection fails.	Text string. The default value is null.
Ascend-FR-Type (159)	Specifies the type of Frame Relay connection.	Ascend-FR-DTE (0) Ascend-FR-DCE (1) Ascend-FR-NNI (2) The default is Ascend-FR-DTE.
Ascend-Idle-Limit (244)	Specifies the number of seconds the MAX waits before clearing a call when a session is inactive.	Integer between 0 and 65535. The default value is 120. If you accept the default and an existing Answer profile specifies a value for the analogous Idle parameter in the MAX configuration interface, the MAX ignores the Idle value and uses the Ascend-Idle-Limit default.

If the primary connection is a nailed-up link to a Frame Relay switch, follow these steps to configure the unit for backup:

1 In the Frame Relay profile for the primary connection, set Ascend-FR-Type=Ascend-FR-DTE, Ascend-FR-DCE, or Ascend-FR-NNI.

2 In the Frame Relay user profile, set the Ascend-backup attribute to the name of the backup RADIUS user profile.

3 In the backup RADIUS user profile, set the Ascend-Idle-Limit attribute.

When the MAX restores the primary nailed-up connection, it redirects traffic to the link, idling the secondary connection. The MAX releases the secondary connection after the period of time specified by the Ascend-Idle-Limit attribute.

Setting Up Routing and Bridging Links

6

This chapter describes how to configure a RADIUS user profile for IP routing, IPX routing, and bridging connections. The chapter contains:

Setting up a system-based IP routing connection

This section covers the following topics:

- Before you begin
- Introducing system-based IP routing
- Overview of RADIUS attributes for IP routing
- Specifying IP routing and RIP behavior
- Requiring that a caller accept an IP address from the MAX
- Defining a pool of IP addresses for dynamic assignment
- Configuring IP redirection
- Specifying default routes on a per-user basis
- Configuring static IP routes
- Summarizing host routes in an IP address pool

Before you begin

Before you set up system-based IP routing in RADIUS, you must set up the MAX as a router. For details, see the *MAX ISP and Telecommuting Configuration Guide*.

Introducing system-based IP routing

The MAX supports system-based IP routing over PPP, MP, MP+, raw TCP, and frame relay connections. In system-based routing, the entire unit has a single IP address. You can configure IP routing along with IPX routing and protocol-independent bridging. However, you cannot bridge and route TCP/IP packets across the same connection. When you configure the MAX as an IP router, it routes IP packets at the network layer, and does not bridge them at the link layer. The MAX bridges all other protocols, unless you turn off bridging.

The MAX creates a routing table when it powers up. When you power on or reset the MAX, it adds all the routes it knows about to the table, including the following:

- Static routes from MAX IP Route profiles
- Static routes from RADIUS pseudo-user profiles
- Static routes from MAX Connection profiles
- Dynamic routes from Routing Information Protocol (RIP) updates
- Dynamic routes from Open Shortest Path First (OSPF) updates

A static route is a path from one network to another that you define in a profile. A dynamic route is a route that the MAX adds to the routing table based on updates it receives. Routers that use RIP broadcast their entire routing tables every thirty seconds, updating other routers with the most current information. OSPF routers also perform periodic updates.

The MAX cannot read some static routes at power up. These routes do not become part of the routing table until they are up and usable, and include the following:

- Routes you configure in incoming RADIUS user profiles.

  Every RADIUS user profile that specifies an explicit IP address is a static route.
- Host routes to addresses the MAX assigns dynamically from a pool.
- Routes you add using the Iproute Add terminal server command.
- Routes placed in the table by SNMP MIB II.

For complete details about IP routing and the IP routing table, see the *MAX ISP and Telecommuting Configuration Guide*.

Overview of RADIUS attributes for IP routing

Table 6-1 lists the attributes relevant to IP routing.

Table 6-1. IP routing attributes

Attribute	Description	Possible values
Ascend-Assign-IP-Client (144)	Specifies the IP address of an Ascend unit that can use global IP address pools.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0.
Ascend-Assign-IP-Global-Pool (146)	Specifies the global address pool from which RADIUS should assign a user an address.	Text string. The default value is null.
Ascend-Assign-IP-Pool (218)	Specifies the address pool that incoming calls use.	Integer between 1 and 50. The default value is 1.

Table 6-1. IP routing attributes (continued)

Attribute	Description	Possible values
Ascend-Assign-IP-Server (145)	Specifies the IP address of the host running radipad.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0.
Ascend-Client-Gateway (132)	Specifies the default route for IP packets coming from the user on this connection.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0.
Ascend-IP-Direct (209)	Specifies the IP address to which the MAX redirects packets from the user.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0. This setting specifies that the MAX does not perform IP redirection.
Ascend-IP-Pool-Definition (217)	Specifies the first IP address in an IP address pool, and the number of addresses in the pool.	***`num`*** is the number of the pool. The default value is 1. ***`first_ipaddr`*** is the first IP address in the pool. The default value is 0.0.0.0. ***`max_entries`*** is the maximum number of entries in the pool. The default value is 0 (zero).
Ascend-Metric (225)	Specifies the virtual hop count of the route.	Integer between 1 and 15. The default value is 7.
Ascend-Route-IP (228)	Specifies whether the MAX enables IP routing for the user profile.	Route-IP-No (0) Route-IP-Yes (1) The default value is Route-IP-Yes.
Framed-Address (8)	Specifies the IP address of the caller.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0. An answering user profile with this setting matches all IP addresses.
Framed-Netmask (9)	Specify the subnet mask in use for a caller.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0.

Table 6-1. IP routing attributes (continued)

Attribute	Description	Possible values
Framed-Route (22)	Specifies a static IP route for inclusion in the MAX unit's routing table.	***host_ipaddr/subnet_mask*** is the IP address of a host or subnet reached by the route. The default value is 0.0.0.0/0. ***router_ipaddr*** is the IP address of the router at the remote end of the connection. The default value is 0.0.0.0. ***metric*** is the metric for the route. The default value is 8. ***private*** has the value **y** if the route is private, or **n** if it is not private. The default value is **n**. ***profile_name*** is the name of the outgoing user profile that uses the route. The default value is null. ***preference*** is the preference the MAX gives the route. Routes with lower preferences take precedence over routes with large preferences. The default value is 120.
Framed-Routing (10)	Specifies whether the MAX sends RIP packets, receives RIP packets, or both.	None (0) Broadcast (1) Listen (2) Broadcast-Listen (3) Broadcast-v2 (4) Listen-v2 (5) Broadcast-Listen-v2 (6) The default value is None.

Specifying IP routing and RIP behavior

To specify IP routing and RIP behavior for a user profile, follow these steps:

1 Specify the User-Name and Password attributes, authentication attributes, and WAN connection attributes.

For details on setting the User-Name, Password, and authentication attributes, see Chapter 3, "Setting Up RADIUS Authentication." For details on setting up WAN connection attributes, see Chapter 4, "Setting Up WAN Connections in RADIUS."

2 To turn on IP routing for the user profile, set Ascend-Route-IP=Route-IP-Yes.

3 To specify the caller's IP address, set the Framed-Address attribute (and, optionally, the Framed-Netmask attribute).

RADIUS can authenticate an incoming call by matching its IP address to one specified in the RADIUS user profile. In addition, if the remote end requires an IP address on an outgoing call, and does not assign one dynamically, you must specify it in the user profile.

Every Connection profile and RADIUS user profile that specifies an explicit IP address is a static route.

Note: The most common cause of trouble in establishing an IP connection is incorrect configuration of the IP address or subnet specification for the remote host or calling device.

4 To specify RIP behavior for the profile, set the Framed-Routing attribute.

You can specify one of these values:

– None (0) indicates that the MAX does not send or receive RIP updates.

  None is the default. Many sites turn off RIP on the WAN interface in order to avoid storing very large local routing tables. If you turn off RIP, the MAX does not listen to RIP updates across the connection. To route to other networks through that connection, the MAX must rely on static routes you specify in a pseudo-user profile. For details, see "Configuring static IP routes" on page 6-15.

– Broadcast (1) indicates that the MAX sends RIP version 1 updates, but does not receive them.

– Listen (2) indicates that the MAX receives RIP version 1 updates, but does not send them.

– Broadcast-Listen (3) indicates that the MAX both sends and receives RIP version 1 updates.

– Broadcast-v2 (4) indicates that the MAX sends RIP version 2 updates, but does not receive them.

– Listen-v2 (5) indicates that the MAX receives RIP version 2 updates, but does not send them.

– Broadcast-Listen-v2 (6) indicates that the MAX both sends and receives RIP version 2 updates.

If you enable RIP to both send and receive RIP updates on the WAN interface, the MAX broadcasts its routing table to the remote network and listens for RIP updates from that network. Gradually, all routers on both networks have consistent routing tables (all of which may become quite large).

5 Because routers send RIP updates every 30 seconds, you should configure WAN connections that use RIP in one of these ways:

– Set the Ascend-Idle-Limit attribute set to a value less than 30, as described in "Specifying a time limit and idle connection attributes" on page 4-57.

– Apply a call filter for RIP updates on the WAN by setting the Ascend-Call-Filter attribute, as described in "Configuring IP filters" on page 4-67.

If you don't carry out one of these tasks, the connection never disconnects, because RIP traffic resets the idle timer.

6 To specify the virtual hop count of the route, set the Ascend-Metric attribute.

If there are two routes available to a single destination network, you can ensure that the MAX uses any available nailed-up channel before using a switched channel. Simply set the Ascend-Metric attribute to a value higher than the metric of any nailed-up route. The higher the value you enter, the less likely that the MAX will bring the link online. The MAX uses the lowest metric.

For example, if a route to a station takes three hops over nailed-up lines, and Ascend-Metric=4 in a user profile that reaches the same station, the MAX does not bring the user's link online. However, if the link is already online, the MAX does not use the nailed-up line.

Host-to-router connection example

When a device connecting to the MAX is a host running PPP dial-in software, the MAX adds a host route to its routing table and functions as an IP router between its local and WAN interfaces.

A host route connection enables the dial-in host to keep its own IP address when logging into the MAX IP network. For example, in Figure 6-1, if a PC user telecommutes to one IP network and uses an ISP on another IP network, one of those connections can assign an IP address and the other can configure a host route to the PC.

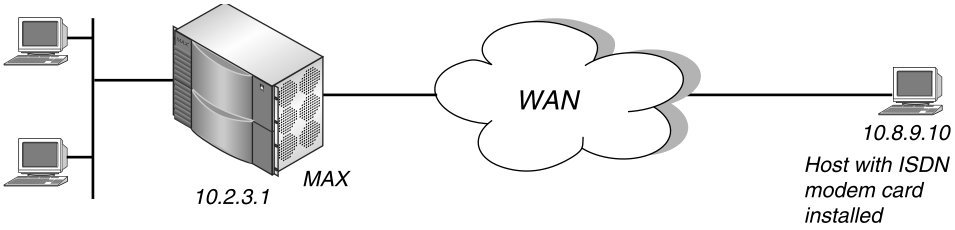

Figure 6-1. Host-to-router IP connection

In this example, the PC is running PPP software and the TCP/IP stack and has an ISDN modem card. The PPP software includes settings like these:

```
Username=Emma
Accept Assigned IP=N/A (or No)
IP address=10.8.9.10
Netmask=255.255.255.255
Default Gateway=N/A (or None)
Name Server=10.7.7.1
Domain suffix=abc.com
VAN Jacobsen compression ON
```

You set up the RADIUS user profile in this way:

```
Emma Password="m2dan", User-Service=Framed-User
     Framed-Protocol=PPP,
     Ascend-Route-IP=Route-IP-Yes,
     Framed-Address=10.8.9.10,
     Framed-Netmask=255.255.255.255,
     Framed-Routing=None,
     Ascend-Metric=2,
     Framed-Compression=Van-Jacobson-TCP-IP,
     Ascend-Idle-Limit=20
```

Router-to-router connection example

When the device connecting to the MAX is an IP router that belongs to an IP network, the connection results in a route to that remote network or subnet. In this example, the MAX is connected to a corporate IP network and needs a switched connection to another company that has its own IP configuration. Figure 6-2 shows the network diagram.

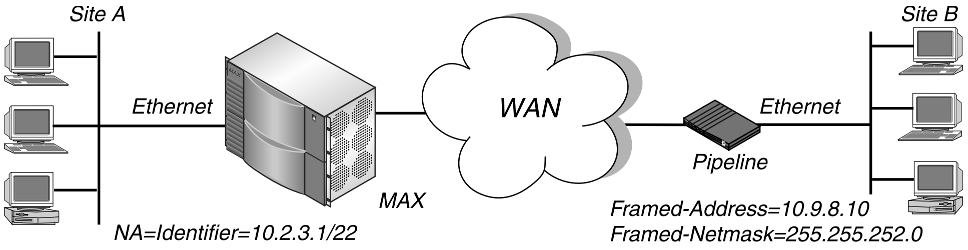

Figure 6-2. A router-to-router IP connection

To configure the site A MAX for a connection to site B, set up the RADIUS user profile in this way:

```
PipelineB Password="m2dan", User-Service=Framed-User
          Framed-Protocol=MPP,
          Ascend-Route-IP=Route-IP-Yes,
          Framed-Address=10.8.9.10,
          Framed-Netmask=255.255.252.0,
          Framed-Routing=Broadcast,
          Ascend-Metric=2,
          Framed-Compression=Van-Jacobson-TCP-IP,
          Ascend-Idle-Limit=20
```

Requiring that a caller accept an IP address from the MAX

To require that a caller accept an IP address from the MAX, follow these steps:

1 To specify that the MAX try to assign an IP address to a calling device, set Assign Adrs=Yes in the Ethernet > Answer menu.

The MAX asks the device to accept an assigned address. The address can be a static address or a dynamic address.

– Static address

You specify a static address using the LAN Adrs parameter in a Connection profile or by the Framed-Address attribute in a RADIUS user profile.

– Dynamic address

A dynamic address comes from the pool of addresses set by the Pool #*n* Start and Pool #*n* Count parameters in the MAX configuration interface, by the Ascend-IP-Pool-Definition attribute in RADIUS, or both. An IP address pool you set up in RADIUS overrides an IP address pool you set up in the MAX configuration interface only if you designate the two pools by the same number.

If the calling end accepts the IP address, the MAX sets the LAN Adrs parameter (in a Connection profile) or Framed-Address attribute (in a RADIUS user profile) to the assigned address. If a static address is already set in a Connection profile or RADIUS user profile, it overrides any IP address from an IP address pool.

Note: In some TCP/IP implementations, when the workstation needs the MAX to set the IP address, you must set the workstation's address to 0.0.0.0. Setting the address to any other value tells the workstation to use that value and notify the MAX.

2 To require a calling station to accept an IP address from the MAX, set Pool Only=Yes in the Ethernet>Mod Config>WAN Options menu.

This setting requires the calling station to accept a static address (specified in a Connection profile or RADIUS user profile), or a dynamic address. If the calling station rejects the assignment, the MAX ends the call.

If you set Pool Only=No, the MAX accepts the IP address the caller specifies.

3 In the RADIUS user profile, configure a static address or specify an IP address pool from which users will receive IP addresses.

To configure a static IP address, set the Framed-Address and Framed-Netmask attributes. To configure an IP address pool and specify the pool an incoming caller should use, follow the instructions in "Defining a pool of IP addresses for dynamic assignment" on page 6-8.

Defining a pool of IP addresses for dynamic assignment

When the device connecting to the MAX is a host running PPP dial-in software, the MAX adds a host route to its routing table. If the host belongs to its own IP network, the MAX must have a Connection profile or RADIUS user profile stating the host's address and using a 32-bit subnet mask. If the host does *not* belong to an IP network, the MAX can add it to the local IP network by assigning a local address from a designated pool of addresses. You can designate a pool of addresses on the MAX or in RADIUS.

A pool is a range of contiguous IP addresses on your local network. The MAX chooses an address from these pools and assigns it to an incoming call when Assign Adrs=Yes in the Ethernet > Answer menu, or when the calling station requests an address assignment. Assigning an address to a device is called performing dynamic IP. Dynamic IP can apply when the calling end is a station. However, if the calling end is a router, that router usually rejects attempts to perform dynamic IP.

By default, each MAX handles dynamic IP address allocation individually from a pool of addresses pre-assigned to each MAX. However, you can also set up your system to allocate IP addresses to callers from a global pool of addresses among many units.

If you need to define more than ten pools of addresses, you must use RADIUS. An IP address pool you set up in RADIUS overrides an IP address pool you set up in the MAX configuration interface only if you designate the two pools by the same number.

When you assign a pool of addresses, make sure that you do not include addresses that are in use. Although the MAX will inform you of a configuration error if you try to specify a pool whose addresses overlap or conflict with an existing pool, it does not have an automatic protection against including an address in a pool that is already in use elsewhere. If you allocate IP addresses on a separate IP network or subnet, other IP hosts on the local network need to know about the route to that new network or subnet.

Before you begin

Before you create IP address pools in RADIUS, you must perform these tasks using the MAX configuration interface:

1 To specify that the MAX try to assign an IP address to a calling device, set Assign Adrs=Yes in the Ethernet > Answer menu.

2 To require calling stations to accept an IP address from the MAX, set Pool Only=Yes in the Ethernet > Mod Config > WAN Options menu.

If the calling station rejects the assignment, the MAX ends the call.

For details on how these parameters work with RADIUS, see “Requiring that a caller accept an IP address from the MAX” on page 6-7.

Configuring MAX-specific IP address pools in RADIUS

To define MAX-specific pools of IP addresses for dynamic assignment to callers, follow these steps:

1 Create the first line of a RADIUS pseudo-user profile using the User-Name, Password, and User-Service attributes.

You create a pseudo-user to store information that the MAX can query—in this case, in order to store IP address pool information. Specify the first line of a pseudo-user profile in this format:

`Pools-`*`unit_name`* **`Password="Ascend", User-Service=Dialout-Framed-User`**

`unit_name` is the system name of the MAX—that is, the name specified by the Name parameter in the System profile.

2 To define one or more address pools, set the Ascend-IP-Pool-Definition attribute.

The Ascend-IP-Pool-Definition attribute has this format:

`Ascend-IP-Pool-Definition="`*`num first_ipaddr max_entries`***`"`**

Table 6-2 describes each Ascend-IP-Pool-Definition argument.

Table 6-2. Ascend-IP-Pool-Definition arguments

Argument	Description
num	Indicates the number of the pool. The default value is 1. Specify pool numbers starting with 1, unless you have defined pools in the MAX interface using the Pool #*n* Start and Pool #*n* Count parameters and do not wish to override these settings. In this case, for the ***num*** argument, specify the highest number of an address pool on the MAX + 1. For example, if you have set up address pools 1 through 5 on the MAX, specify pool numbers starting with 6 in RADIUS.
first_ipaddr	Specifies the first IP address in the address pool. The address you indicate should not accept a subnet mask, because it always becomes a host route. The default value is 0.0.0.0.
max_entries	Specifies the maximum number of IP addresses in the pool. The MAX assigns addresses sequentially, from ***first_ipaddr*** on, up to the limit of addresses specified by ***max_entries***. The default value is 0 (zero).

3 In each RADIUS user profile requiring dynamic addressing for dial-in users, set the Ascend-Assign-IP-Pool attribute to specify the address pool from which RADIUS should assign each user an address.

If you set Ascend-Assign-IP-Pool=0, RADIUS chooses an address from any pool that has one available.

Do not set the Framed-Address attribute. If you do, the MAX requires the caller to use the static IP address the attribute specifies.

MAX-specific address pools example

Figure 6-3 shows a MAX connected to a dial-in host with a modem and PPP software. The remote host requests a dynamic IP address, and the MAX provides one.

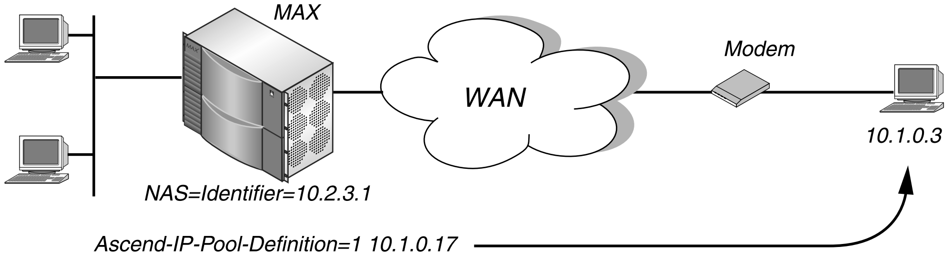

Figure 6-3. An IP routing connection with a dial-in host requiring dynamic IP addressing

The RADIUS pseudo-user file contains the IP pool definitions. In this example, you create two IP address pools for the MAX to use. Address pool #1 contains a block of 7 IP addresses from

10.1.0.1 to 10.1.0.7. Address pool #2 contains a block of 48 IP addresses from 10.2.0.1 to 10.2.0.48.

```
Pools-MAX Password="Ascend", User-Service=Dialout-Framed-User
    Ascend-IP-Pool-Definition="1 10.1.0.1 7",
    Ascend-IP-Pool-Definition="2 10.2.0.1 48"
```

In the user profile, the host requests an address from address pool #1:

```
Emma Password="m2dan", User-Service=Framed-User
     Framed-Protocol=PPP,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Metric=2,
     Framed-Routing=None,
     Ascend-Assign-IP-Pool=1
```

Configuring global IP address pools shared by several MAX units

To define global IP address pools that several MAX units share, follow these steps:

1 Install radipad, as described in “Installing radipad for global IP pools” on page 2-3.

2 Create the first line of a pseudo-user profile called Radipa-Hosts in this format:

```
Radipa-Hosts Password="Ascend", User-Service=Dialout-Framed-User
```

You create a pseudo-user to store information that the MAX can query—in this case, in order to store the IP addresses of Ascend units that can use global IP pools, and the IP address of the host running radipad. The RADIUS daemon reads this pseudo-user profile before connecting to the host running radipad.

3 For the Ascend-Assign-IP-Client attribute, specify the IP address of an Ascend unit that can use global IP address pools.

The default value is 0.0.0.0. You can specify multiple instances of this attribute. At present, the MAX does not use the list of radipad client units. If no Ascend-Assign-IP-Client attribute is present, the list of client units defaults to those present in the RADIUS clients file.

4 For the Ascend-Assign-IP-Server attribute, specify the IP address of the host running radipad.

The default value is 0.0.0.0. Only one instance of this attribute can appear in the profile. The default value is a place-holder only. You must specify a valid IP address for radipad to work.

5 Create the first line of another RADIUS pseudo-user profile using this format:

Global-Pool-*name* **Password="Ascend", User-Service=Dialout-Framed-User**

name is a designation for any class of users you want to define.

6 To define one or more address pools, set the Ascend-IP-Pool-Definition attribute.

The Ascend-IP-Pool-Definition attribute has this format:

Ascend-IP-Pool-Definition="*num first_ipaddr max_entries***"**

For information on each Ascend-IP-Pool-Definition argument, see Table 6-2 on page 6-10.

7. In each RADIUS user profile requiring dynamic addressing for dial-in users, set the Ascend-Assign-IP-Global-Pool attribute to specify the global address pool from which RADIUS should assign each user an address.

   Specify the name of the pseudo-user profile containing the global IP pool definitions. The Ascend unit tries to allocate an address from the pools in order, and chooses an address from the pool with the first available IP address.

   Do not set the Framed-Address attribute. If you do, the MAX will require the caller to use the static IP address the attribute specifies.

At startup, the MAX syslog notes RADIUS requests to release any RADIUS-allocated IP addresses. Some versions of the RADIUS server timeout the request, resulting in one of these log messages:

```
RADIUS release global-pool address

RADIUS release all global-pool addresses
```

Global IP pools example

In this example, two MAX units are connected to several dial-in clients. The global IP pool configuration consists of these elements:

- A pseudo-user profile containing the IP address of the host running radipad
- A pseudo-user profile contains the global IP pool definitions
- A user profile containing a pointer to the pseudo-user profile containing the pool definitions

In this example, radipad is running on a host at IP address 10.4.0.1. The Radipa-Hosts pseudo-user profile looks like this one:

```
Radipa-Hosts Password="Ascend", User-Service=Dialout-Framed-User
    Ascend-Assign-IP-Server=10.4.0.1
```

The global pools pseudo-user profile looks like this one:

```
Global-Pool-CA Password="Ascend", User-Service=Dialout-Framed-User
    Ascend-IP-Pool-Definition="1 10.1.0.1 7",
    Ascend-IP-Pool-Definition="2 10.2.0.1 48"
    Ascend-IP-Pool-Definition="3 10.3.0.1 49"
```

The profile creates three global IP address pools for the MAX units to use. Address pool #1 contains a block of 7 IP addresses from 10.1.0.1 to 10.1.0.7. Address pool #2 contains a block of 48 IP addresses from 10.2.0.1 to 10.2.0.48. Address pool #3 contains a block of 49 addresses from 10.3.0.1 to 10.3.0.49.

In the user profile, the user requests an address from a pool specified in the Global-Pool-CA pseudo-user profile:

```
Emma Password="m2dan", User-Service=Framed-User
     Framed-Protocol=PPP,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Metric=2,
```

Framed-Routing=None,

```
Ascend-Assign-Global-IP-Pool=Global-Pool-CA
```

Configuring IP redirection

You can configure a RADIUS user profile to automatically redirect incoming IP packets to a specified host on the local IP network. When you specify IP redirection, the MAX bypasses all internal routing and bridging tables, and simply sends all packets it receives on a connection’s WAN interface to the specified IP address. IP redirection does not affect outbound packets.

To set up IP redirection, follow these steps:

1. Specify the User-Name and Password attributes, authentication attributes, and WAN connection attributes.

   For details on setting the User-Name, Password, and authentication attributes, see Chapter 3, “Setting Up RADIUS Authentication.” For details on setting up WAN connection attributes, see Chapter 4, “Setting Up WAN Connections in RADIUS.”

2. To specify the caller’s IP address, set the Framed-Address attribute (and, optionally, the Framed-Netmask attribute).

3. Set Ascend-Route-IP=Route-IP-Yes.

4. Set Ascend-Bridge=Bridge-No.

5. Set Ascend-IP-Direct to the IP address to which the MAX redirects packets from the user.

   For example, to specify that the MAX redirects packets to IP address 10.2.3.11, specify this setting:

   Ascend-IP-Direct=10.2.3.11

6. Set Framed-Routing=None.

   Ascend-IP-Direct connections typically turn off RIP. If you configure the connection to receive RIP, the MAX keeps all RIP packets from the remote end and forwards them to the IP address you specify.

7. Ensure that Framed-Protocol is not set to COMB or FR.

Note: Do not set Ascend-IP-Direct and Ascend-FR-Direct in the same user profile. If you do, an error occurs.

IP direct example

This example shows IP redirection specified for a PPP link.

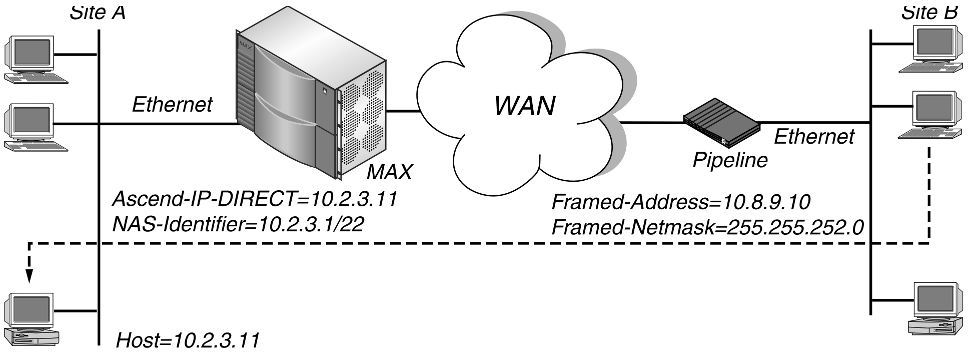
Site A
Site B
Ethernet
MAX
WAN
Pipeline
Ethernet
Ascend-IP-DIRECT=10.2.3.11
NAS-Identifier=10.2.3.1/22
Framed-Address=10.8.9.10
Framed-Netmask=255.255.252.0
Host=10.2.3.11

Figure 6-4. Directing incoming IP packets to one local host

In Figure 6-4, the MAX redirects incoming packets from site B to the host at IP address 10.2.3.11. The user profile looks like this one:

```
Emma Password="m2dan", User-Service=Framed-User
     Framed-Protocol=PPP,
     Framed-Address=10.8.9.10,
     Framed-Netmask=255.255.252.0,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Bridge=Bridge-No,
     Ascend-IP-Direct=10.2.3.11,
     Ascend-Metric=2,
     Framed-Routing=None,
     ...
```

Specifying default routes on a per-user basis

You can specify the default route for IP packets coming from a user in each RADIUS user profile. When you do so, the MAX routes IP packets in this way:

1. The MAX consults its routing table to find a next-hop address.
2. If the next hop is the default route for the system (destination 0.0.0.0), the Ascend unit uses the per-user default address as a next hop instead of the system-wide default route.

   The unit also uses the per-user default if the normal routing logic fails to find a route and there is no system-wide default route.

This feature applies to routing all packets the MAX receives on an interface using a given profile, regardless of the specific IP source address. Therefore, you can use this feature when the profile belongs to another access router and all hosts behind that router use the default gateway. The MAX unit handles packets from other users or from the Ethernet normally. In addition, this feature does not alter the global routing table.

To configure a per-user route, follow these steps:

1. Configure the RADIUS user profile with a User-Name and Password on the first line.
2. On the second or succeeding lines, set the Ascend-Client-Gateway attribute to the IP address of the next hop router.

   Enter the IP address in dotted decimal notation. The default value is 0.0.0.0. If you accept this value, the Ascend unit routes packets as specified in the routing table, using the system-wide default route if it cannot find a more specific route.

   The Ascend unit must have a direct route to the address you specify. The direct route can take place via a profile or an Ethernet connection. If the Ascend unit does not have a direct route, it drops the packets on the connection. When you diagnose routing problems with a profile using this feature, an error in a per-user gateway address is not apparent from inspection of the global routing table.

For example, if you specify Ascend-Client-Gateway=10.0.0.3 in the profile "Berkeley", IP packets from the user with destinations through the default route go through the router at 10.0.0.3.

Configuring static IP routes

A static route is a path from one network to another. This path specifies the destination network and the router to use to get to that network. For routes that must be reliable, you can configure more than one path, in which case the MAX chooses the route to use based on an assigned metric.

A dynamic route can overwrite a static route to the same network if the dynamic route’s metric is lower than that of the static route. However, dynamic routes age. If the MAX does not receive updates for a route, the route eventually expires. In this case, the hidden static route reappears in the routing table.

In RADIUS, you can create a static route in one of two ways:

- In a pseudo-user profile containing one or more explicit routes
- In a user profile specifying a WAN connection

When the MAX has a RADIUS user profile that defines a static route to the same destination as one of the MAX unit’s IP Route profiles or a RADIUS pseudo-user profile, the metric in the RADIUS user profile overrides the metric in the other profiles, but only when the RADIUS user connects.

For example, suppose a MAX has a static route to network 1.10.1.10 with a metric of 10. A user profile in RADIUS has a metric of 7 in a static route to the same network. When the route is not connected, the MAX routing table indicates that the route has a metric of 10. When the route is connected, the MAX routing table indicates that the route has a metric of 7, with an `r` in the flags column to indicate that the route came from RADIUS. Furthermore, the old route with a metric of 10 remains in the routing table, with an asterisk (*) in the flags column, indicating that it is a hidden route.

Specifying static IP routes in a pseudo-user profile

When you disable RIP in a RADIUS user profile (Framed-Routing=None), the MAX does not listen to RIP updates across that connection. To route to other networks through that connection, the MAX must rely on static routes you define in a RADIUS pseudo-user profile.

If you configure the MAX with a subnet address on a backbone network using the IP Adrs parameter in the Ethernet>Mod Config>Ether Options menu, you must set up a static route to the backbone router on the main network. If you do not, the MAX can only see the subnets to which it directly connects.

You cannot create static routes for dynamically assigned IP addresses, because the actual route to those addresses changes with each dynamic assignment.

To set up static IP routes in a RADIUS pseudo-user profile, follow these steps:

1 Create the first line of a pseudo-user profile using the User-Name, Password, and User-Service attributes.

You create a pseudo-user profile to store information that the MAX can query—in this case, in order to store IP routing information. You can configure pseudo-users for both global and MAX-specific configuration control of IP dialout routes. The MAX adds the unit-specific dialout routes in addition to the global dialout routes.

For a unit-specific IP dialout route, specify the first line of a pseudo-user profile in this format:

```
Route-unit_name-num Password="Ascend", User-Service=Dialout-Framed-
User
```

For a global IP dialout route, specify the first line of a pseudo-user profile in this format:

```
Route-num Password="Ascend", User-Service=Dialout-Framed-User
```

unit_name is the system name of the MAX—that is, the name specified by the Name parameter in the System profile. ***num*** is a number in a sequential series, starting at 1.

2 For each pseudo-user profile, specify one or more routes using the Framed-Route attribute.

The Framed-Route attribute has this format:

```
Framed-Route="host_ipaddr[/subnet_mask] router_ipaddr
metric [private] [profile_name][preference]"
```

You should limit each profile to about 25 routes—that is, you should specify up to 25 settings for the Framed-Route attribute. The MAX fetches information from each pseudo-user profile in order to initialize its routing table.

Table 6-3 describes each Framed-Route argument.

Table 6-3. Framed-Route arguments

Syntax element	Description
host_ipaddr/*subnet_mask*	Indicates the IP address of the destination host or subnet reached by the route. The default value is 0.0.0.0/0. If the address includes a subnet mask, the remote router specified by ***router_ipaddr*** is a router to that subnet, rather than to a whole remote network. To specify the entire remote network, do not specify a subnet mask.
router_ipaddr	Specifies the IP address of the router at the remote end of the connection. The default value is 0.0.0.0. The 0.0.0.0 address is a wildcard entry the MAX replaces with the caller’s IP address. When RADIUS authenticates a caller and sends the MAX an Access-Accept message with a value of 0.0.0.0 for ***router_ipaddr***, the MAX updates its routing tables with the Framed-Route value, but substitutes the caller’s IP address for the router. This setting is especially useful when RADIUS cannot know the IP address of the caller because the IP address comes from an address pool.
metric	Indicates the metric for the route. If the MAX has more than one possible route to a destination network, it chooses the one with the lower metric. The default value is 8.
private	Specifies **y** if the route is private, or **n** if it is not private. If you specify that the route is private, the MAX does not disclose the existence of the route when queried by RIP or another routing protocol. The default value is **n**.
profile_name	Indicates the name of the outgoing user profile that uses the route. The default value is null.
preference	Specifies the preference that the MAX gives the route.

Whenever you power on or reset the MAX, or when you select the Upd Rem Cfg command from the Sys Diag menu, RADIUS adds IP dialout routes to the routing table in this way:

1. RADIUS looks for profiles having the format Route-***unit_name***-1, where ***unit_name*** is the system name.
2. If at least one profile exists, RADIUS loads all existing profiles with the format Route-***unit_name***-***num*** to initialize the IP routing table.

The variable ***num*** is a number in a sequential series, starting with 1.

3 The MAX queries Route-***unit_name***-1, then Route-***unit_name***-2, and so on, until it receives an authentication reject from RADIUS.

4 RADIUS loads the global configuration profiles.

These configurations have the format Route-***num***.

5 The MAX queries Route-1, then Route-2, and so on, until it receives an authentication reject from RADIUS.

Static IP route configuration example

The network diagram in Figure 6-5 shows a remote network that does not have its own Connection profile or RADIUS user profile, but can be reached through an existing RADIUS user profile.

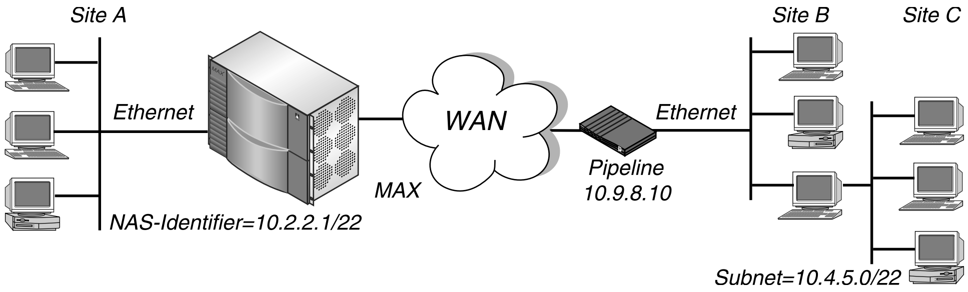

Figure 6-5. A two-hop connection that requires a static route when RIP is off

In Figure 6-5, if RIP is disabled in the RADIUS user profile for site B, the MAX must have a static route like this one to route to site C:

```
Route-1 Password="Ascend", User-Service=Dialout-Framed-User
        Framed-Route="10.4.5.0/22 10.9.8.10 1 n inu-out"
```

Specifying static IP routes in a dial-in user profile

Every Connection profile and RADIUS user profile that specifies an explicit IP address is a static route. For details on creating an implicit static route in a dial-in profile, see “Specifying IP routing and RIP behavior” on page 6-4.

In addition, you might wish to update the MAX unit’s routing tables when connecting to a user whose profile specifies User-Service=Framed-User. In this case, you can set the Framed-Route attribute in an incoming user profile to specify the user’s IP address and subnet mask with the ***host_ipaddr*** and ***/subnet_mask*** arguments. The route you specify in this manner exists only during the time the call is online. However, when you enter a nonzero router address for the ***router_ipaddr*** argument that is different from the caller’s address, the static route of a dial-in framed-user persists even after the connection goes offline.

Summarizing host routes in an IP address pool

By default, the MAX adds dynamically assigned IP addresses to the routing table as individual host routes. However, to reduce the size of routing table advertisements, you can summarize the entire pool. When you do so, the router advertises a single route for the network you define in an address pool, rather than individual host routes for each address. The MAX routes packets to a valid host address, and rejects packets with an invalid host address.

Before you begin

Before setting up the pool summary feature in RADIUS, set Pool Summary=Yes in the Ethernet > Mod Config > WAN Options menu.

Configuring host route summaries in RADIUS

To set up the pool summary feature, follow these steps:

1 Using the Ascend-IP-Pool-Definition attribute, make sure that each and every address pool is network aligned.

For an address pool to be network aligned, these conditions must apply:

– The first address in the pool must be the first host address.

The value ***first_ipaddr*** – 1 determines the network alignment—that is, the zero address on the subnet. ***first_ipaddr*** specifies the first IP address in the pool for the Ascend-IP-Pool-Definition attribute.

– The maximum number of entries you specify with the ***max_entries*** argument of Ascend-IP-Pool-Definition must be two less than the total number of addresses in the pool.

The value ***max_entries*** + 2 determines the total number of addresses in the subnet. You can calculate the subnet mask based on this total.

For example, suppose you have this specification for Ascend-IP-Pool-Definition:

Ascend-IP-Pool-Definition="1 10.12.253.1 62"

Because ***first_ipaddr***=10.12.253.1, the network alignment address is 10.12.153.0 (***first_ipaddr*** – 1).

Because ***max_entries***=62, you must specify a subnet mask for 64 addresses (***max_entries*** + 2). The subnet mask for 64 addresses is 255.255.255.192. (Note that 256–64=192). The Ascend notation for a 255.255.255.192 subnet mask is /26.

The resulting address pool network is 10.12.253.0/26. This address and subnet mask become the first values you specify for the Framed-Route attribute in step 3.

For instructions on setting up address pools, see “Defining a pool of IP addresses for dynamic assignment” on page 6-8.

2 Create the first line of a pseudo-user profile containing static routes using the User-Name, Password, and User-Service attributes.

You can configure pseudo-users for both global and MAX-specific configuration control of IP routes. The MAX adds the unit-specific routes in addition to the global routes.

For a unit-specific IP route, specify the first line of a pseudo-user profile in this format:

```
Route-unit_name-num Password="Ascend", User-Service=Dialout-
Framed-User
```

For a global IP route, specify the first line of a pseudo-user profile in this format:

```
Route-num Password="Ascend", User-Service=Dialout-Framed-User
```

unit_name is the system name of the MAX—that is, the name specified by the name parameter in the System profile. ***num*** is a number in a sequential series, starting at 1.

3. For each Framed-Route attribute, specify the host address and subnet mask for a summarized address pool.

   The Framed-Route attribute has this format:

   ```
   Framed-Route="host_ipaddr[/subnet_mask] router_ipaddr
   metric [private] [profile_name][preference]"
   ```

   For the ***host_ipaddr*** argument, specify the address of the summarized network. For the ***subnet_mask*** argument, specify the associated subnet mask.

4. For the ***router_ipaddr*** argument, specify the router address for each summarized network.

   Because the MAX creates a host route for every address assigned from the pools, and because host routes override subnet routes, the MAX routes packets whose destination matches an assigned IP address from the pool. However, because the MAX advertises the entire pool as a route, and only privately knows which IP addresses in the pool are active, a remote network might improperly send the MAX a packet to an inactive IP address.

   The router address handles all IP addresses not assigned to users. When the MAX receives a packet whose IP address matches an unused IP address in a pool, it either returns the packet to the sender with an ICMP reject message, or simply discards the packet.

   To enable the router to handle packets with destinations to invalid hosts on the summarized network, you must specify one of these internal interfaces as the ***router_ipaddr*** argument.

   – The reject interface (rj0)

     The reject interface has an IP address of 127.0.0.2. When you specify this address as the router to the destination pool network, the MAX rejects packets to an invalid host on that network, appending an ICMP host unreachable message.

   – The black-hole interface (bh0)

     The black-hole interface has an IP address of 127.0.0.3. When you specify this address as the router to the destination pool network, the MAX silently discards packets to an invalid host on that network.

5. Set the ***metric*** argument to 0.
6. Set the ***private*** argument to **n** for No.
7. Set the ***profile_name*** argument to the name of the pseudo-user profile.
8. If you want to specify a preference other than the default value of 120, set the ***preference***.

For example, to set up a static route for address pool network 10.12.253.0/26 with a reject interface, enter this setting in a pseudo-user profile called Summary:

```
Framed-Route="10.12.253.0/26 127.0.0.2 0 n Summary 130"
```

Setting up an interface-based IP routing connection

All Ascend products implement system-based routing, in which the entire unit has a single IP address. For systems that have a single backbone connection, system-based routing is the simplest way to configure the MAX.

An alternative form of routing is called interface-based routing. With interface-based routing, each physical or logical interface on the unit has its own IP address. In some situations, it is useful to number some of the interfaces— in other words, to have the MAX operate partially as a system-based router and partially as an interface-based router. Reasons for using numbered interfaces include troubleshooting nailed-up point-to-point connections and forcing routing decisions between two links going to the same final destination. More generally, interface-based routing allows the MAX to operate more as a multi-homed Internet host behaves.

You can now configure each link in RADIUS as numbered (interface-based) or unnumbered (system-based). If no interfaces are numbered, the MAX operates as a purely system-based router.

If a MAX is using a numbered interface, you should be aware of these features:

- IP packets that the MAX generates and sends to the remote address have an IP source address corresponding to the numbered interface, not to the default (Ethernet) address of the MAX.
- During authentication of a call the MAX places using a numbered interface, the MAX reports the address of the interface as its IP address.
- The MAX adds all numbered interfaces listed in Connection profiles and RADIUS user profiles to its routing table.
- The MAX accepts IP packets whose destination is a numbered interface listed in a Connection profile or a RADIUS user profile, considering them to be destined for the MAX itself.

  The packet may actually arrive over any interface, and the numbered interface corresponding to the packet's destination address need not be in the active state.

Before you begin

Before you carry out the tasks outlined in this section, be sure to set up the WAN connection, specifying system-based IP routing attributes. For information on configuring a WAN connection, see Chapter 4, "Setting Up WAN Connections in RADIUS." For information on configuring system-based IP routing, see "Setting up a system-based IP routing connection" on page 6-1.

Overview of RADIUS attributes for interface-based routing

Table 6-4 lists the RADIUS attributes you set for interface-based routing.

Table 6-4. RADIUS attributes for interface-based routing

Attribute	Description	Possible values
Ascend-IF-Netmask (153)	Specifies the subnet mask in use for the local numbered interface.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0.
Ascend-PPP-Address (253)	Specifies the IP address of the MAX as reported to the calling unit during PPP IPCP negotiations.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0.

Table 6-4. RADIUS attributes for interface-based routing (continued)

Attribute	**Description**	**Possible values**
Ascend-Remote-Addr (154)	Specifies the IP address of the link's remote interface to the WAN.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0.

Configuring interface-based routing in RADIUS

This section provides some guidelines on configuring interface-based routing in RADIUS.

If both the system and interface addresses are known

If you are adding interface-based routing to a MAX with system-based routing already configured, follow these steps:

1. To specify the IP address of the MAX, set the Ascend-PPP-Address attribute.
2. To specify the subnet mask in use for the local interface, specify the Ascend-IF-Netmask attribute.
3. To specify the remote interface address, set the Ascend-Remote-Addr attribute.

When you save these specifications and the MAX is running, these events take place:

1. The MAX generates host routes to both Framed-Address and Ascend-Remote-Addr.

   The Ascend-Remote-Addr appears in the routing table as the next hop to Framed-Address.
2. The MAX generates a route the remote system's subnet, showing the Ascend-Remote-Addr value as the next hop.
3. An incoming PPP, MP, or MP+ call must report its IP address as the Ascend-Remote-Addr attribute (rather than the Framed-Address attribute)—that is, the caller must be using a numbered interface, and its interface address must agree with the Ascend-Remote-Addr value on the receiving side.

If you want to create static routes to hosts at the remote end, you can use the Ascend-Remote-Addr or Framed-Address value as the next hop (gateway) field.

If only the interface address is known

You can omit the remote side's system address from the profile and use interface-based routing exclusively. If the remote system is on a backbone network that the administrator may periodically reconfigure, you might want to refer to the remote system only by its interface address. Follow these steps:

1. To specify the IP address of the MAX, set the Ascend-PPP-Address attribute.
2. To specify the subnet mask in use on the local interface, set the Ascend-IF-Netmask attribute.
3. Accept the default address of 0.0.0.0 for the Ascend-Remote-Addr attribute.

   Note that the Framed-Address attribute must always have a value, so if the only known address is the interface address, specify it using the Framed-Address attribute rather than the Ascend-Remote-Addr attribute.

If the Framed-Address attribute specifies the remote system address, the following events take place:

1. The MAX creates a host route to Framed-Address.
2. The MAX creates a route to the subnet of the remote interface.
3. An incoming PPP, MP, or MP+ call must report its IP address as Framed-Address.

If you do not specify the remote interface address

If interface-based routing is in use and the local interface is numbered, the remote address will usually be known. In practice, administrators at both sites must agree upon the subnet. It is possible, but not recommended, to number the local interface, omitting the interface address of the remote site and using only its system address. In this case, do not use the remote interface address in any static routes.

When a local interface is numbered but no corresponding remote interface address exists, the remote interface must have an address on the same subnet as the local, numbered interface. RADIUS rejects incoming PPP calls if the user profile numbers the local interface and the remote caller supplies an address not on the same subnet.

Setting up an IPX routing connection

This section covers the following topics:

- Before you begin
- Introducing IPX routing
- Overview of RADIUS attributes for IPX routing
- Specifying IPX routing
- Configuring static IPX routes

Before you begin

Before you set up an IPX routing connection in RADIUS, carry out these tasks in the MAX configuration interface:

1 Set up the MAX as a router.

2 In the Ethernet > Answer > PPP Options menu, set the Recv Auth parameter to PAP, CHAP, MS-CHAP, or Either.

Unlike an IP routing configuration, in which the MAX uniquely identifies the calling device by its IP address, an IPX routing configuration does not include a built-in way to uniquely identify callers. For this reason, you must use PAP, CHAP, or MS-CHAP password authentication, unless you configure IP routing in the same RADIUS user profile.

For details on carrying out these tasks, see the *MAX ISP and Telecommuting Configuration Guide*.

Introducing IPX routing

The MAX supports IPX routing between sites that run Novell NetWare version 3.11 or later. The MAX operates as an IPX router with one interface on the local Ethernet and the other across the WAN. It supports IPX routing over PPP, MP, MP+, and frame relay connections. Each RADIUS user profile that sets up an IPX connection is an IPX WAN interface.

NetWare servers broadcast Service Advertising Protocol (SAP) packets every 60 seconds to make sure that routers (such as the MAX) know about their services. Each router builds a SAP table with an entry for each service advertised by each known server. The router uses the SAP table to respond to client queries.

When a NetWare client sends a SAP request to locate a service, the MAX consults its SAP table and replies with its own hardware address and the internal address of the requested server. The client can then transmit packets whose destination address is the internal address of the server. When the MAX receives those packets, it consults its IPX RIP table. If it finds an entry for that destination address, it brings up the connection or forwards the packet across the active connection.

For complete information on IPX routing, see the *MAX ISP and Telecommuting Configuration Guide*.

Overview of RADIUS attributes for IPX routing

Table 6-5 lists the attributes relevant to IPX routing.

Table 6-5. IPX routing attributes

Attribute	Description	Possible values
Ascend-IPX-Alias (224)	Specifies the network number the MAX assigns to a point-to-point link. You need to specify a value for this attribute only if the MAX operates with a non-Ascend router that uses a numbered interface. It does not apply if you are routing from one MAX to another, or to a router that does not use a numbered interface.	8-digit (4-byte) hexadecimal value. The default value is 00000000.
Ascend-IPX-Peer-Mode (216)	Specifies whether the caller is an Ethernet client with its own IPX network address, or a dial-in PPP client.	IPX-Peer-Router (0) IPX-Peer-Dialin (1) The default value is IPX-Peer-Router.

Table 6-5. IPX routing attributes (continued)

Attribute	Description	Possible values
Ascend-IPX-Route (174)	Specifies a static route to an *internal* network of a NetWare server.	***profile_name*** specifies the RADIUS user profile to use to reach the network. The default value is null. ***network#*** indicates the unique internal network number of a NetWare server. The default value is 00000000. ***node#*** specifies the node number of the NetWare server. The default value is 000000000001. ***socket#*** specifies the socket number of the NetWare server. The default value is 0000. ***server_type*** specifies the SAP service type of the NetWare server. The default value is 0000. ***hop_count*** indicates the distance to the destination network in hops. The default value is 1. ***tick_count*** specifies the distance to the destination network in IBM PC clock ticks (one-eighteenth of a second). The default value is 12. ***server_name*** indicates the name of an IPX server. The default value is null.
Ascend-IPX-Route (174)	Specifies a static route to an *external* network.	***route-only*** is an idenfier to inform the MAX that this is a route to an external destination IPX network. ***network #*** indicates the unique external destination network number. ***transit_number*** is an intermediate route between the MAX and the destination network. The MAX must know how to route to this intermediate network.
Ascend-Route-IPX (229)	Indicates whether the MAX enables IPX routing for the user profile.	Route-IPX-No (0) Route-IPX-Yes (1) The default value is Route-IPX-No.

Specifying IPX routing

To specify IPX routing, follow these steps:

1 In the RADIUS user profile, specify the User-Name and Password attributes and WAN connection attributes.

For details on setting the User-Name and Password attributes, see Chapter 3, “Setting Up RADIUS Authentication.” For details on setting up WAN connection attributes, see Chapter 4, “Setting Up WAN Connections in RADIUS.”

2 To turn on IPX routing for the user profile, set Ascend-Route-IPX=Route-IPX-Yes.

3 If the MAX operates with a non-Ascend router that uses a numbered interface, set the Ascend-IPX-Alias attribute to specify a network number for the link.

4 To specify whether the caller is a dial-in PPP client or an Ethernet client with its own IPX network address, set the Ascend-IPX-Peer-Mode attribute.

Dial-in clients do not belong to an IPX network, so you must assign them an IPX network number. When you do so, a dial-in client can establish a routing connection with the MAX. To provide an IPX network number, you must define a virtual IPX network using the IPX Pool# parameter in the MAX configuration interface. The MAX advertises the route to this virtual network and assigns it as the network address for dial-in clients.

For the Ascend-IPX-Peer-Mode attribute, specify one of these settings:

– IPX-Peer-Router (0) indicates that the calling device is on the Ethernet network and has its own IPX address.

  This setting is the default.

– IPX-Peer-Dialin (1) indicates that the caller is a dial-in NetWare client that incorporates PPP software and dial-out hardware, but has no Ethernet interface.

  This setting causes the MAX to assign the caller an IPX address using the value of the IPX Pool# parameter on the MAX. If the client does not supply its own unique node number, the MAX assigns a unique node number as well. The MAX does not send IPX RIP and SAP advertisements across the connection and ignores IPX RIP and SAP advertisements it receives from the remote end. However, it does respond to IPX RIP and SAP queries it receives from dial-in clients.

Dial-in client connection example

In this example, a NetWare client dials into a corporate IPX network that supports both servers and clients (Figure 6-6).

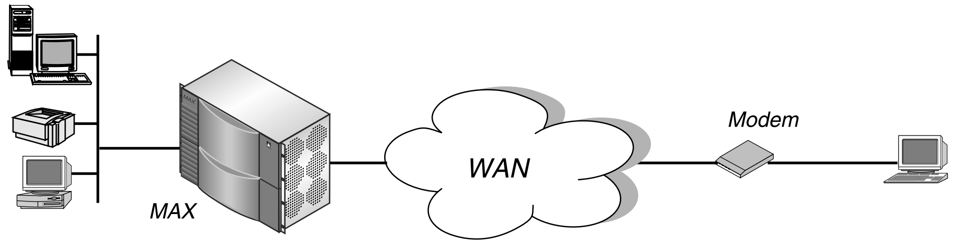

Figure 6-6. A dial-in NetWare client requiring dynamic IPX network assignment

In this example, the MAX is connected to a corporate NetWare LAN and the dial-in client has a modem, NetWare client software, and PPP dial-up software. This example assumes that the IPX Pool# attribute has been set in the Ethernet>Mod Config>Ether Options menu. To configure the MAX to accept a connection from the PC dial-in user, enter these specifications:

```
NetWareClient1 Password="m2dan", User-Service=Framed-User
    Framed-Protocol=PPP,
    Ascend-Route-IPX=Route-IPX-Yes,
    Ascend-IPX-Peer-Mode=IPX-Peer-Dialin,
    ...
```

Configuring static IPX routes

After the MAX unit clears its IPX RIP and SAP tables during a reset or power cycle, it adds the static routes upon initialization. Each static IPX route contains all the information necessary to reach one NetWare server on a remote network. When the MAX receives an outbound packet for that server, it finds the corresponding RADIUS user profile and dials the connection.

Most sites configure only a few IPX routes and rely on IPX RIP for most other connections. If you have servers on both sides of the WAN connection, we recommend that you define a static route to the remote site even if your environment requires dynamic routes. If you have one static route to a remote site, it should specify a master NetWare server that knows about many other services. NetWare workstations can then learn about other remote services by connecting to that remote NetWare server. If the MAX does not receive IPX RIP broadcasts from a remote unit, you should configure a static route to at least one server on that network.

You must manually update static routes whenever the administrator at the remote end removes the specified server or updates its address. You do not need to create IPX routes to servers that reside on the local Ethernet network.

To set up static IPX routes in RADIUS, follow these steps:

1 Create the first line of a pseudo-user profile using the User-Name, Password, and User-Service attributes.

You create a pseudo-user profile to store information that the MAX can query—in this case, in order to store IPX routing information. You can configure pseudo-users for both global and MAX-specific configuration control of IPX dialout routes. The MAX loads the unit-specific dialout routes in addition to the global dialout routes.

For a unit-specific IPX dialout route, specify the first line of a pseudo-user profile in this format:

```
IPXRoute-unit_name-num Password="Ascend", User-Service=Dialout-
Framed-User
```

For a global IPX dialout route, specify the first line of a pseudo-user profile in this format:

```
IPXRoute-num Password="Ascend", User-Service=Dialout-Framed-User
```

unit_name is the system name of the MAX—that is, the name specified by the Name parameter in the System profile. ***num*** is a number in a sequential series, starting at 1.

2 For each pseudo-user profile, specify one or more routes using the Ascend-IPX-Route attribute.

When you define a static route to an internal network, the Ascend-IPX-Route attribute has the following format:

```
Ascend-IPX-Route="profile_name network# [node#] [socket#]
[server_type] [hop_count] [tick_count] [server_name]"
```

Limit each profile to about 25 routes—that is, you should specify up to 25 settings for the Ascend-IPX-Route attribute. The MAX fetches information from each pseudo-user profile in order to gather routing information.

Table 6-6 describes each Ascend-IPX-Route argument.

Table 6-6. Ascend-IPX-Route arguments

Argument	Description
profile_name	Specifies the RADIUS user profile to use to reach the network. The default value is null.
network#	Indicates the unique internal network number of the NetWare server. The default value is 00000000.
node#	Specifies the node number of the NetWare server. The default value is 000000000001—the typical node number for a NetWare file server.
socket#	Indicates the socket number of the NetWare server. Typically, NetWare file servers use socket 0451. The default value is 0000. The number you specify must be a well-known socket number. Services that use dynamic socket numbers may use a different socket each time they load. To bring up a connection to a remote service that uses a dynamic socket number, specify a master server that uses a well-known socket number.

Table 6-6. Ascend-IPX-Route arguments (continued)

Argument	Description
server_type	Specifies the SAP service type of the NetWare server. NetWare file servers have SAP service type 0004. The default value is 0000.
hop_count	Indicates the distance to the destination network in hops. The default value is 1.
tick_count	Specifies the distance to the destination network in IBM PC clock ticks (one-eighteenth of a second). This value is for round-trip timer calculation and for determining the nearest server of a given type.The default value is 12.
server_name	Indicates the name of an IPX server. The default value is null.

When you define a static route to an internal network, the Ascend-IPX-Route attribute has the following format:

`Ascend-IPX-Route= “route-only` *`network# transit_network#`***`”`**

Table 6-7 describes each Ascend-IPX-Route argument.

Table 6-7. Ascend-IPX-Route arguments

Argument	Description
network #	Indicates the unique external network number. The default value is 00000000.
transit_network #	Indicates an intermediate network: • Between the MAX and the destination network. • To which the MAX knows how to route.

Whenever you power on or reset the MAX, or when you select the Upd Rem Cfg command from the Sys Diag menu, RADIUS adds IPX dialout routes to the routing table in this way:

1. RADIUS looks for profiles having the format IPXRoute-***`unit_name`***-1, where ***`unit_name`*** is the system name.
2. If at least one profile exists, RADIUS loads all existing profiles having the format `IPXRoute-`***`unit_name`***-***`num`*** to initialize the IPX routing table.

   The variable ***`num`*** is a number in a sequential series, starting with 1.
3. The MAX queries `IPXRoute-`***`unit_name`***-1, then `IPXRoute-`***`unit_name`***-2, and so on, until it receives an authentication reject from RADIUS.
4. RADIUS loads the global configuration profiles.

   These configurations have the form IPXRoute-***`num`***.
5. The MAX queries IPXRoute-1, then IPXRoute-2, and so on, until it receives an authentication reject from RADIUS.

Static IPX route configuration examples

The first example defines a unit-specific IPX route. The second example defines a global IPX route.

```
IPXRoute-CA-1 Password="Ascend", User-Service=Dialout-Framed-User

        Ascend-IPX-Route="def 6 7 8 9 10"

IPXRoute-1 Password="Ascend", User-Service=Dialout-Framed-User

        Ascend-IPX-Route="abc 1 2 3 4 5 "
```

Setting up a bridging connection

This sections covers the following topics:

- Before you begin
- Introducing bridging
- Overview of special IPX bridging requirements
- Overview of RADIUS bridging attributes
- Specifying protocol-independent bridging
- Configuring bridge entries

Before you begin

Before you set up a bridging connection in RADIUS, you must set up the MAX as a bridge. For details, see the *MAX ISP and Telecommuting Configuration Guide*.

Introducing bridging

The MAX uses bridging to provide connectivity for protocols other than IP and IPX, although you can also use bridging to join segments of an IP or IPX network. Because a bridging connection forwards packets at the link layer, it does not distinguish between protocol types and requires no protocol-specific configuration.

When you configure the MAX for bridging, it accepts all packets on the Ethernet network and forwards only those that do not have a physical address on the local Ethernet segment, or that have a broadcast address. A physical address is a unique, hardware-level address associated with a specific network controller. A device’s physical address is also called its Media Access Control (MAC) address. A broadcast address is recognized by multiple nodes on a network. All devices on the same network receive packets with the same address (FFFFFFFFFFFF on Ethernet).

The MAX is a transparent bridge (also called a learning bridge). As the MAX forwards a packet, it notes the packet’s source address and creates a bridge table that associates node addresses with a particular interface. Figure 6-7 shows the physical addresses of some nodes on the local Ethernet and at a remote site. The MAX at site A acts as a bridge.

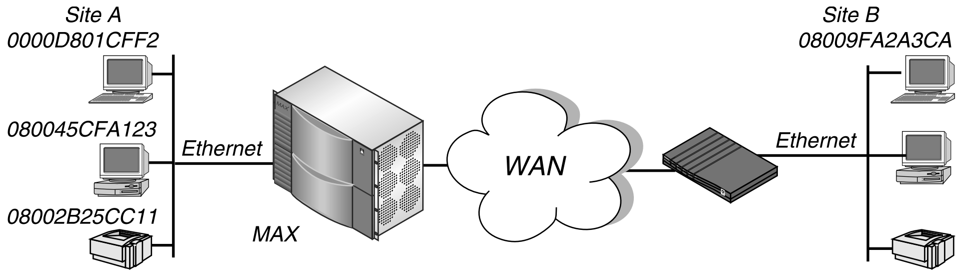

Figure 6-7. Bridging configuration

The MAX at site A gradually learns addresses on both networks by looking at each packet's source address, and it develops a bridge table like this one:

```
0000D801CFF2        SITEA
080045CFA123        SITEA
08002B25CC11        SITEA
08009FA2A3CA        SITEB
```

If the MAX receives a packet whose destination MAC address is not on the local network, it first checks its internal bridge table. If it find the packet's destination MAC address, the MAX dials the connection and bridges the packet. If it does not find the address, the MAX checks for active sessions that have bridging enabled. If one or more active bridging links are up, the MAX forwards the packet across all active sessions that have bridging enabled.

The MAX associates a Connection profile or RADIUS user profile with a bridging link either because the remote caller used the profile to dial the link, or because the profile matched an incoming call. You can also specify static bridge table entries in RADIUS pseudo-user profiles.

Overview of special IPX bridging requirements

IPX bridging has special requirements for facilitating NetWare client-server logins across the WAN, and for preventing IPX RIP and SAP broadcasts from keeping a bridged connection up indefinitely. To specify special IPX bridging behavior, you use the Ascend-Handle-IPX attribute.

For the Ascend-Handle-IPX attribute to have any effect, the IPX Frame parameter in the MAX configuration interface must specify the IPX frame type in use. Your setting for Ascend-Handle-IPX depends upon your bridging configuration. The following sections describe different types of bridging configurations.

Bridging when only the local network supports NetWare clients

If the local Ethernet supports NetWare clients only and no NetWare servers, the bridging connection should enable a local client to bring up the WAN connection by querying (broadcasting) for a NetWare server on a remote network. However, the connection should not stay up indefinitely based on RIP or SAP broadcasts. If your configuration matches this one, set Ascend-Handle-IPX=Handle-IPX-Client.

Bridging when only the local network supports NetWare servers

If the local network supports NetWare servers (or a combination of clients and servers) and the remote network supports NetWare clients only, the bridging connection should enable the MAX to respond to NCP watchdog requests for remote clients, but bring down inactive connections whenever possible. To accomplish this task, set Ascend-Netware-timeout=30 (for example), and Ascend-Handle-IPX=Handle-IPX-Client.

Bridging when both sides of the link support NetWare servers

If NetWare servers reside on both sides of the WAN connection, we strongly recommend that you use an IPX routing configuration instead of bridging IPX. If you bridge IPX in this type of environment, client-server logins are lost when the MAX brings down an inactive WAN connection.

IPX routing and bridging on the same connection

When you enable IPX routing for a connection, the MAX routes only one packet frame type for IPX packets across that connection. For example, if the IPX frame type is 802.3, the MAX routes only 802.3 packets. If some NetWare servers on the local network use a different frame type, such as 802.2, the MAX bridges those packets if you enable bridging, or discards them if you do not.

If IPX Frame=802.3 on the MAX, the settings you make in RADIUS have the following effects:

- If Ascend-Route-IPX=Route-IPX-Yes and Ascend-Bridge=Bridge-No in the RADIUS user profile, the MAX routes only 802.3 IPX packets, and drops all other packets.
- If Ascend-Route-IPX=Route-IPX-Yes and Ascend-Bridge=Bridge-Yes in the RADIUS user profile, the MAX routes 802.3 IPX packets and bridges all other packets, including IPX packets in other frame types.

  For example, if the MAX receives an IPX packet in the 802.2 packet frame, it uses the physical address in that packet to bridge it across all active bridging sessions.

Overview of RADIUS bridging attributes

Table 6-8 lists the bridging attributes.

Table 6-8. Bridging attributes

Attribute	Description	Possible values
Ascend-Bridge (230)	Enables or disables protocol-independent bridging for the call.	Bridge-No (0) Bridge-Yes (1) The default value is Bridge-No.

Table 6-8. Bridging attributes (continued)

Attribute	Description	Possible values
Ascend-Bridge-Address (168)	Specifies the IP address and associated MAC address of a device on a remote LAN to which the MAX can form a bridging connection. Also specifies the name of the dialout profile the MAX uses to bring up the connection.	***MAC_address*** specifies the destination device's hardware address. The default value is 000000000000. ***profile_name*** specifies the dialout profile that brings up the connection. ***IP_address*** specifies the destination device's IP address. The default value is 0.0.0.0.
Ascend-Handle-IPX (222)	Specifies how the MAX handles NCP watchdog requests on behalf of IPX clients during IPX bridging.	Handle-IPX-None (0) Handle-IPX-Client (1) Handle-IPX-Server (2) The default value is Handle-IPX-None.
Ascend-Netware-timeout (223)	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 connection.	Integer between 0 and 65535. The default value is 0 (zero).

Specifying protocol-independent bridging

To specify that bridging is available to a user profile, follow these steps:

1 Specify the User-Name and Password attributes, authentication attributes, and WAN connection attributes.

The most common cause of trouble when setting up a bridging connection is specifying the wrong name for the MAX or the remote device. You must specify the name of the remote device or user exactly as it appears remotely, including case changes, dashes, and underscores.

For details on setting the User-Name, Password, and authentication attributes, see Chapter 3, "Setting Up RADIUS Authentication." For details on setting up WAN connection attributes, see Chapter 4, "Setting Up WAN Connections in RADIUS."

2 To turn on bridging for the user profile, set Ascend-Bridge=Bridge-Yes.

3 To turn off IPX routing, set Ascend-Route-IPX=Route-IPX-No.

4 To specify special IPX bridging behavior, set the Ascend-Handle-IPX attribute.

For details on the appropriate setting for your environment, see "Overview of special IPX bridging requirements" on page 6-32. Note that if Ascend-Route-IPX=Route-IPX-Yes in the RADIUS user profile, the Ascend-Handle-IPX attribute acts as though it is set to Handle-IPX-Server.

5 If you set Ascend-Handle-IPX=Handle-IPX-Server, set the Ascend-Netware-timeout attribute to indicate the maximum length of idle time during which the MAX performs watchdog spoofing for NetWare connections.

IPX client bridge example (local clients)

In Figure 6-8, the local Ethernet supports NetWare clients, and the remote network supports both NetWare servers and clients.

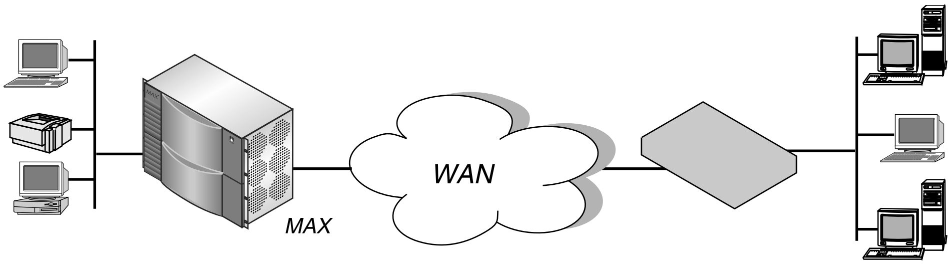

Figure 6-8. An example IPX client bridging connection

To configure the MAX in this example, you might use a profile like this one:

```
MAX1 Password="m2dan", User-Service=Framed-User
     Framed-Protocol=PPP,
     Ascend-Route-IPX=Route-IPX-No,
     Ascend-Bridge=Bridge-Yes,
     Ascend-Handle-IPX=Handle-IPX-Client,
     Ascend-Netware-timeout=30
```

IPX server bridge example (local servers)

In Figure 6-9, the local network supports a combination of NetWare clients and servers, and the remote network supports clients only.

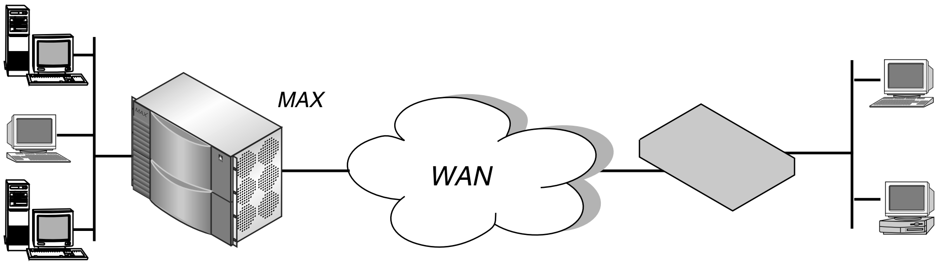

Figure 6-9. An example IPX server bridging connection

To configure the MAX in this example, you might use a profile like this one:

```
MAX1 Password="m2dan", User-Service=Framed-User
     Framed-Protocol=PPP,
     Ascend-Route-IPX=Route-IPX-No,
     Ascend-Bridge=Bridge-Yes,
     Ascend-Handle-IPX=Handle-IPX-Server,
     Ascend-Netware-timeout=30
```

Configuring bridge entries

To set up bridge entries in RADIUS for the bridge table, follow these steps:

1 Create the first line of a pseudo-user profile using the User-Name, Password, and User-Service attributes.

You create a pseudo-user profile to store information that the MAX can query—in this case, in order to store bridging information. For a unit-specific bridge profile, specify the first line of a pseudo-user profile in this format:

```
Bridge-unit_name-num Password="Ascend", User-Service=
Dialout-Framed-User
```

unit_name is the system name of the MAX—that is, the name specified by the Name parameter in the System profile. ***num*** is a number in a sequential series, starting at 1.

2 For each pseudo-user profile, specify one or more bridge entries using the Ascend-Bridge-Address attribute.

The Ascend-Bridge-Address attribute has this format:

Ascend-Bridge-Address="*MAC_address profile_name IP_address*"

Table 6-9 describes Ascend-Bridge-Address arguments.

Table 6-9. Ascend-Bridge-Address arguments

Argument	Description
MAC_address	Specifies a MAC address in standard 12-digit hexadecimal format (yyyyyyyyyyyy) or in colon-separated format (yy:yy:yy:yy:yy:yy). If the leading digit of a colon-separated pair is 0 (zero), you do not need to enter it. That is, **:y** is the same as **:0y**. The default value is 000000000000.
profile_name	Specifies the name of the dialout profile the MAX uses to bring up the connection. You can specify either a Connection profile or a RADIUS user profile. The MAX looks for a local profile first.
IP_address	Specifies an IP address in dotted decimal notation. The default value is 0.0.0.0.

Each Ascend-Bridge-Address setting specifies the IP address and associated MAC address of a device on a remote LAN to which the MAX can form a bridging connection. When your MAX receives an ARP request for one of the IP addresses you specify, the MAX replies with the corresponding MAC address and uses the specified profile to bring up a connection to that address. Because the MAX replies to these ARP requests as if the IP devices were local, you must have user profiles that bridge IP packets to each device.

Whenever you power on or reset the MAX, or when you select the Upd Rem Cfg command from the Sys Diag menu, RADIUS adds bridging entries to the bridge table in this way:

1. RADIUS looks for profiles having the format Bridge-***unit_name***-***num***, where ***unit_name*** is the system name and ***num*** is a number in a sequential series, starting with 1.
2. RADIUS loads the data to create the bridging tables.

Bridge profile configuration examples

This example creates two bridging table entries.

```
Bridge-Ascend-1 Password="Ascend", User-Service=Dialout-Framed-User

        Ascend-Bridge-Address="2:2:3:10:11:12 Prof1 1.2.3.4 1",

        Ascend-Bridge-Address="2:2:3:13:14:15 Prof2 5.6.7.8 2"
```

Setting up a DHCP connection

When you set up a Dynamic Host Configuration Protocol (DHCP) connection in a RADIUS user profile, the MAX can assign a dynamic IP address to a remote DHCP client over a bridged connection. The MAX becomes a DHCP server.

For example, if a group of DHCP clients reside on a LAN connected to a Pipeline, and the Pipeline connects to the MAX over a bridged PPP connection, the MAX can assign dynamic IP addresses to any of the DHCP clients on the remote LAN (Figure 6-10).

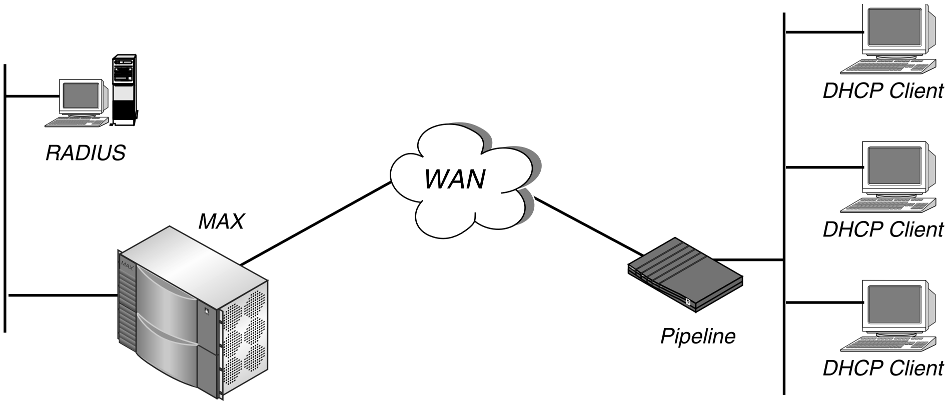

Figure 6-10. Pipeline connected to DHCP clients

The RADIUS server holds the configuration information the MAX uses to identify and authenticate each DHCP client.

When the DHCP client requests an address, the MAX allocates an IP address from one of its IP address pools and assigns it to the client for 30 minutes. The client must renew the IP address assignment after the 30-minute period expires. In its local memory, the MAX keeps track of all IP addresses it has assigned. Therefore, it loses the entries for current, unexpired IP address assignments when you reset it.

A client may hold an unexpired IP address assignment when you reset the MAX. After the reset, the MAX may assign that address to a new client. These duplicate IP addresses cause network problems until the first assignment expires or one of the clients reboots.

Overview of DHCP attributes

Table 6-10 lists the DHCP attributes.

Table 6-10.DHCP attributes

Attribute	**Description**	**Possible values**
Ascend-DHCP-Pool-Number (148)	Specifies the address pool that incoming calls use.	Integer between 1 and the number of defined IP address pools. The default value is 0 (zero), which represents the first defined IP address pool.
Ascend-DHCP-Reply (147)	Specifies whether the MAX processes DHCP packets and acts as a DHCP server on this connection.	DHCP-Reply-No (0) DHCP-Reply-Yes (1) The default value is DHCP-Reply-No.

Configuring a DHCP connection

To configure a DHCP connection, follow these steps:

1 Set up one or more IP address pools in a RADIUS pseudo-user profile.

For details, see “Defining a pool of IP addresses for dynamic assignment” on page 6-8.

2 Configure a bridging connection in a RADIUS user profile.

For details, see “Setting up a bridging connection” on page 6-31.

3 In the RADIUS user profile, set Ascend-DHCP-Reply=DHCP-Reply-Yes.

This setting enables DHCP functionality.

4 In the RADIUS user profile, set the Ascend-DHCP-Pool-Number attribute.

Specify the number of the IP address pool the MAX uses when allocating a dynamic IP address to this connection. You can specify a number between 1 and the number of IP pools defined on the MAX. The default value is 0 (zero). When you accept the default, the MAX uses the first defined IP address pool.

Setting up Network Address Translation (NAT) for LAN

Access to public networks requires the use of an official IP address that is unique across the entire network. Typically, a central authority assigns a range of addresses, and a local administrator distributes them. If access to a public network is not necessary, the local manager can assign addresses as he or she sees fit, even if the addresses are not official or belong to another company.

Because the supply of addresses is rapidly diminishing, a company may not be able to get official addresses for its entire network. Other sites may already have unofficial addresses, but now need access to the Internet, where an official address is required. For these reasons, you need a facility to borrow an official address and dynamically translate between the local and official addresses.

NAT for LAN allows a Pipeline to connect a LAN to another network even if the devices on the LAN do not have valid addresses for the remote network. The Pipeline translates between the local network addresses and the remote network addresses.

When you enable NAT for LAN, the Pipeline attempts to perform IP address translation on all packets it receives. The Pipeline has no notion of what may or may not be official addresses on the LAN. The Pipeline acts as a DHCP client on behalf of all hosts on the LAN and relies on the MAX unit (acting as the DHCP server) to provide addresses suitable for the remote network from its IP address pool. On the local network, the Pipeline and the hosts all have local addresses on the same network, and use them only for local communication between the hosts and the Pipeline over the Ethernet.

Figure 6-11 illustrates a basic NAT for LAN setup.

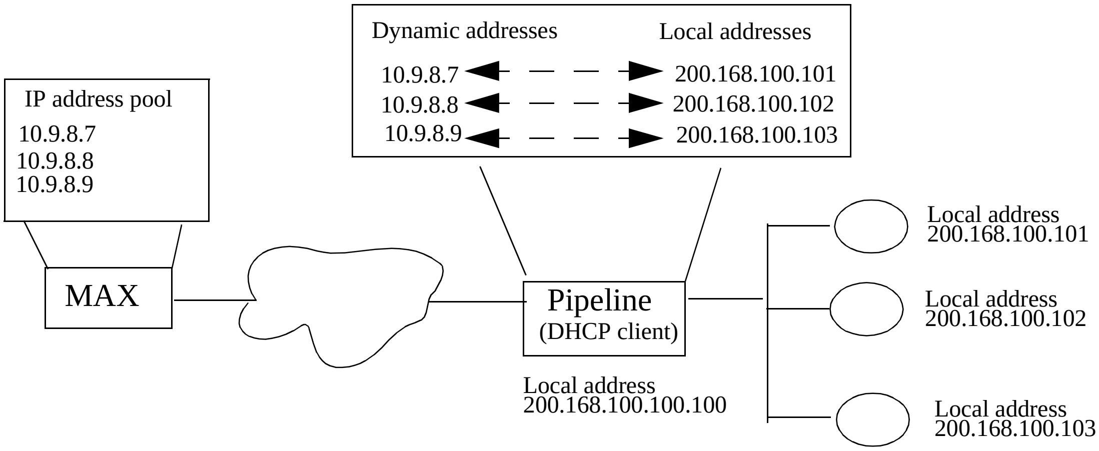

Figure 6-11. NAT for LAN setup

In Figure 6-11, the Pipeline itself does not have an address on the remote network. Therefore, clients can gain access to the Pipeline only from the local network, not from the WAN.

When the first client on the LAN requests access to the remote network, the Pipeline gets the address through PPP negotiation. When subsequent clients request access to the remote network, the Pipeline asks for an IP address from the MAX using a DHCP request packet. In return, the MAX sends an address to the Pipeline from its IP address pool. The Pipeline uses the dynamic addresses it receives from the MAX to translate IP addresses on behalf of local clients.

As it receives packets on the LAN, the Pipeline determines whether the source IP address has a corresponding translated address. If so, the Pipeline translates the packet, and forwards it out the WAN. If the Pipeline has not assigned a translated address (and one is not pending), the Pipeline issues a new DHCP request for this IP address. While waiting for the MAX to offer an IP address, the Pipeline drops corresponding source packets. For packets it receives from the WAN, the Pipeline checks the destination address against its table of translated addresses. If the destination address exists and is active, the Pipeline forwards the packet. If the destination address does not exit, or is not active, the Pipeline drops the packet.

The MAX typically offers IP addresses for a limited duration, but the Pipeline automatically renews the lease on these addresses. If the connection to the remote server goes down, all leased addresses are considered revoked. Therefore, TCP connections do not persist across calls.

In some installations, the MAX handles both NAT for LAN DHCP requests and ordinary DHCP requests. In this situation, if the ordinary DHCP clients are connecting to the MAX over a non-bridged connection, you must have a separate DHCP server to handle these requests.

Before you begin

If you use RADIUS to authenticate users, and you do not authenticate users that request DHCP, set Use Answer as Default=Yes in the Answer profile. If you set Use Answer as Default=No, the MAX cannot act as a DHCP server for these clients.

Configuring the Pipeline for NAT for LAN

For details on configuring NAT on the Pipeline, consult the Pipeline documentation.

Configuring the MAX for NAT for LAN

To configure the MAX for NAT for LAN, you can specify settings in an Answer profile, a Connection profile, or a RADIUS user profile. This section describes how to set up a RADIUS user profile. For information on setting up an Answer profile or a Connection profile, see the *MAX ISP and Telecommuting Configuration Guide*.

To configure NAT for LAN in RADIUS, you use the attributes listed in Table 6-11.

Table 6-11.NAT for LAN attributes

Attribute	Description	Possible values
Ascend-DHCP-Pool-Number (148)	Specifies the address pool to use for allocating an IP address to a NAT for LAN client on this connection.	Integer between 1 and the number of defined IP address pools. The default value is 0 (zero), which represents the first defined IP address pool.

Table 6-11.NAT for LAN attributes (continued)

Attribute	**Description**	**Possible values**
Ascend-DHCP-Reply (147)	Specifies whether the MAX processes DHCP packets and acts as a DHCP server on this connection.	DHCP-Reply-No (0) DHCP-Reply-Yes (1) The default value is DHCP-Reply-No.
Ascend-DHCP-Maximum-Leases	Specifies the maximum number of dynamic addresses the MAX can assign to NAT for LAN clients using this connection	Integer between 1 and 254. The default value is 4.

To set up NAT for LAN for a MAX in a RADIUS user profile, follow these steps:

1 Set up one or more IP address pools in a RADIUS pseudo-user profile.

For details, see “Defining a pool of IP addresses for dynamic assignment” on page 6-8.

2 Set up routing or bridging in RADIUS.

For information on setting up routing, see “Setting up a system-based IP routing connection” on page 6-1. For information on setting up bridging, see “Setting up a bridging connection” on page 6-31.

3 To enable DHCP functionality, set Ascend-DHCP-Reply=DHCP-Reply-Yes.

– For a bridged connection, the MAX responds to all DHCP requests.

– For a non-bridged connection, the MAX responds only to NAT for LAN DHCP packets.

4 Set the Ascend-DHCP-Pool-Number attribute.

Specify the number of the IP address pool the MAX uses when allocating a dynamic IP address to a NAT client on this connection. You can specify a number between 1 and number of IP pools defined on the MAX. The default value is 0 (zero). When you accept the default, the MAX uses the first defined IP address pool.

5 Set the Ascend-DHCP-Maximum-Leases attribute to specify the maximum number of addresses that the MAX can give to the Pipeline.

You can specify a value between 1 and 254. The default value is 4.

Setting Up Virtual Private Networks in RADIUS

7

This chapter contains:

Introducing ATMP

Ascend Tunnel Management Protocol (ATMP) is a UDP/IP-based protocol that provides a tunnelling mechanism between two Ascend units across the Internet or a frame relay network. Each Ascend unit can be a MAX or a Pipeline 400. The protocol uses standard Generic Routing Encapsulation (GRE).

ATMP provides a Virtual Private Network (VPN) solution over the backbone resources of Internet Service Providers (ISPs) and carriers. Without ATMP, each mobile node and remote user has to dial directly into the network, resulting in long-distance charges. With ATMP, these users can make a local call and have the transmission securely tunnelled across the Internet or frame relay network.

As described in RFC 1701, GRE hides packet contents and enables transmission of packets that would otherwise be unacceptable on the Internet. These include IP packets that use unregistered addresses or IPX packets from roaming clients.

ATMP creates and tears down the tunnel between two Ascend units. In effect, the tunnel collapses the Internet cloud and provides what looks like direct access to a home network from a remote node. ATMP applies only to IP or IPX networks.

You can also set up RADIUS accounting so that the Accounting Stop packet indicates if a session authenticated and encapsulated using the ATMP tunneling protocol. See “Non-accounting attributes in accounting records” on page 8-13.

How ATMP connections work

Figure 7-1 shows a sample ATMP tunnel connection.

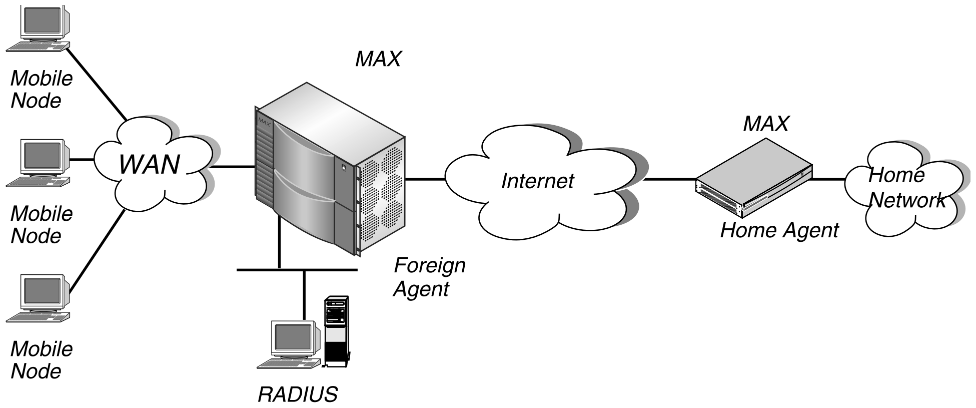

Figure 7-1. Sample cross-Internet ATMP tunnel

Table 7-1 lists the network elements that work together in an ATMP connection.

Table 7-1. ATMP network elements

Element	Description
Home network	The home network is a private corporate network. A private network is one that cannot communicate directly on the Internet. It might be an IPX network, or an IP network with an unregistered network number.
Mobile node	A mobile node is a user who accesses a private home network across the Internet. The mobile node could be a salesperson on the road who wants to dial into a local ISP and log into his or her home network.
Foreign agent	The foreign agent is an Ascend unit that the mobile node dials into. It is the starting point of the ATMP tunnel. The foreign agent must be able to bring up an IP connection to the home agent, and it must authenticate the mobile node using a RADIUS user profile that includes ATMP attributes.
Home agent	The home agent is an Ascend unit that represents the terminating part of the tunnel. It must be able to communicate with the home network directly, through another router, or across a nailed-up WAN connection.

When a mobile node wants to establish an ATMP connection with the home network, these events take place:

1 The mobile node dials a connection to the foreign agent.

2 The foreign agent authenticates the mobile node using a RADIUS user profile.

3 The foreign agent locates a Connection profile or RADIUS user profile for the home agent based on the Ascend-Primary-Home-Agent or Ascend-Secondary-Home-Agent attribute in the mobile node’s RADIUS user profile.

The Ascend-Primary-Home-Agent attribute specifies the IP address or hostname of the first home agent the foreign agent tries to reach when setting up an ATMP tunnel. The Ascend-Secondary-Home-Agent specifies the home agent the foreign agent tries to reach if the primary home agent is unavailable.

4 The foreign agent connects to the home agent using a regular IP connection.

The MAX authenticates the connection in the usual way (for example, by using CHAP).

5 The foreign agent informs the home agent that the mobile node has connected, and requests a tunnel.

The foreign agent sends up to ten RegisterRequest messages at two-second intervals, timing out and logging a message if it receives no response to those requests.

6 The home agent requests authentication of the mobile node by sending a challenge request to the foreign agent.

7 The foreign agent sends back a challenge reply to the home agent.

This reply includes an encrypted version of the Ascend-Home-Agent-Password value in the mobile node’s RADIUS profile. This password must match the value of the home agent’s Password parameter in the Ethernet > Mod Config > ATMP Options menu.

8 The home agent returns a RegisterReply with a number that identifies the tunnel.

If registration fails, the home agent logs a message and the foreign agent disconnects the mobile node. If registration succeeds, the MAX creates a tunnel between the foreign agent and the home agent. At this point, the mobile node connects to the home network as though it had dialed locally, and can transfer data across the tunnel.

9 When the mobile node disconnects from the foreign agent, the foreign agent sends a DeregisterRequest to the home agent to close down the tunnel.

The foreign agent can send its request a maximum of ten times, or until it receives a DeregisterReply. If the foreign agent receives packets for a mobile node whose connection has gone down, the foreign agent silently discards the packets.

ATMP router and gateway modes

You can configure the home agent as a router or a gateway to the home network.

Router mode

When you configure the home agent as a router, the home agent’s routing module forwards packets it receives from the foreign agent onto the local network. The network can be the home network, or it can support another router that can connect to the home network. In either case, packet delivery relies on a routing mechanism, such as a static or dynamic route, and not on a WAN connection.

In the case of routing an IPX packet from the mobile node, the home agent must see the mobile node as connected to another IPX network. ATMP adds this virtual IPX network to the home agent's routing table based on the IPX attributes it receives from the foreign agent. The RADIUS user profile for the mobile node must specify the IPX network number unique within the enterprise.

Gateway mode

When you configure the home agent as a gateway, the home agent tunnels packets from the foreign agent to the home network across an open WAN connection. The WAN connection must be on line. The home agent does not bring up a WAN connection to the home network based on a packet it receives through the tunnel. For this reason, the home agent must have a nailed-up WAN connection to the home network.

Overview of RADIUS attributes for ATMP

The foreign agent must have a RADIUS user profile that authenticates the mobile node and specifies the attributes listed Table 7-2. The IPX attributes shown in Table 7-2 are not ATMP-specific, but may be required for ATMP connections to an IPX home network.

Table 7-2. RADIUS attributes required for ATMP connections

Attribute	Description	Possible values
Ascend-Home-Agent-Password (184)	Indicates the password that the foreign agent sends to the home agent during ATMP operation. This password must match the home agent's ATMP password.	Text string containing up to 20 characters. The default value is null.
Ascend-Home-Agent-UDP-Port (186)	Specifies the UDP port number for communicating ATMP messages between the foreign agent and the home agent.	Integer between 0 and 65535. The default value is 5150. You need not specify a value for Ascend-Home-Agent-UDP-Port if you specify a UDP port number for Ascend-Primary-Home-Agent or Ascend-Secondary-Home Agent, or if you accept the default for either of these attributes.
Ascend-Home-Network-Name (185)	Specifies the name of the home agent's nailed-up Connection profile to the home network (required only if the home agent is operating in gateway mode).	Text string. The default value is null.
Ascend-IPX-Node-Addr (182)	Indicates a unique IPX node address on the network specified by Framed-IPX-Network. This value completes the IPX address of a mobile node.	12-digit ASCII string. The default value is 000000000001.

Table 7-2. RADIUS attributes required for ATMP connections (continued)

Attribute	**Description**	**Possible values**
Framed-IPX-Network (23)	Specifies a virtual IPX network required for the home agent to route IPX packets to the mobile node. This network must be unique in the IPX routing domain.	Decimal value representing the IPX network number of the IPX router at the remote end of the connection. The default value is null.
Ascend-Primary-Home-Agent (129)	Specifies the first home agent the foreign agent tries to reach when setting up an ATMP tunnel, and indicates the UDP port the foreign agent uses for the link.	A symbolic hostname, or an IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. You can also specify an optional UDP port number. The default IP address is 0.0.0.0. The default UDP port number is 5150. **Note:** You can use Ascend-Home-Agent-IP-Addr in the user profile for the same purpose as Ascend-Primary-Home-Agent, but it is preferable to use Ascend-Primary-Home-Agent and Ascend-Secondary-Home-Agent to provide additional information in the user profile.
Ascend-Secondary-Home-Agent (130)	Specifies the secondary home agent the foreign agent tries to reach when the primary home agent (specified by Ascend-Primary-Home-Agent) is unavailable. Also indicates the UDP port the foreign agent uses for the link.	A symbolic hostname, or an IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. You can also specify an optional UDP port number. The default IP address is 0.0.0.0. The default UDP port number is 5150.

For information on non-ATMP attributes

The home agent and the foreign agent must have their own outgoing RADIUS user profiles in order to connect to each other. Each user profile must enable IP routing, and make use of non-ATMP attributes. In addition, if you are tunneling IPX, you must set IPX attributes. This chapter provides the basic steps for setting up these profiles. For complete information on each attribute you can set, see Chapter 9, “Reference to RADIUS Attributes.”

Overview of MAX configuration parameters for ATMP

Both the foreign agent and home agent require some ATMP configuration on the MAX. The related parameters appear in Table 7-3.

Table 7-3. ATMP parameters

Location	**Parameter**	**Description**
Ethernet > Connections > Any Connection profile > Session Options	ATMP Gateway	Specifies whether the home agent acts as a gateway in its connection to the home network.
Ethernet > Mod Config > ATMP Options	ATMP Mode	Specifies whether the unit is a foreign agent or a home agent.
	Type	Specifies whether the home agent acts as a gateway or a router.
	Password	On the home agent, specifies the password the mobile node must specify in the Ascend-Home-Agent-Password attribute.
	UDP Port	Specifies the port to use for ATMP communications. Both ends of the tunnel must specify the same port number.

For information on non-ATMP parameters

A home agent in gateway mode must have its own Connection profile to the home network. Except for the ATMP Gateway setting, this profile uses non-ATMP parameters. The present chapter provides the basic steps for setting up the Connection profile. For complete information on each non-ATMP Connection profile parameter you can set in the MAX configuration interface, see the MAX *Reference Guide*.

Setting up a tunnel in router mode for an IP network

A private IP network is a network with an unregistered IP address. An ATMP tunnel enables a remote user to log into a private IP network across the Internet using a local ISP connection.

Figure 7-2 shows a tunnel in which the home agent is in router mode.

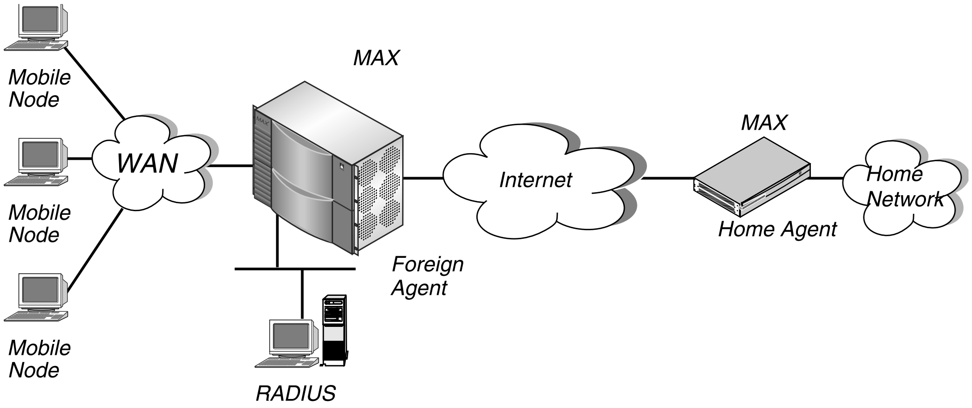

Figure 7-2. ATMP router mode

When the home agent is in router mode, it receives GRE-encapsulated IP packets from the foreign agent, strips off the encapsulation, and passes the packets to its bridge/router software. It also adds a host route to the mobile node in its routing table.

This section describes how to set up a foreign agent and a home agent in router mode.

Configuring the foreign agent in router mode

To configure the foreign agent in router mode, you must perform these tasks:

- Configure ATMP in the foreign agent's Ethernet profile using the MAX configuration interface.
- Configure the foreign agent to authenticate via RADIUS.
- Create an incoming RADIUS user profile for the mobile node.
- For the foreign agent, configure an outgoing RADIUS user profile with IP routing to the home agent.

  Instead of an outgoing RADIUS user profile, you can set up a Connection profile to the home agent. For details, see the MAX *ISP and Telecommuting Configuration Guide*.

Configuring ATMP in the foreign agent's Ethernet profile

To configure ATMP in the foreign agent's Ethernet profile, follow these steps:

1 Open the Ethernet menu.

2 Open the Mod Config menu.

3 Open the ATMP Options menu.

4 Set these parameters:

```
ATMP options...
    ATMP Mode=Foreign
    Type=N/A
    Password=N/A
    UDP Port=5150
```

5 Save your changes.

Configuring the foreign agent to authenticate via RADIUS

Follow the instructions in “Configuring the MAX to use the RADIUS server” on page 2-4.

Configuring an incoming RADIUS profile for the mobile node

To create a RADIUS users profile for the mobile node, follow these steps:

1 On the first line of the profile, specify the User-Name and Password attributes:

2 To specify the type of encapsulation in use for the call, set the Framed-Protocol attribute.

3 Enable IP routing for the profile by setting Ascend-Route-IP=Route-IP-Yes.

4 To specify the mobile node’s IP address, set the Framed-Address attribute, and optionally, the Framed-Netmask attribute.

5 Set the Ascend-Primary-Home-Agent attribute.

This attribute specifies the first home agent the foreign agent tries to reach when setting up the ATMP tunnel, and indicates the UDP port the foreign agent uses for the link.

Specify the primary home agent using this syntax:

Ascend-Primary-Home-Agent="*hostname* **|** *ip_address* **[:***udp_port***]"**

– The ***hostname*** argument indicates the home agent’s symbolic hostname.

– The ***ip_address*** argument indicates the home agent’s IP address in dotted decimal notation. Specify an IP address if no DNS server exists for the home agent. You can specify a hostname or an IP address, but not both.

– The optional ***udp_port*** argument indicates the UDP port on which the foreign agent communicates with the home agent. The default value is 5150.

– The colon (:) separates the hostname or IP address from the UDP port specification.

6 Set the Ascend-Secondary-Home-Agent attribute.

This attribute specifies the secondary home agent the foreign agent tries to reach when the primary home agent (specified by Ascend-Primary-Home-Agent) is unavailable. The attribute also indicates the UDP port the foreign agent uses for the link.

7 For the Ascend-Home-Agent-Password attribute, specify the home agent’s password.

You must specify the same password indicated by the Password parameter in the Ethernet > Mod Config > ATMP Options menu on the home agent.

8 To specify the UDP port for ATMP operation, set the Ascend-Home-Agent-UDP-Port attribute.

By default, ATMP uses UDP port 5150 for communicating ATMP messages between the foreign and home agents. Both the foreign and home agent must agree on the UDP port number. If you specify a non-default UDP port number in one unit’s configuration, make sure that the other end of the tunnel specifies the same number.

You need not specify a value for Ascend-Home-Agent-UDP-Port if you specify a UDP port number for Ascend-Primary-Home-Agent or Ascend-Secondary-Home Agent, or if you accept the default for any of these attributes.

This user profile specifies a mobile node named Node1 and a single home agent at the IP address 10.9.8.10:

```
Node1 Password="Top-secret"
      Ascend-Metric=2,
      Framed-Protocol=PPP,
      Ascend-IP-Route=Route-IP-Yes,
      Framed-Address=200.1.1.2,
      Framed-Netmask=255.255.255.0,
      Ascend-Primary-Home-Agent=10.8.9.10,
      Ascend-Home-Agent-Password="private"
```

When the mobile node logs into the foreign agent with the password Top-secret, the foreign agent authenticates the mobile node. The foreign agent then looks for a profile with an IP address that matches the Ascend-Primary-Home-Agent value, so it can bring up an IP connection to the home agent.

Configuring an outgoing RADIUS user profile for the foreign agent

For the foreign agent, you must create an outgoing user profile to the home agent. Follow these steps:

1 On the first line of the user profile, specify the User-Name, Password, and User-Service attributes.

Set the attributes on the first line in this way:

– For the User-Name attribute, specify the name of the foreign agent, appending **`-Out`** to the user name.

– Set Password="Ascend".

– Set User-Service=Dialout-Framed-User. This setting ensures that RADIUS cannot use the profile for authentication of an incoming call.

For example, you might enter this first line in the profile for the foreign agent Alameda:

```
Alameda-Out Password="Ascend", User-Service=Dialout-Framed-User
```

2 On the second line of the user profile, set the User-Name attribute to the name of the foreign agent.

3 To specify the encapsulation type in use on the line, set the Framed-Protocol attribute.

4 Enable IP routing for the profile by setting Ascend-Route-IP=Route-IP-Yes.

5 If the receiving end (the home agent) requires an IP address, and does not assign one dynamically, specify the foreign agent's IP address using the Framed-Address attribute (and, optionally, the Framed-Netmask attribute).

The values of the Framed-Address and Framed-Netmask attributes for the local MAX must match the value of the NAS-Identifier attribute on the home agent. If there is no match, the home agent clears the call.

6 To indicate the phone number the MAX dials to reach the home agent, set the Ascend-Dial-Number attribute.

7 To specify the type of phone number the MAX dials, set the Ascend-PRI-Number-Type attribute.

8 Set the Ascend-Send-Auth attribute.

The Ascend-Send-Auth attribute specifies the authentication protocol that the MAX requests when initiating a connection using PPP or MP+ encapsulation. The answering side of the connection determines which authentication protocol, if any, the connection uses.

9 If you request PAP or CHAP authentication, you must also specify a password using Ascend-Send-Secret or Ascend-Send-Passwd.

Both of these attributes specify the password that the MAX sends to the remote end of a connection on outgoing calls. If the value you specify for Ascend-Send-Secret or Ascend-Send-Password does not match the value of the remote end's Ascend-Receive-Secret attribute (in a RADIUS user profile) or Recv PW parameter (in a Connection profile), the remote system rejects the call.

Use Ascend-Send-Passwd only if your version of the MAX does not support Ascend-Send-Secret.

This user profile enables a MAX called Alameda to dial calls to the MAX at 1-800-555-5555:

```
Alameda-Out Password="Ascend", User-Service=Dialout-Framed-User
     User-Name="Alameda",
     Framed-Protocol=PPP,
     Ascend-Route-IP=Route-IP-Yes,
     Framed-Address=10.0.100.1,
     Framed-Netmask=255.255.255.0,
     Ascend-Metric=2,
     Framed-Routing=None,
     Ascend-Idle-Limit=30,
     Ascend-Dial-Number=1-800-555-5555,
     Ascend-PRI-Number-Type=National-Number,
     Ascend-Send-Auth=Send-Auth-PAP,
     Ascend-Send-Secret="Password1"
```

Configuring the home agent in router mode

To configure the home agent in router mode, you must perform these tasks:

- Configure ATMP in the home agent's Ethernet profile using the MAX configuration interface.
- For the home agent, configure an outgoing RADIUS user profile with IP routing to the foreign agent.

  Instead of an outgoing RADIUS user profile, you can set up a Connection profile to the foreign agent. For details, see the MAX *ISP and Telecommuting Configuration Guide*.
- Ensure that other hosts or networks can route to the mobile node.

Configuring ATMP in the home agent's Ethernet profile

To configure ATMP in the home agent's Ethernet profile, follow these steps:

1. Open the Ethernet menu.
2. Open the Mod Config menu.
3. Open the ATMP Options menu.
4. Set these parameters:

   ```
   ATMP options...
       ATMP Mode=Home
       Type=Router
       Password=private
       UDP Port=5150
   ```

   The value you specify for Password must match the value of the Ascend-Home-Agent-Password attribute in the mobile node's RADIUS user profile. All mobile node profiles that access this home agent must specify the *same* password for Ascend-Home-Agent-Password.
5. Save your changes.

Configuring an outgoing RADIUS user profile to the foreign agent

For the home agent, you must create an outgoing user profile with the foreign agent as its destination. Follow these steps:

1. On the first line of the user profile, specify the User-Name, Password, and User-Service attributes.

   Set the attributes on the first line in this way:

   – For the User-Name attribute, specify the name of the home agent, appending **`-Out`** to the user name.

   – Set Password="Ascend".

   – Set User-Service=Dialout-Framed-User. This setting ensures that RADIUS cannot use the profile for authentication of an incoming call.

   For example, you might enter this first line in the profile for the home agent Boston:

   `Boston-Out Password="Ascend", User-Service=Dialout-Framed-User`
2. On the second line of the user profile, specify the name of the home agent by indicating a value for the User-Name attribute.
3. To specify the encapsulation type in use on the line, set the Framed-Protocol attribute.
4. Enable IP routing for the profile by setting Ascend-Route-IP=Route-IP-Yes.
5. If the receiving end (the foreign agent) requires an IP address, and does not assign one dynamically, specify the home agent's IP address using the Framed-Address attribute (and, optionally, the Framed-Netmask attribute).

   The values of the Framed-Address and Framed-Netmask attributes for the local MAX must match the value of the NAS-Identifier attribute on the foreign agent. If there is no match, the home agent clears the call.
6. To indicate the phone number the MAX dials to reach the foreign agent, set the Ascend-Dial-Number attribute.

7. To specify the type of phone number the MAX dials, set the Ascend-PRI-Number-Type attribute.
8. Set the Ascend-Send-Auth attribute.
9. If you request PAP or CHAP authentication, you must also specify a password using Ascend-Send-Secret or Ascend-Send-Passwd.

This user profile enables a MAX called Boston to dial calls to the MAX at 1-800-555-1111:

```
Boston-Out Password="Ascend", User-Service=Dialout-Framed-User
    User-Name="Boston",
    Framed-Protocol=PPP,
    Ascend-Route-IP=Route-IP-Yes,
    Framed-Address=10.0.100.1,
    Framed-Netmask=255.255.255.0,
    Ascend-Metric=2,
    Framed-Routing=None,
    Ascend-Idle-Limit=30,
    Ascend-Dial-Number=1-800-555-1111,
    Ascend-PRI-Number-Type=National-Number,
    Ascend-Send-Auth=Send-Auth-PAP,
    Ascend-Send-Secret="Password1"
```

Ensuring that other hosts can route to the mobile node

When the home agent receives packets through the ATMP tunnel, it adds a host route to the mobile node in its IP routing table. It then handles routing in the usual way. To ensure that other hosts or networks can route to the mobile node, you can use one of the routing mechanisms described in Table 7-4.

Table 7-4. Routing mechanisms

Mode	Description
Routing Information Protocol (RIP)	If you enable RIP on the home agent’s Ethernet interface, other routers learn about the host route in RIP updates. Enabling RIP is particularly useful if the home network is one or more hops away from the home agent’s Ethernet.
Static route	If you turn off RIP on the home agent’s Ethernet interface, other routers require static routes that specify the home agent as the route to the mobile node.
Proxy Address Resolution Protocol (ARP)	If the home agent’s Ethernet interface is the home network (a direct connection), you should turn on proxy ARP (Proxy ARP=Always). Then, when local hosts ARP for the mobile node, the home agent responds on behalf of the mobile node.

Setting up a tunnel in gateway mode for an IP network

In gateway mode, the home agent forwards packets it receives through the tunnel to the home network across an open WAN connection. The home agent must have a nailed-up connection to the home network, because it will not dial the WAN connection based on packets it receives through the tunnel.

Figure 7-3 shows an ATMP gateway mode setup:

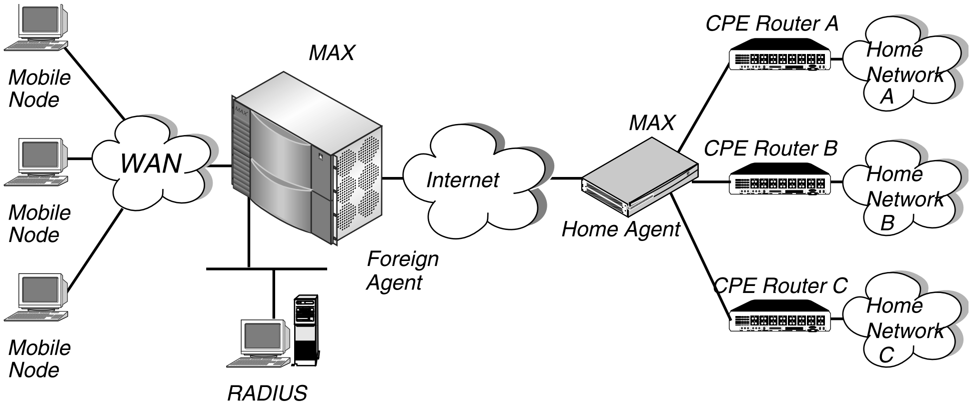

Figure 7-3. ATMP gateway mode

When the home agent is in gateway mode, it receives GRE-encapsulated IP packets from the foreign agent, strips off the encapsulation, and passes the packets across a nailed-up WAN connection to the home network.

To enable hosts and routers on the home network to reach the mobile node, you must configure a static route on the Customer Premises Equipment (CPE) router on the home network (not on the home agent). The static route must specify the home agent as the route to the mobile node. For information on setting up static IP routes, see “Configuring static IP routes” on page 6-15.

Configuring the foreign agent in gateway mode

To configure the foreign agent in gateway mode, you must perform these tasks:

- Configure ATMP in the foreign agent’s Ethernet profile using the MAX configuration interface.
- Configure the foreign agent to authenticate via RADIUS.
- Create an incoming RADIUS user profile for the mobile node.
- For the foreign agent, configure an outgoing RADIUS user profile with IP routing to the home agent.

  Instead of an outgoing RADIUS user profile, you can set up a Connection profile to the home agent. For details, see the MAX *ISP and Telecommuting Configuration Guide*.

Configuring ATMP in the foreign agent's Ethernet profile

To configure ATMP in the foreign agent's Ethernet profile, follow these steps:

1 Open the Ethernet menu.

2 Open the Mod Config menu.

3 Open the ATMP Options menu.

4 Set these parameters:

```
ATMP options...
    ATMP Mode=Foreign
    Type=N/A
    Password=N/A
    UDP Port=5150
```

5 Save your changes

Configuring the foreign agent to authenticate via RADIUS

Follow the instructions in "Configuring the MAX to use the RADIUS server" on page 2-4.

Configuring an incoming RADIUS user profile for the mobile node

To create a RADIUS users profile for the mobile node, follow these steps:

1 On the first line of the profile, specify the User-Name and Password attributes:

2 To specify the type of encapsulation in use for the call, set the Framed-Protocol attribute.

3 Enable IP routing for the profile by setting Ascend-Route-IP=Route-IP-Yes.

4 To specify the mobile node's IP address, set the Framed-Address attribute, and optionally, the Framed-Netmask attribute.

5 Set the Ascend-Primary-Home-Agent attribute.

This attribute specifies the first home agent the foreign agent tries to reach when setting up the ATMP tunnel, and indicates the UDP port the foreign agent uses for the link.

Specify the primary home agent using this syntax:

Ascend-Primary-Home-Agent="*hostname* **|** *ip_address* **[:***udp_port***]"**

– The ***hostname*** argument indicates the home agent's symbolic hostname.

– The ***ip_address*** argument indicates the home agent's IP address in dotted decimal notation. Specify an IP address if no DNS server exists for the home agent. You can specify a hostname or an IP address, but not both.

– The optional ***udp_port*** argument indicates the UDP port on which the foreign agent communicates with the home agent.

The default value is 5150.

– The colon (:) separates the hostname or IP address from the UDP port specification.

6 Set the Ascend-Secondary-Home-Agent attribute.

This attribute specifies the secondary home agent the foreign agent tries to reach when the primary home agent (specified by Ascend-Primary-Home-Agent) is unavailable. The attribute also indicates the UDP port the foreign agent uses for the link.

7 For the Ascend-Home-Agent-Password attribute, specify the home agent's password.

You must specify the same password indicated by the Password parameter in the Ethernet > Mod Config > ATMP Options menu on the home agent.

8 To identify the home agent's resident Connection profile to the home network, set the Ascend-Home-Network-Name attribute.

The Connection profile must have the ATMP Gateway parameter set to Yes in the Session Options submenu.

9 To specify the UDP port for ATMP operation, set the Ascend-Home-Agent-UDP-Port attribute.

By default, ATMP uses UDP port 5150 for communicating ATMP messages between the foreign and home agents. Both the foreign and home agent must agree on the UDP port number. If you specify a non-default UDP port number in one unit's configuration, make sure that the other end of the tunnel specifies the same number.

You need not specify a value for Ascend-Home-Agent-UDP-Port if you specify a UDP port number for Ascend-Primary-Home-Agent or Ascend-Secondary-Home Agent, or if you accept the default for any of these attributes.

The following profile specifies a mobile node named Node3 and a single home agent at the IP address 10.9.8.10. The home agent uses the Homenet Connection profile to the home network.

```
Node3 Password="Top-secret"
    Ascend-Metric=2,
    Framed-Protocol=PPP,
    Ascend-Route-IP=Route-IP-Yes,
    Framed-Address=200.1.1.2,
    Framed-Netmask=255.255.255.0,
    Ascend-Primary-Home-Agent=10.8.9.10,
    Ascend-Home-Agent-Password="private",
    Ascend-Home-Network-Name="Homenet"
```

When the mobile node logs into the foreign agent with the password Top-secret, the foreign agent authenticates the mobile node. The foreign agent then looks for a RADIUS user profile with an IP address that matches the Ascend-Primary-Home-Agent value, so it can bring up an IP connection to the home agent. Note that for an ATMP gateway mode connection, you must specify the name of the home agent's Connection profile to the home network using Ascend-Home-Network-Name.

Configuring an outgoing RADIUS user profile for the foreign agent

To configure an outgoing RADIUS user profile for the foreign agent with the home agent as the destination of the call, follow these steps:

1 On the first line of the user profile, specify the User-Name, Password, and User-Service attributes.

Set the attributes on the first line in this way:

- For the User-Name attribute, specify the name of the foreign agent, appending **`-Out`** to the user name.
- Set Password="Ascend".

   – Set User-Service=Dialout-Framed-User. This setting ensures that RADIUS cannot use the profile for authentication of an incoming call.

   For example, you might enter this first line in the profile for the foreign agent Alameda:

   Alameda-Out Password="Ascend", User-Service=Dialout-Framed-User

2. On the second line of the user profile, set the User-Name attribute to the name of the foreign agent.
3. To specify the encapsulation type in use on the line, set the Framed-Protocol attribute.
4. Enable IP routing for the profile by setting Ascend-Route-IP=Route-IP-Yes.
5. If the receiving end (the home agent) requires an IP address, and does not assign one dynamically, specify the foreign agent's IP address using the Framed-Address attribute (and, optionally, the Framed-Netmask attribute).

   The values of the Framed-Address and Framed-Netmask attributes for the local MAX must match the value of the NAS-Identifier attribute for the home agent. If there is no match, the home agent clears the call.
6. To indicate the phone number the MAX dials to reach the home agent, set the Ascend-Dial-Number attribute.
7. To specify the type of phone number the MAX dials, set the Ascend-PRI-Number-Type attribute.
8. Set the Ascend-Send-Auth attribute.

   The Ascend-Send-Auth attribute specifies the authentication protocol that the MAX requests when initiating a connection using PPP or MP+ encapsulation. The answering side of the connection determines which authentication protocol, if any, the connection uses.
9. If you request PAP or CHAP authentication, you must also specify a password using Ascend-Send-Secret or Ascend-Send-Passwd.

   Both of these attributes specify the password that the MAX sends to the remote end of a connection on outgoing calls. If the value you specify for Ascend-Send-Secret or Ascend-Send-Password does not match the value of the remote end's Ascend-Receive-Secret attribute (in a RADIUS user profile) or Recv PW parameter (in a Connection profile), the remote system rejects the call.

   Use Ascend-Send-Passwd only if your version of the MAX does not support Ascend-Send-Secret.

This user profile enables a MAX called Alameda to dial calls to the MAX at 1-800-555-5555:

```
Alameda-Out Password="Ascend", User-Service=Dialout-Framed-User
User-Name="Alameda",
    Framed-Protocol=PPP,
    Framed-Address=10.0.100.1,
    Framed-Netmask=255.255.255.0,
    Ascend-Route-IP=Route-IP-Yes,
    Ascend-Metric=2,
    Framed-Routing=None,
    Ascend-Idle-Limit=30,
    Ascend-Dial-Number=1-800-555-5555,
    Ascend-PRI-Number-Type=National-Number,
    Ascend-Send-Auth=Send-Auth-PAP,
    Ascend-Send-Secret="Password1"
```

Configuring the home agent in gateway mode

To configure the home agent in gateway mode, you must perform these tasks:

- Configure ATMP in the home agent's Ethernet profile using the MAX configuration interface.
- For the home agent, configure an outgoing RADIUS user profile to the foreign agent.

  Instead of an outgoing RADIUS user profile, you can set up a Connection profile to the foreign agent. For details, see the MAX *ISP and Telecommuting Configuration Guide*.
- Configure a nailed-up Connection profile to the home network using the MAX configuration interface.

  The Connection profile to the home network must be a resident profile. You cannot configure this profile in RADIUS.

Configuring ATMP in the home agent's Ethernet profile

To configure ATMP in the home agent's Ethernet profile, follow these steps:

1 Open the Ethernet menu.

2 Open the Mod Config menu.

3 Open the ATMP Options menu.

4 Set these parameters:

```
ATMP options...
    ATMP Mode=Home
    Type=Gateway
    Password=private
    UDP Port=5150
```

The value you specify for Password must match the value of the Ascend-Home-Agent-Password attribute in the mobile node's RADIUS user profile. All mobile node profiles that access this home agent must specify the *same* password for Ascend-Home-Agent-Password.

5 Save your changes.

Configuring an outgoing RADIUS user profile to the foreign agent

For the home agent, you must create an outgoing user profile with the foreign agent as its destination. Follow these steps:

1 On the first line of the user profile, specify the User-Name, Password, and User-Service attributes.

Set the attributes on the first line in this way:

– For the User-Name attribute, specify the name of the home agent, appending **`-Out`** to the user name.

– Set Password="Ascend".

– Set User-Service=Dialout-Framed-User. This setting ensures that RADIUS cannot use the profile for authentication of an incoming call.

For example, you might enter this first line in the profile for the home agent Boston:

Boston-Out Password="Ascend", User-Service=Dialout-Framed-User

2 On the second line of the user profile, specify the name of the home agent by indicating a value for the User-Name attribute.

3 To specify the encapsulation type in use on the line, set the Framed-Protocol attribute.

4 Enable IP routing for the profile by setting Ascend-Route-IP=Route-IP-Yes.

5 If the receiving end (the foreign agent) requires an IP address, and does not assign one dynamically, specify the home agent's IP address using the Framed-Address attribute (and, optionally, the Framed-Netmask attribute).

The values of the Framed-Address and Framed-Netmask attributes for the local MAX must match the value of the NAS-Identifier attribute on the foreign agent. If there is no match, the home agent clears the call.

6 To indicate the phone number the MAX dials to reach the foreign agent, set the Ascend-Dial-Number attribute.

7 To specify the type of phone number the MAX dials, set the Ascend-PRI-Number-Type attribute.

8 Set the Ascend-Send-Auth attribute.

9 If you request PAP or CHAP authentication, you must also specify a password using Ascend-Send-Secret or Ascend-Send-Passwd.

This user profile enables a MAX called Boston to dial calls to the MAX at 1-800-555-1111:

```
Boston-Out Password="Ascend", User-Service=Dialout-Framed-User
     User-Name="Boston",
     Framed-Protocol=PPP,
     Ascend-Route-IP=Route-IP-Yes,
     Framed-Address=10.0.100.1,
     Framed-Netmask=255.255.255.0,
     Ascend-Metric=2,
     Framed-Routing=None,
     Ascend-Idle-Limit=30,
     Ascend-Dial-Number=1-800-555-1111,
     Ascend-PRI-Number-Type=National-Number,
     Ascend-Send-Auth=Send-Auth-PAP,
     Ascend-Send-Secret="Password1"
```

Configuring a Connection profile for a nailed-up connection

To configure a Connection profile for a nailed-up connection to the home network, follow these steps:

1 Open the Ethernet menu.

2 Open the Connections menu.

3 Open a Connection profile.

4 For the Station parameter, specify the name of the home agent.

The value you enter becomes the name of the Connection profile. The name of this Connection profile must match the name specified by the Ascend-Home-Network-Name attribute in the mobile node's RADIUS user profile.

5. To activate the profile, set Active=Yes.
6. Set Encaps=FR.
7. To specify the type of phone number the MAX dials, set the PRI # Type parameter
8. Set Route IP=Yes.
9. Set Bridge=No.
10. In the Encaps Options submenu, set the FR Prof parameter to specify the name of the Frame Relay profile this connection uses.
11. For the DLCI parameter, specify the name of the DLCI used for the connection.
12. In the IP Options submenu, specify the IP address of the home agent.
13. In the Session Options submenu, set ATMP Gateway=Yes.
14. Close the Connection profile, saving your changes.

Your specifications might look like these:

```
Station=homenet
Active=Yes
Encaps=FR
PRI # Type=National
Dial #=N/A
Calling #=N/A
Route IP=Yes
Route IPX=N/A
Bridge=No
Dial brdcast=N/A
Encaps options...
    FR Prof=Pac Bell
    DLCI=18
IP options...
    LAN Adrs=10.9.8.32/24
Session options...
    ATMP Gateway=Yes
```

Tunneling ATMP between two IP networks

Typically, the mobile node at the remote end of an ATMP tunnel is a dial-in user. If the home network is an IP network, ATMP can also enable LAN-to-LAN connectivity through the tunnel. An IP router can connect as a mobile node. This functionality does not apply to IPX home networks.

When configuring ATMP for LAN-to-LAN connectivity, you follow the same steps as when you configure ATMP for a dial-in user, keeping in mind the additional instructions in this section.

For details on configuring a tunnel when the home agent is a router, see “Setting up a tunnel in router mode for an IP network” on page 7-6. For details on configuring a tunnel when the home agent is a gateway, see “Setting up a tunnel in gateway mode for an IP network” on page 7-13.

Specifying the mobile node’s subnet mask

To enable an IP router to connect as a mobile node, the foreign agent’s RADIUS entry for the mobile node must specify *the same subnet mask as the home network*.

For example, to connect to a home network whose router has the address 10.168.3.1/28, the foreign agent’s RADIUS entry for the remote router must contain these lines:

```
Framed-Address=10.168.6.21,
Framed-Netmask=255.255.255.240,
```

With this address for the mobile node router, the connecting LAN can support up to 14 hosts.

- The all zeros (network base) address for the subnet is 10.168.6.16.
  The network base address represents the network cable itself, which is always address 0 (zero).
- The all ones (broadcast) address for the subnet is 10.168.6.31.
  The broadcast address of any subnet is always all ones.
- The remaining host address range for the LAN is10.168.6.17 — 10.168.6.30
  In this example, the mobile node router has this address 10.168.6.21/28.

Configuring route handling between IP networks

The MAX handles routes to and from the mobile node’s LAN in different ways, depending on whether the home agent is in router mode or gateway mode.

Home agent in router mode

If the home agent connects directly to the home network, you must configure it to respond to ARP requests for the mobile node by setting Proxy ARP=Always.

If the home agent does not connect directly to the home network, the situation is the same as for any remote network—you must enable the router to learn about routes through dynamic updates, or you must configure static routes.

The mobile node always requires static routes to the home agent as well as to other networks it reaches through the home agent. (It cannot learn routes from the home agent.)

Home agent in gateway mode

If the home agent forwards packets from the mobile node across a nailed-up WAN link to the home IP network, the answering unit on the home network must have a static route to the mobile node's LAN.

In addition, because the mobile node and the home agent do not exchange routing information, the mobile node’s LAN can only support local subnets that fall within the network specified in the RADIUS entry.

For example, a mobile node router at the address 10.168.6.21/28 could support two subnets with a subnet mask of 255.255.255.248—one at the 10.168.6.16 address and the other at the 10.168.6.24 address. The answering unit on the home network would have only one route to the router itself (10.168.6.21/28).

Tunneling IPX across the Internet

ATMP tunnels enable remote NetWare clients to log into corporate IPX networks across the Internet by using a local ISP connection.

You can configure the home agent in an IPX routing connection in ATMP router mode or gateway mode, as defined in “ATMP router and gateway modes” on page 7-3. The example in this section shows router mode.

Configuring the foreign agent

For the home agent to route correctly to the mobile node, the foreign agent must specify a virtual IPX network number for its mobile nodes. This network number must be unique within the IPX routing domain. Typically, the foreign agent’s RADIUS profiles for mobile nodes all use the same virtual IPX network, with unique IPX node addresses on that virtual network. When the home agent receives IPX packets through the ATMP tunnel, it adds the unique virtual network number to its routing table.

To configure the foreign agent, you must perform these tasks:

- Configure ATMP in the foreign agent’s Ethernet profile using the MAX configuration interface.
- Configure the foreign agent to authenticate via RADIUS.
- Create an incoming RADIUS user profile for the mobile node.
- For the foreign agent, configure an outgoing RADIUS user profile with IP routing to the home agent.

  Instead of an outgoing RADIUS user profile, you can set up a Connection profile to the home agent. For details, see the MAX *ISP and Telecommuting Configuration Guide*.

Configuring ATMP in the foreign agent’s Ethernet profile

To configure ATMP in the foreign agent’s Ethernet profile, follow these steps:

1 Open the Ethernet menu.

2 Open the Mod Config menu.

3 Open the ATMP Options menu.

4 Set these parameters:

```
ATMP options...
    ATMP Mode=Foreign
    Type=N/A
    Password=N/A
    UDP Port=5150
```

5 Save your changes.

Configuring the foreign agent to authenticate via RADIUS

Follow the instructions in “Configuring the MAX to use the RADIUS server” on page 2-4.

Configuring an incoming RADIUS user profile for the mobile node

To create a RADIUS users profile for the mobile node, follow these steps:

1 On the first line of the profile, specify the User-Name and Password attributes:

2 To specify the type of encapsulation in use for the call, set the Framed-Protocol attribute.

3 To enable IPX routing, set Ascend-Route-IPX=Route-IPX-Yes.

4 To specify whether the mobile node is an IPX router or a device dialing in without an Ethernet interface, see the IPX-Peer-Dialin attribute.

5 To specify a virtual IPX network number that is unique within the enterprise, set the Framed-IPX-Network attribute.

You must specify the IPX network number in decimal format, not hexadecimal. (IPX network numbers are typically specified in hexadecimal.) It must be unique in the IPX routing domain. All mobile nodes logging into an IPX home network through the same foreign agent typically use the same Framed-IPX-Network number.

6 To assign the mobile node a unique IPX node address on the network specified by Framed-IPX-Network, set the Ascend-IPX-Node-Addr attribute.

The number you indicate must be unique for each mobile node on the virtual IPX network. Specify the number as a 12-digit string enclosed in double quotes. This value completes the IPX address of a mobile node.

7 Set the Ascend-Primary-Home-Agent attribute.

This attribute specifies the first home agent the foreign agent tries to reach when setting up the ATMP tunnel, and indicates the UDP port the foreign agent uses for the link.

Specify the primary home agent using this syntax:

Ascend-Primary-Home-Agent="*hostname* **|** *ip_address* **[:***udp_port***]"**

– The ***hostname*** argument indicates the home agent's symbolic hostname.

– The ***ip_address*** argument indicates the home agent's IP address in dotted decimal notation. Specify an IP address if no DNS server exists for the home agent. You can specify a hostname or an IP address, but not both.

– The optional ***udp_port*** argument indicates the UDP port on which the foreign agent communicates with the home agent. The default value is 5150.

– The colon (:) separates the hostname or IP address from the UDP port specification.

8 Set the Ascend-Secondary-Home-Agent attribute.

This attribute specifies the secondary home agent the foreign agent tries to reach when the primary home agent (specified by Ascend-Primary-Home-Agent) is unavailable. The attribute also indicates the UDP port the foreign agent uses for the link.

9 For the Ascend-Home-Agent-Password attribute, specify the home agent's password.

You must specify the same password indicated by the Password parameter in the Ethernet > Mod Config > ATMP Options menu on the home agent.

10 To identify the home agent's resident Connection profile to the home network, set the Ascend-Home-Network-Name attribute.

The named Connection profile must have the ATMP Gateway parameter set to Yes in the Session Options submenu.

11 To specify the UDP port for ATMP operation, set the Ascend-Home-Agent-UDP-Port attribute.

By default, ATMP uses UDP port 5150 for communicating ATMP messages between the foreign and home agents. Both the foreign and home agent must agree on the UDP port number. If you specify a non-default UDP port number in one unit's configuration, make sure that the other end of the tunnel specifies the same number.

You need not specify a value for Ascend-Home-Agent-UDP-Port if you specify a UDP port number for Ascend-Primary-Home-Agent or Ascend-Secondary-Home Agent, or if you accept the default for any of these attributes.

The following profile specifies a mobile node named Node2 and a single home agent at the IP address 10.9.8.10. The home agent uses the Homenet Connection profile to the home network:

```
Node2 Password="Top-secret"
    Ascend-Metric=2,
    Framed-Protocol=PPP,
    Ascend-Route-IPX=Route-IPX-Yes,
    Ascend-IPX-Peer-Mode=IPX-Peer-Dialin,
    Framed-IPX-Network=4999,
    Ascend-IPX-Node-Addr="001122334567",
    Ascend-Route-IPX=Route-IPX-Yes
    Ascend-Primary-Home-Agent=10.8.9.10,
    Ascend-Home-Agent-Password="private",
    Ascend-Home-Network-Name="Homenet"
```

When the mobile node logs into the foreign agent with the password Top-secret, the foreign agent looks for a Connection profile or RADIUS profile with an IP address that matches the Ascend-Primary-Home-Agent value, so it can bring up an IP connection to the home agent.

Configuring an outgoing RADIUS user profile for the foreign agent

To configure an outgoing RADIUS user profile for the foreign agent, follow these steps:

1 On the first line of the user profile, specify the User-Name, Password, and User-Service attributes.

Set the attributes on the first line in this way:

- For the User-Name attribute, specify the name of the foreign agent, appending **`-Out`** to the user name.
- Set Password="Ascend".
- Set User-Service=Dialout-Framed-User. This setting ensures that RADIUS cannot use the profile for authentication of an incoming call.

For example, you might enter this first line in the profile for the foreign agent Alameda:

```
Alameda-Out Password="Ascend", User-Service=Dialout-Framed-User
```

2 On the second line of the user profile, set the User-Name attribute to the name of the foreign agent.

3 To specify the encapsulation type in use on the line, set the Framed-Protocol attribute.

4 Enable IP routing for the profile by setting Ascend-Route-IP=Route-IP-Yes.

5 If the receiving end (the home agent) requires an IP address, and does not assign one dynamically, specify the foreign agent's IP address using the Framed-Address attribute (and, optionally, the Framed-Netmask attribute).

The values of the Framed-Address and Framed-Netmask attributes for the local MAX must match the value of the NAS-Identifier attribute on the home agent. If there is no match, the home agent clears the call.

6 To indicate the phone number the MAX dials to reach the home agent, set the Ascend-Dial-Number attribute.

7 To specify the type of phone number the MAX dials, set the Ascend-PRI-Number-Type attribute.

8 Set the Ascend-Send-Auth attribute.

The Ascend-Send-Auth attribute specifies the authentication protocol that the MAX requests when initiating a connection using PPP or MP+ encapsulation. The answering side of the connection determines which authentication protocol, if any, the connection uses.

9 If you request PAP or CHAP authentication, you must also specify a password using Ascend-Send-Secret or Ascend-Send-Passwd.

Both of these attributes specify the password that the MAX sends to the remote end of a connection on outgoing calls. If the value you specify for Ascend-Send-Secret or Ascend-Send-Password does not match the value of the remote end's Ascend-Receive-Secret attribute (in a RADIUS user profile) or Recv PW parameter (in a Connection profile), the remote system rejects the call.

Use Ascend-Send-Passwd only if your version of the MAX does not support Ascend-Send-Secret.

This user profile enables a MAX called Alameda to dial calls to the MAX at 1-800-555-5555:

```
Alameda-Out Password="Ascend", User-Service=Dialout-Framed-User
      User-Name="Alameda",
      Framed-Protocol=PPP,
      Ascend-Route-IP=Route-IP-Yes,
      Framed-Address=10.0.100.1,
      Framed-Netmask=255.255.255.0,
      Ascend-Metric=2,
      Framed-Routing=None,
      Ascend-Idle-Limit=30,
      Ascend-Dial-Number=1-800-555-5555,
      Ascend-PRI-Number-Type=National-Number,
      Ascend-Send-Auth=Send-Auth-PAP,
      Ascend-Send-Secret="Password1"
```

Configuring the home agent

The home agent adds an entry to its IPX routing table for the virtual IPX network number that the foreign agent sends in the Framed-IPX-Network attribute. This entry enables the home agent to route IPX packets from the home network back to mobile nodes.

To configure the home agent in router mode, you must perform these tasks:

- Configure ATMP in the home agent’s Ethernet profile using the MAX configuration interface.
- Configure an outgoing RADIUS user profile to the foreign agent.

  Instead of an outgoing RADIUS user profile, you can set up a Connection profile to the foreign agent. For details, see the MAX *ISP and Telecommuting Configuration Guide*.

Configuring ATMP in the home agent’s Ethernet profile

To configure ATMP in the home agent’s Ethernet profile, follow these steps:

1 Open the Ethernet menu.

2 Open the Mod Config menu.

3 Open the ATMP Options menu.

4 Set these parameters:

```
ATMP options...
    ATMP Mode=Home
    Type=Router
    Password=private
    UDP Port=5150
```

The value you specify for Password must match the value of the Ascend-Home-Agent-Password attribute in the mobile node’s RADIUS user profile. All mobile node profiles that access this home agent must specify the *same* password for Ascend-Home-Agent-Password.

5 Save your changes.

Configuring an outgoing RADIUS user profile to the foreign agent

For the home agent, you must create an outgoing user profile with the foreign agent as its destination. Follow these steps:

1 On the first line of the user profile, specify the User-Name, Password, and User-Service attributes.

Set the attributes on the first line in this way:

– For the User-Name attribute, specify the name of the home agent, appending **`-Out`** to the user name.

– Set Password=“Ascend”.

– Set User-Service=Dialout-Framed-User. This setting ensures that RADIUS cannot use the profile for authentication of an incoming call.

For example, you might enter this first line in the profile for the home agent Boston:

```
Boston-Out Password="Ascend", User-Service=Dialout-Framed-User
```

2 On the second line of the user profile, specify the name of the home agent by indicating a value for the User-Name attribute.

3 To specify the encapsulation type in use on the line, set the Framed-Protocol attribute.

4 Enable IP routing for the profile by setting Ascend-Route-IP=Route-IP-Yes.

5. If the receiving end (the foreign agent) requires an IP address, and does not assign one dynamically, specify the home agent's IP address using the Framed-Address attribute (and, optionally, the Framed-Netmask attribute).

   The values of the Framed-Address and Framed-Netmask attributes for the local MAX must match the value of the NAS-Identifier attribute on the foreign agent. If there is no match, the home agent clears the call.
6. To indicate the phone number the MAX dials to reach the foreign agent, set the Ascend-Dial-Number attribute.
7. To specify the type of phone number the MAX dials, set the Ascend-PRI-Number-Type attribute.
8. Set the Ascend-Send-Auth attribute.
9. If you request PAP or CHAP authentication, you must also specify a password using Ascend-Send-Secret or Ascend-Send-Passwd.

This user profile enables a MAX called Denver to dial calls to the MAX at 1-800-555-7777:

```
Denver-Out Password="Ascend", User-Service=Dialout-Framed-User
     User-Name="Denver",
     Framed-Protocol=PPP,
     Ascend-Route-IP=Route-IP-Yes,
     Framed-Address=10.0.100.1,
     Framed-Netmask=255.255.255.0,
     Ascend-Metric=2,
     Framed-Routing=None,
     Ascend-Idle-Limit=30,
     Ascend-Dial-Number=1-800-555-7777,
     Ascend-PRI-Number-Type=National-Number,
     Ascend-Send-Auth=Send-Auth-PAP,
     Ascend-Send-Secret="Password1"
```

Setting up the MAX as a multi-mode agent

You can configure the MAX to act as a home agent or a foreign agent on a tunnel-by-tunnel basis. A typical network topology appears in Figure 7-4.

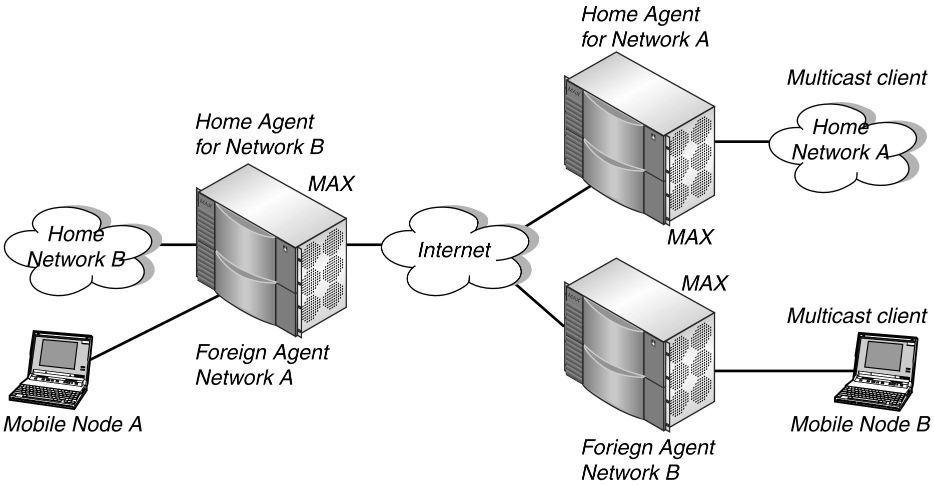

Figure 7-4. The MAX acting as a home agent and a foreign agent

To configure the MAX to act as a foreign agent and home agent on a tunnel-by-tunnel basis, follow these steps:

1 Open the Ethernet menu.

2 Open the Mod Config menu.

3 Open the ATMP Options menu.

4 Set ATMP Mode=Both.

This setting indicates that the MAX will function as both a home agent and foreign agent on a tunnel-by-tunnel basis.

5 Set the Type parameter to Router or Gateway, as appropriate.

6 For the Password parameter, specify a password.

The mobile node must specify this password only when the unit acts as its home agent.

7 Set SAP Reply to Yes or No.

This parameter applies only when the unit is acting as a home agent. It enables or disables a home agent’s ability to reply to the mobile node’s IPX Nearest Server Query. If you set SAP Reply=Yes, the home agent replies to the mobile node’s Nearest Server Query if it knows about a server on the home network. If you set SAP Reply=No, the home agent simply tunnels the mobile node’s request to the home network.

8 For the UDP Port parameter, specify the UDP port or accept the default of 5150.

9 Save your changes.

Setting up ATMP to bypass a foreign agent

If a home agent MAX has the appropriate RADIUS entry for a mobile node, the mobile node can connect directly to the home agent, bypassing the foreign agent entirely.

An ATMP-based RADIUS entry local to the home agent enables the mobile node to bypass a foreign agent connection, but it does not preclude a foreign agent. If both the home agent and the foreign agent have local RADIUS profiles for the mobile node, the node can choose between a direct connection or a tunneled connection through the foreign agent.

For information about how to set up a RADIUS user profile for the mobile node in router mode, see “Configuring an incoming RADIUS profile for the mobile node” on page 7-8. For information about how to set up a RADIUS user profile for the mobile node in gateway mode, see “Configuring an incoming RADIUS user profile for the mobile node” on page 7-14.

In this example, the RADIUS user profile authenticates a mobile NetWare client that connects directly to a home agent in gateway mode.

```
Mobile-IPX Password="unit"
        User-Service=Framed-User,
        Ascend-Route-IPX=Route-IPX-Yes,
        Framed-Protocol=PPP,
        Ascend-IPX-Peer-Mode=IPX-Peer-Dialin,
        Framed-IPX-Network=40000000,
        Ascend-IPX-Node-Addr=12345678,
        Ascend-Primary-Home-Agent=192.168.6.18,
        Ascend-Home-Network-Name="Dave’s Max",
        Ascend-Home-Agent-Password="Pipeline"
```

If the home agent were in router mode, you would not include the Ascend-Home-Network-Name line in the user entry. The Ascend-Home-Network-Name attribute specifies the name of the answering unit across the WAN on the home IPX network.

Configuring call routing to PPTP servers

You can use RADIUS to route PPP calls to the Point-to-Point Tunneling Protocol (PPTP) server based on the calling or dialed number, and access more than four PPTP servers.

Creating tunnels on a per-user basis

In previous releases, when a client dialed into the MAX and wanted to use a PPTP tunnel, the MAX chose a tunnel on the basis of the Route Line *n* parameters. Each T1 PRI line was associated with a different Route Line *n* parameter. Each parameter specified a particular PPTP server at the end of the PPTP tunnel. The MAX simply created a tunnel for each T1 line on which the user connected.

While you can still use the Route Line *n* parameters to create tunnels on the basis of the T1 line, you can now create a tunnel on a per-user basis as well. In a RADIUS user profile, you specify the IP address or host name of a PPTP server. The profile creates a tunnel between the MAX and the PPTP server. When the name and password of an incoming call match the name and password in a RADIUS user profile set up for PPTP, the MAX creates the PPTP tunnel to the PPTP server.

The changes to PPTP functionality affect PPP connections and terminal-server users. This release includes the following new RADIUS attributes:

- Tunnel-Type (64)
- Tunnel-Medium-Type (65)
- Tunnel-Server-Endpoint (66)
- Tunnel-Client-Endpoint (67)
- Tunnel-ID (68)

Attributes for routing PPTP on the basis of CLID or DNIS

You can use PPP authentication (CLID and DNIS) to tunnel to PPTP. You are not required to dedicate a T1 line to each destination PNS address, and you are not limited to four PPTP servers, as was the case in previous releases.

Note: It is still possible to dedicate a WAN line to PPTP.

When a PPP call comes in on any WAN line and the authentication process begins, the MAX will first check whether the line is a dedicated PPTP line (the same behavior as previously).

However, if the line is not a PPTP line, the MAX will check the data returned from RADIUS to determine whether:

- CLID or DNIS is supported
- the call is PPTP-based

If the call is a PPTP call and CLID or DNIS is supported, the RADIUS information returned will specify a server endpoint and MAX will route the call through PPTP to the endpoint server. The PPTP server then communicates with the caller.

Example RADIUS entries

The following examples show RADIUS entries for CLID and DNIS. The MAX must have RADIUS user entries that specify DNIS.

CLID RADIUS entry

```
5105551212 Password = "Ascend-CLID"
        Tunnel-Server-Endpoint = "192.168.6.199",
        Tunnel-Type = PPTP,
        Tunnel-Medium-Type = IP
```

DNIS RADIUS entry

```
7894 Password = "Ascend-DNIS"
        Tunnel-Server-Endpoint = "eng-lab-199",
        Tunnel-Type = PPTP,
        Tunnel-Medium-Type = IP
```

Setting Up RADIUS Accounting

8

This chapter discusses how to set up RADIUS accounting. This chapter contains:

What is RADIUS accounting?

RADIUS accounting is a way to log information about three types of events:

- Start session

  This event denotes the beginning of a session with the MAX. Information about this event appears in an accounting Start record.

- Stop session

  This event denotes the end of a session with the MAX. Information about this event appears in an accounting Stop record.

- Failure-to-start session

  This event denotes that a login attempt has failed. Information about this event appears in an accounting Failure-to-start record.

When the MAX recognizes one of these events, it sends an accounting request to RADIUS. When the accounting server receives the request, it combines the information into a record and timestamps it. Each type of accounting record contains attributes associated with an event type, and can show the number of packets the MAX transmits and receives, the protocol in use, the username and IP address of the client, and so on.

You can also specify that RADIUS send periodic Checkpoint records during a user's session. If there is a disruption in the network that disconnects active users, you can use these Checkpoint records to reconstruct usage in the absence of accounting Stop records. See "Accounting attributes in Checkpoint records" on page 8-22 for more information.

You can use RADIUS accounting for either of these purposes:

- To gather billing information.

  You can use the information in an accounting record to determine who called, how long the session lasted, and how much traffic occurred during the session.

- To perform troubleshooting of RADIUS and MAX operations.

  Accounting records can contain information about how many login failures occurred, and can describe the characteristics of the failed attempts.

- to determine whether RADIUS accounting is enabled, and the specific time when an accounting server begins operating or is stopped.

Where are accounting records stored?

The RADIUS accounting server writes each record to a log file. If you are running an unmodified Ascend RADIUS daemon, the names 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 unit's symbolic hostname or IP address in dotted decimal notation.

What kinds of packets does RADIUS accounting use?

RADIUS accounting makes use of these kinds of Accounting packets:

- Accounting Start packets, signaling a Start session event

  When the MAX begins a terminal server, bridging, or routing session, and the call passes authentication or the user logs in, the MAX 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. In some cases, a session begins with a user login and then authentication follows, such as when a terminal server user chooses PPP or SLIP after login.

  If User-Service=Login-User, or if User-Service is unspecified, the MAX sends an Accounting Start packet after login. Information from an Accounting Start packets appears in a Start record in the log file.

  Note: Set Ethernet > Mod Config > Auth > Framed Addr Start to Yes to direct the MAX to generate a second Start record when a user logs in using the terminal server and starts a PPP session. The second Start records contains the user's Framed-Address and Framed-Protocol attributes.

- Accounting Stop packets, signaling a Stop session or Failure-to-start session event.

  At the end of a session, including cases in which a user fails to authenticate, the MAX sends an Accounting Stop packet. Information from an Accounting Stop packet appears in a Stop record or Failure-to-start record in the log file.

- Failure-to-start packets, indicating that a login attempt has failed. Information from a Failure-to-start packet appears in a call logging Failure-to-start record.

  When the MAX recognizes a call logging event, it sends a call logging request to the call logging server. When the call logging server receives the request, it combines the information into a record and timestamps it. Each type of call logging record contains attributes associated with an event type, and can show the number of packets the MAX transmits and receives, the protocol in use, the user name and IP address of the client, and so on.

  For information on setting up call logging, see "Configuring call logging on a system-wide basis" on page 8-5.

- Accounting checkpoint packets, sent during an active user session at intervals you specify.

  These enable you to reconstruct information on each user session before a disruption if connectivity is lost before a RADIUS stop record can be sent for the session.
- Ascend-Event-Request packets, signaling the occurence of an event, such as a coldstart.
- Ascend-Event-Response packets, sent in response to an Ascend-Event-Request packet.

Note: For more information on the kinds of information RADIUS accounting records can convey in the attributes they contain, and which kinds of packets can contain these attributes, see “Understanding accounting records” on page 8-13.

Setting up RADIUS accounting

When you configure RADIUS accounting, you carry out one or more of these tasks:

- Install and configure the RADIUS daemon.
- Specify system-wide accounting server parameters.
- Configure system-wide call logging, ifyou plan to send records to a different call logging server than the primary RADIUS accounting server.
- Configure accounting on a per-user basis.
- Use SNMP to specify the primary RADIUS server.
- Configure accounting with dynamic IP addressing

Installing and configuring the RADIUS daemon for accounting

Follow these steps:

1 Install the most recent Ascend RADIUS daemon, as described in “Installing the RADIUS daemon” on page 2-2.

2 Add a line to /etc/services file identifying the RADIUS daemon’s accounting port.

For example, you might enter this command line:

```
radacct   1646/udp   #radius-accounting
```

The port number you specify must match the port number indicated by the Acct Port parameter in the Ethernet>Mod Config>Accounting menu, as discussed in step 6 on page 1-4. You can use a value other than 1646, as long as the Acct Port setting matches the value.

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

Or, when starting the daemon, you can use the –a option 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 in the directory you specify using the -a option. The *detail* file will contain accounting records.

4 Start the RADIUS daemon with the –A option enabled.

To start the RADIUS daemon using a flat ASCII file, enter this command line:

```
radiusd -A services | incr
```

When you specify the **`services`** argument, the daemon creates the accounting process only if a line defining the UDP port to use for accounting appears in the /etc/services file. Otherwise, daemon does not start.

When you specify the `incr` argument, the daemon creates the accounting process with the UDP port specified as the accounting port in the /etc/services file. If you have not defined the port, the daemon increments the UDP port specified for radiusd and uses that port number. This action is the default you do not specify the **`-A`** argument.

To start the RADIUS daemon using a UNIX DBM database, enter this command line:

```
radiusd.dbm -A services
```

You must specify the **`services`** argument when you start the daemon in DBM mode.

Specifying system-wide accounting parameters on the MAX

To set accounting parameters that affect all users on a system-wide basis, follow these steps:

1 In the MAX configuration interface, open the Ethernet menu.

2 Open the Mod Config menu.

3 Open the Accounting menu.

4 Set Acct=RADIUS.

This setting indicates that the MAX sends accounting information to the RADIUS server specified by Acct Host #1, Acct Host #2, or Acct Host #3, whichever is available.

5 For each Acct Host parameter, specify the IP address of a RADIUS accounting server.

You can specify up to three addresses. The MAX first tries to connect to Acct Host #1. If it receives no response within the time specified by the Acct Timeout parameter, it tries to connect to Acct Host #2. If it again receives no response within the time specified by Acct Timeout, it tries to connect to Acct Host #3. If the MAX unit’s request again times out, it reinitiates the process with Acct Host #1. The MAX can complete this cycle of requests a maximum of ten times.

When it successfully connects to an accounting server, the MAX uses that machine until it fails to serve requests. By default, the MAX does not use the first host until the second machine fails, even if the first host has come online while the second host is still servicing requests. However, you can use SNMP to specify that the MAX use the first host again. For details, see “Specifying when the MAX uses the primary accounting server” on page 8-11.

You can also specify the same address for all three Acct Host parameters. If you do so, the MAX keeps trying to create a connection to the same server.

6 For the Acct Port parameter, enter the UDP port number you specified for the authentication process of the daemon in /etc/services.

Or, if you used the `incr` keyword with the –A option when starting the daemon, specify the number of the UDP port for authentication services + 1.

7 To specify the number of seconds the MAX waits for a response to a RADIUS accounting request, set the Acct Timeout parameter.

You can specify a value between 1 and 10. The default value is 1.

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

9 Set the Sess Timer parameter.

The MAX can report the number of sessions by class to a RADIUS accounting server. The Sess Timer parameter specifies the interval in seconds in which the MAX sends session reports. You can specify a number between 0 and 65535.The default value is 0 (zero), which indicates that the MAX does not send reports on session events.

10 To specify whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16, set the Acct-ID Base parameter.

This parameter controls how the MAX presents the Acct-Session-ID attribute to the accounting server. You can specify one of these settings:

- 10 (decimal) indicates that the numeric base is 10. The default value is 10.
- 16 (hexadecimal) indicates that the numeric base is 16.

For example, when you set Acct-ID Base=10, the MAX presents a typical session ID to the accounting server in this way:

"1234567890"

When you set Acct-ID Base=16, the MAX presents the same session ID in this way:

"499602D2"

Note: Changing the value of Acct-ID Base while sessions are active results in inconsistent reporting between the Start and Stop records.

11 To specify the source port to use for sending a RADIUS accounting request, set the Acct Src Port parameter.

Specify a port number between 0 and 65535. The default value is 0 (zero). If you accept this value, the Ascend unit can use any port number between 1024 and 2000. You can specify the same source port for authentication and accounting requests.

12 Specify the number of time the MAX sends an accounting request before it gives up in the Acct Max Retry parameter.

Enter an integer to specify the maximum number of retries permitted. Enter a 0 to disable this feature.

13 Set the Allow Stop Only parameter to specify whether the MAX can send accounting Stop packets that do not contain a username to the RADIUS server.

Yes allows the MAX to send a Stop packet with no username if a connection is terminated before authentication occurs or if the password supplied by the user if rejected. No prevents the MAX from sending such a Stop packet.

14 Set the Acct Checkpoint parameter to specify the interval at which the MAX sends checkpoint log records for an active user session.

Enter a number between 0 to 60 to specify the interval in minutes. 0 is the default, and specifies that the MAX send no checkpoint messages.

15 Save your changes.

Configuring call logging on a system-wide basis

Call Logging is a way to track information about three types of events:

- Start session. Denotes the beginning of a session with the MAX. Information about this event appears in an logging Start record.
- Stop session. Denotes the end of a session with the MAX. Information about this event appears in a call logging Stop record.
- Failure-to-start session. Denotes that a login attempt has failed. Information about this event appears in a call logging Failure-to-start record.

When the MAX recognizes a call logging event, it sends a call logging request to the call logging server. When the call logging server receives the request, it combines the information into a record and timestamps it. Each type of call logging record contains attributes associated with an event type, and can show the number of packets the MAX transmits and receives, the protocol in use, the user name and IP address of the client, and so on.

You can use call logging for either of the following purposes:

- To gather management information. You can use the information in a call logging record to determine who called, how long the session lasted, and how much traffic occurred during the session.

To perform troubleshooting. Call Logging records can contain information about how many login failures occurred, and can describe the characteristics of the failed attempts.

Performing required accounting configuration tasks

When you set up call logging, you must specify:

- System-wide call logging parameters
- Call Logging port in `/etc/services`
- Call Logging directory

Specifying system-wide call logging parameters on the MAX

To set accounting parameters that affect all users on a system-wide basis, perform the following steps at the MAX configuration interface:

1. In the External-Auth profile, set Acct-Type =RADIUS.
2. Open the Call Logging subprofile.
3. For each Host #*n* parameter, specify the IP address of a Call Logging host.
4. For the Dst Port parameter, enter the UDP port number you specified, in `/etc/services`, for the authentication process of the daemon. Or, if you used the **`incr`** keyword with the –A option when starting the daemon, add 1 to the number of the UDP port for authentication services and enter the sum.
5. For the `Key` parameter, enter the RADIUS client password, exactly as it appears in the RADIUS clients file.

Specifying the call logging port

Add to the /etc/services file a line identifying the RADIUS daemon’s call logging port. Use the following format:

```
radacct   1646/udp   #Call Logging
```

The port number you specify must match the port number indicated by the Dst Port parameter in the Call Logging subprofile.

Specifying the call logging directory

Create the `/usr/adm/radacct` directory. Or, when starting the daemon, use the –a option to specify a different directory in which to store call logging information. The call logging process in the daemon creates a file named `detail` in /usr/adm/radacct, or in the directory you specify with the `-a` option. The `detail` file contains call logging records.

Performing optional call logging configuration tasks

When you configure call logging, you may optionally specify:

- Timeout value
- Numeric base for the session ID
- Call Logging port

You set each value in the Call Logging subprofile.

Specifying a timeout value

To specify the number of seconds the MAX waits for a response to a call logging request, set the Acct-Timeout parameter to a value between 1 and 10. The default value is 1.

Specifying the numeric base for the session ID

The Acct-Session-Id attribute is a unique numeric string identified with the session reported in an call logging packet. The Acct-ID Base parameter controls whether the MAX presents Acct-Session-ID to the call logging server in base 10 or base 16. You can specify one of the following settings for the Acct-Id-Base parameter:

- Acct-Base-10 (decimal) indicates that the numeric base is 10. The default value is 10.
- Acct-Base-16 (hexadecimal) indicates that the numeric base is 16.

For example, when you set Acct-Id-Base=Acct-Base-10, the MAX presents a typical session ID to the call logging server in the following format:

```
"1234567890"
```

When you set Acct-Id-Base=Acct-Base-16, the MAX presents the same session ID in the following format:

```
"499602D2"
```

Note: Changing the value of Acct-Id-Base while sessions are active creates inconsistencies between the Start and Stop records.

Specifying the call logging port

To specify the source port the MAX uses to send a call logging request, set the Dst Port parameter to a value between 0 and 65535. The default value is 0 (zero), which specifies that the Ascend unit can use any port number between 1024 and 2000. You may specify the same source port for authentication and call logging requests.

Setting up call logging with dynamic IP addressing

In some networks, the call logging server requires an IP address for all callers. For callers that receive an IP address from a pool, this requirement presents a problem. During PPP authentication, RADIUS verifies the name and password information, but not the IP address of the caller.

To track calls during the authentication period, you must set up one or more IP address pools, as described elsewhere. Then, in the Rad-Auth-Client subprofile of the External-Auth profile, set Auth-Pool=Yes.

When Auth-Pool=Yes, the MAX includes the caller's assigned IP address as the value of the Framed-Address attribute. The MAX allocates this address from pool #1. (If you do not define pool #1, the call does not have an IP address during authentication.) Because an IP assignment is not usually part of an Access-Request, you must modify the RADIUS daemon.

The assigned IP address might not last the duration of the connection, or it might not be meaningful. Here are five possibilities:

- If Assign-Address=No in the IP-Answer subprofile of the Answer-Defaults profile, and the caller's RADIUS user profile does not supply an IP address for the caller, the MAX returns the IP address to pool #1. However, the address continues to appear in call logging entries.
- If Assign-Address=No and the caller's RADIUS user profile supplies an IP address for the caller, the MAX returns the IP address to pool #1. The IP address from the user profile appears in call logging entries.
- If Assign-Address=Yes, and Ascend-Assign-IP-Pool in the RADIUS user profile points to a pool that has no valid IP address, the IP address from pool #1 appears in call logging entries. The MAX returns the address to the pool only when the call disconnects.
- If Assign-Address=Yes and Must-Accept-Address-Assign=Yes on the MAX, and Ascend-Assign-IP-Pool points to a pool that has a valid IP address, the IP address from that pool appears in call logging entries for the duration of the call. The MAX returns the address to the pool when the call disconnects.
- If Assign-Address=Yes, Must-Accept-Address-Assign=No, Ascend-Assign-IP-Pool points to a pool that has a valid IP address, and the caller does not specify an address, the IP address from the pool appears in call logging entries. If the caller does specify an IP address, that address appears in call logging entries.

Configuring accounting on a per-user basis

A network reseller can service many different ISPs, each with a different access policy. The reseller carries traffic for individual users and must filter and bill this usage according to the policies of the appropriate ISP.

The per-user accounting feature allows a network reseller to direct accounting information about specific users to a RADIUS server belonging to each ISP. Each RADIUS user profile can determine the accounting policy by specifying that accounting data goes to one of these locations:

- The RADIUS accounting server specified by the Ascend-User-Acct-Host attribute in the RADIUS user profile.
- The default server specified in the Ethernet>Mod Config>Accounting menu by Acct Host #1, Acct Host #2, or Acct Host #3, whichever is available.

  By default, the MAX uses the server specified in the Accounting menu.
- Both servers.

When an accounting event occurs, the MAX sends an accounting message to the appropriate server. The MAX places each accounting message on a list and waits for an acknowledgment from the RADIUS server. If an acknowledgment does not arrive within the period of time specified by the Acct Timeout parameter, the MAX resends the accounting message, up to the maximum you specify in the Acct Max Retry parameter. RADIUS discards the oldest entry on the list when the total number of entries exceeds the maximum.

When you set up accounting on a per-user basis, you use the attributes specified in Table 8-1.

Table 8-1. Per-user accounting attributes

Attribute	Description	Possible values
Ascend-User-Acct-Base (142)	Specifies whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16.	Ascend-User-Acct-Base-10 (0) Ascend-User-Acct-Base-16 (1) The default value is Ascend-User-Acct-Base-10.
Ascend-User-Acct-Host (139)	Specifies the IP address of the RADIUS server to use for this connection.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0.
Ascend-User-Acct-Key (141)	Specifies the RADIUS client password as it appears in the clients file.	Text string. The default value is null.
Ascend-User-Acct-Port (140)	Specifies a UDP port number for the connection.	The UDP port number you indicated for the authentication process of the daemon in /etc/services. Or, if you used the **`incr`** keyword to the –A option when starting the daemon, the number of the UDP port to use for authentication services + 1. You can specify a number between 1 and 32767.
Ascend-User-Acct-Time (143)	Specifies the number of seconds the MAX waits for a response to a RADIUS accounting request.	Integer from 1 to 10. The default value is 1.
Ascend-User-Acct-Type (138)	Specifies the RADIUS accounting server(s) to use for this connection.	Ascend-User-Acct-None (0) Ascend-User-Acct-User (1) Ascend-User-Acct-User-Default (2) The default value is Ascend-User-Acct-None.

To specify a RADIUS accounting server in a RADIUS user profile, follow these steps:

1 Set up the RADIUS user profile, as discussed in the preceding chapters.

2 Set the Ascend-User-Acct-Type attribute.

You can specify one of these settings:

- Ascend-User-Acct-None (0). This setting indicates that the MAX sends accounting information to the RADIUS server specified by the Acct Host #1, Acct Host #2, or Acct Host #3 parameter in the Ethernet>Mod Config>Accounting menu, depending on which server is available. This server is known as the default server.
- Ascend-User-Acct-User (1). This setting indicates that the MAX sends accounting information to the RADIUS server specified by the Ascend-User-Acct-Host attribute in the RADIUS user profile.
- Ascend-User-Acct-User-Default (2). This setting indicates that the MAX sends accounting information both to the RADIUS server specified by the Ascend-User-Acct-Host attribute in the RADIUS user profile and to the default server.

3 To specify the IP address of the RADIUS accounting server to use for this connection, set the Ascend-User-Acct-Host attribute.

4 For the Ascend-User-Acct-Port attribute, enter the UDP port number you specified for the authentication process of the daemon in /etc/services.

Or, if you used the **`incr`** keyword to the –A option when starting the daemon, specify the number of the UDP port to use for authentication services + 1. You can specify a number between 1 and 32767.

5 To specify the number of seconds the MAX waits for a response to a RADIUS accounting request, set the Ascend-User-Acct-Time attribute.

You can specify a number between 1 and 10. The default value is 1.

If the MAX does not receive a response within the time specified by Ascend-User-Acct-Time, it sends the accounting request to the next accounting server specified by the Acct Host parameter, to the server specified by the Ascend-User-Acct-Host attribute, or both. If Acct=User+Default or Ascend-User-Acct-Type=Ascend-User-Acct-User-Default, the MAX sends two different packets—one to the server defined in the user profile, and one to the default server.

6 For the Ascend-User-Acct-Key attribute, specify the RADIUS client password exactly as it appears in the RADIUS clients file.

7 To specify whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16, set the Ascend-User-Acct-Base attribute.

This attribute controls how the MAX presents the Acct-Session-ID attribute to the accounting server. You can specify one of these settings:

- Ascend-User-Acct-Base-10 indicates that the numeric base is 10. The default value is 10.
- Ascend-User-Acct-Base-16 indicates that the numeric base is 16.

For example, when you set Ascend-User-Acct-Base=Ascend-User-Acct-Base-10, the MAX presents a typical session ID to the accounting server in this way:

"1234567890"

When you set Ascend-User-Acct-Base=Ascend-User-Acct-Base-16, the MAX presents the same session ID in this way:

"499602D2"

Note: Changing the value of Ascend-User-Acct-Base while sessions are active results in inconsistent reporting between the Start and Stop records.

Specifying when the MAX uses the primary accounting server

By default, if the MAX uses a secondary RADIUS accounting server because the primary one goes out of service, and does not return to the first host until the second machine fails. This situation occurs even if the first host has come online while the second host is still servicing requests.

However, you can specify that the MAX use the primary accounting server in two ways:

- Use an SNMP set command to specify that the MAX use the first host again.

  Such a need might arise if the primary server is shut down for service and then becomes available again. Every time you reset the server using the set command, the MAX generates an SNMP trap. The MAX also generates a trap if it changes to the next server because the current server fails to respond.

  For details, see the Ascend Enterprise MIB. You can download the most up-to-date verson of the Ascend Enterprise MIB by logging in as *anonymous* to ftp.ascend.com. (No password is required.)
- Set Acct Reset Timeout in the Ethernet Profile to a value other than zero (0).

Configuring accounting with dynamic IP addressing

In some networks, the RADIUS accounting server needs to have an IP address for all callers. This situation presents a problem during the authentication part of PPP for callers that receive an IP address from a pool. During authentication, RADIUS verifies the name and password information, but not the IP address of the caller. To track calls during this period, follow these steps:

1 Set up one or more IP address pools.

For details, see “Defining a pool of IP addresses for dynamic assignment” on page 6-8.

2 In the MAX configuration interface, open the Ethernet menu.

3 Open the Mod Config menu.

4 Open the Auth menu.

5 Set Auth Pool=Yes.

When Auth Pool=Yes, the MAX includes the caller's assigned IP address in a specially modified Access-Request packet. Since an IP assignment is not normally part of an Access-Request, you must modify the RADIUS daemon receiving the message to receive the Framed-Address value in the Access-Request.

When the MAX sends an Access-Request packet to the RADIUS server, it includes the assigned IP address in the Framed-Address attribute. The MAX allocates this address from pool #1. (If you do not define pool #1, the call does not have an IP address during authentication.) The assigned IP address might not last the duration of the connection or might not be meaningful. Here are five possibilities:

– If Assign Adrs=No and the caller's RADIUS user profile does not supply an IP address for the caller, the MAX returns the IP address to pool #1, but the address continues to appear in RADIUS accounting entries.

– If Assign Adrs=No and the caller's RADIUS user profile does supply an IP address for the caller, the IP address from pool #1 returns to the pool, and the IP address from the user profile appears in RADIUS accounting entries.

- If Assign Adrs=Yes and Ascend-Assign-IP-Pool in the RADIUS user profile points to a pool that has no valid IP address, the IP address from pool #1 appears in RADIUS accounting entries, and returns to the pool only when the call disconnects.
- If Assign Adrs=Yes, Assign Only=Yes, and Ascend-Assign-IP-Pool points to a pool that has a valid IP address, the IP address from that pool appears in RADIUS accounting entries for the duration of the call, and returns to the pool when the call disconnects.
- If Assign Adrs=Yes, Assign Only=No, and Ascend-Assign-IP-Pool points to a pool that has a valid IP address, the IP address from that pool appears in RADIUS accounting entries, unless the caller specifies an address.

  If the caller specifies an IP address, it appears in RADIUS accounting entries and the IP address derived from the pool is returned.

6 Save your changes.

Classifying user sessions in RADIUS

The Class and Ascend-Number-Sessions attributes enable access providers to classify their user sessions, such as for the purpose of billing clients depending on the service option they choose.

If you include the Class attribute in the RADIUS user profile, the RADIUS server sends it to the MAX in the Access-Accept packet when the session begins. Class then appears in Accounting-Request packets the MAX sends to the RADIUS accounting server whenever a session starts and whenever a session stops (as long as the Auth parameter on the MAX is not set to RADIUS/LOGOUT). The accounting entries give the class on a per-user and per-session basis.

The Ascend-Number-Sessions attribute reports information on all user sessions—that is, on the number of current sessions of each class. The attribute has a compound value. The first part specifies a user-session class. The second part reports the number of active sessions in that class. In the case of multichannel calls, such as MP+ calls, each separate connection counts as a session.

On the MAX, you can set the Sess Timer parameter in the Ethernet>Mod Config>Accounting menu to send accounting requests at regular intervals. At the specified interval, the MAX reports the number of open sessions by sending an Ascend-Event-Request packet (code 33). This packet contains the NAS-Identifier attribute, followed by a list of Ascend-Number-Sessions attributes.

Only RADIUS daemons you customize to recognize packet code 33 respond these request packets from the MAX. Other accounting daemons ignore it. Therefore, the standard Livingston RADIUS daemon and the Ascend accounting daemon both ignore this attribute.

When modifying the daemon, make sure that it recognizes an Ascend-Event-Request packet in this format:

```
Code (8-bit)=33

Identifier (8-bit)

Length (16-bit)

Authenticator (48-bit for an accounting server, 64-bit for an
authentication server)

List of attributes
```

User session 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 the MAX sends back to the RADIUS accounting server has three Ascend-Number-Session attributes, one for each of these class/session pairs.

Understanding accounting records

The sections that follow describe the attributes that appear in different types of accounting records:

- non-accounting attributes in accounting records
- accounting attributes in Start records
- accounting attributes in Stop records

Note: Call Logging Start and Stop packets are described in “Call logging records” on page 8-22.

Non-accounting attributes in accounting records

An accounting record can contain attributes that are not accounting specific. Table 8-2 lists these attributes.

Of the attributes listed in Table 8-2, only the NAS-Identifier attribute can appear in a Failure-to-start record.

Table 8-2. Non-accounting attributes in accounting records

Attribute	**Description**
Ascend-Dial-Number (227)	Specifies the phone number of the device that originated the connection.
Ascend-Home-Agent-IP-Addr (183)—Stop records only	Indicates the IP address of the home agent used for this mobile client. This attribute is reported when the following are true: • you use it *or* a combination of attributes 129 and 130 in the user profile • the Accounting-Request packet is a Stop packet • the session was authenticated and encapsulated by means of Ascend Tunnel Management Protocol (ATMP) You should use Ascend-Primary-Home-Agent (129) and Ascend-Secondary-Home-Agent in the user profile. The RADIUS accounting Stop record includes Ascend-Home-Agent-IP-Addr (183) and not attributes 129 and 130.

Table 8-2. Non-accounting attributes in accounting records (continued)

Attribute	Description
Ascend-Home-Agent-UDP-Port (186)—Stop records only	Indicates the UDP port number to use when the foreign agent sends ATMP packets to the home agent.
Ascend-Home-Network-Name (185)	Indicates the name of the Connection profile through which the home agent sends all packets it receives from the mobile client during ATMP operation. This attribute is not present if the home agent is configured in router mode (see Chapter 7, “Setting Up Virtual Private Networks in RADIUS.” Appears in the Stop record when • the Accounting-Request packet is a Stop packet • the session was authenticated and encapsulated by means of Ascend Tunnel Management Protocol (ATMP)
Ascend-Modem-PortNo (120)	Specifies the modem used for the call (Stop records only).
Ascend-Modem-SlotNo (121)	Specifies the slot containing the modem used for the call (Stop records only).
Caller-Id (31)	Specifies the calling-party number, indicating the phone number of the user that has connected to the MAX.
Class (25)	Enables access providers to classify their user sessions, such as for the purpose of billing users depending on the service option they choose. The default value for the Class attribute is null.
Client-Port-DNIS (30)	Specifies the called number, indicating the phone number the user dialed to connect to the MAX.
Framed-Address (8)	Specifies the IP address of the user starting the session. The default value is 0.0.0.0.
Framed-IPX-Network (23)	Specifies the network number of the router at the remote end of the connection. The default value is null.

Table 8-2. Non-accounting attributes in accounting records (continued)

Attribute	**Description**
Framed-Protocol (7)	Specifies the kind of protocol the connection uses: PPP (1) SLIP (2) MPP (256) EURAW (257) EUUI (258) COMB (260) FR (261) ARA (262) FR-CIR (263) By default, the MAX does not restrict the type of protocol a user can access.
NAS-Identifier (4)	Indicates the IP address of the MAX. This attribute does not appear in an Accounting-Stop packet for a Failure-start-session event.
NAS-Port (5)	Indicates the interface and service the session is using with a 5-digit value in this format: **`<service> <line number> <channel>`** This attribute does not appear in an Accounting-Stop packet for a Failure-start-session event.
NAS-Port-Type (61)	Specifies the type of service in use for the session: • synchronous ISDN • asynchronous (MAX routes the call to a modem)
Tunneling-Protocol	Indicates whether or not a session used the ATMP tunneling protocol.
User-Name (1)	Specifies the name of the user starting the session.

Accounting attributes in Start records

Table 8-3 lists the accounting-specific attributes that can appear in a Start record (as taken from the Accounting Start packet).

Table 8-3. Accounting-specific attributes in Start records

Attribute	**Description**
Acct-Authentic (45)	Indicates the method the MAX used to authenticate an incoming call: RADIUS (1) specifies that RADIUS authenticated the incoming call. Local (2) specifies that the MAX used a local Connection profile, TACACS profile, or TACACS+ profile to authenticate the call, or that the MAX accepted the call without authentication.
Acct-Delay-Time (41)	Specifies the number of seconds the MAX has been trying to send the Accounting packet. In an Accounting Start packet, this value is 0 (zero).
Acct-Session-Id (44)	Consists of a unique numeric string identified with the bridging, routing, or terminal server session reported in the Accounting packet. The string is a random number containing up to seven digits. RADIUS correlates the Accounting Start packet and Accounting Stop packet using Acct-Session-Id. Its value can range from 1 to 2,137,383,647.

Table 8-3. Accounting-specific attributes in Start records (continued)

Attribute	Description
Acct-Status-Type (40)	Requests that have Acct-Status-Type=Start (1) are Accounting Start packets. The information in these packets appears in Start records. Requests that have Acct-Status-Type=Stop (2) are Accounting Stop packets. The information in these packets appears in Stop or Failure-to-start records. Requests that have Acct-Status-Type=Accounting-On (7) are sent when either of the following occurs • The MAXis booted up and the Acct=RADIUS in the Ethernet > Mod Config > Accounting menu. • You set the Acct parameter RADIUS and save the configuration while the MAX is running. Requests that have Acct-Status-Type=Accounting-Off (8) are sent when one of the following occurs: • You reset the MAX. • You set Acct to either None or TACACS+ and save the configuration while the MAX is running. • You change the setting of the Auth parameter in the Ethernet>Mod Config>Auth menufrom RADIUS to RADIUS/LOGOUT. When Auth=RADIUS/ LOGOUT, Acct is set to N/A, and RADIUS accounting is disabled.
Ascend-Session-Svr-Key (151)	Identifies the user session in which a client sends a disconnect or filter change request to the RADIUS server.
Ascend-User-Acct-Base (142)	Specifies whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16.
Ascend-User-Acct-Host (139)	Specifies the IP address of the RADIUS server to use for this connection.
Ascend-User-Acct-Key (141)	Specifies the RADIUS client password as it appears in the clients file.
Ascend-User-Acct-Port (140)	Specifies a UDP port number for the connection.
Ascend-User-Acct-Time (143)	Specifies the number of seconds the MAX waits for a response to a RADIUS accounting request.
Ascend-User-Acct-Type (138)	Specifies the RADIUS accounting server(s) to use for this connection.

Accounting attributes in Stop records

Table 8-4 lists the accounting attributes that can appear in a Stop record (as taken from the Accounting Stop packet).

Table 8-4. Accounting-specific attributes in Stop records

Attribute	Description	Conditions for inclusion
Acct-Authentic (45)	Indicates the method the MAX used to authenticate an incoming call: RADIUS (1) specifies that RADIUS authenticated the incoming call. Local (2) specifies that the MAX used a local Connection profile, TACACS profile, or TACACS+ profile to authenticate the call, or that the MAX accepted the call without authentication.	The Auth parameter is not set to RADIUS/LOGOUT. The session must be authenticated.
Acct-Delay-Time (41)	Specifies the number of seconds between the time an event occurred and the time the MAX sent the packet. If RADIUS does not acknowledge the packet, the MAX resends it and the value of Acct-Delay-Time changes to reflect the proper event time.	The Auth parameter is not set to RADIUS/LOGOUT.
Acct-Input-Octets (42)	Indicates the number of octets the MAX received during the session.	The Auth parameter is not set to RADIUS/LOGOUT. The session must be authenticated.
Acct-Input-packets (47)	Indicates the number of packets the MAX received during the session.	The Auth parameter is not set to RADIUS/LOGOUT. The session must be authenticated. A framed protocol must be in use.
Ascend-Modem-PortNo (120)	Specifies the modem used for the call (Stop records only).	Ascend-Modem-PortNo (120)
Ascend-Modem-SlotNo (121)	Specifies the slot containing the modem used for the call (Stop records only).	Ascend-Modem-SlotNo (121)
Acct-Output-Octets (43)	Indicates the number of octets the MAX sent during the session.	The Auth parameter is not set to RADIUS/LOGOUT. The session must be authenticated.
Acct-Output-packets (48)	Indicates the number of packets the MAX sent during the session.	The Auth parameter is not set to RADIUS/LOGOUT. The session must be authenticated. A framed protocol must be in use.

Table 8-4. Accounting-specific attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
Acct-Session-Id (44)	Consists of a unique numeric string identified with the bridging, routing, or terminal server session reported in the Accounting packet. The string is a random number containing up to seven digits. RADIUS correlates the Accounting Start packet and Accounting Stop packet using Acct-Session-Id. Its value can range from 1 to 2,137,383,647.	The Auth parameter is not set to RADIUS/LOGOUT.
Acct-Session-Time (46)	Specifies the number of seconds the session has been logged in.	The Auth parameter is not set to RADIUS/LOGOUT. The session must be authenticated.
Acct-Status-Type (40)	Requests that have Acct-Status-Type=Start are Accounting Start packets. The information in these packets appears in Start records. Requests that have Acct-Status-Type=Stop are Accounting Stop packets. The information in these packets appears in Stop or Failure-to-start records. Requests that have Acct-Status-Type=Accounting-On (7) are sent when either of the following occurs • The MAX is booted up and the Acct=RADIUS in the Ethernet > Mod Config > Accounting menu. • You set the Acct parameter RADIUS and save the configuration while the MAX is running. Requests that have Acct-Status-Type=Accounting-Off (8) are sent when one of the following occurs: • You reset the MAX. • You set Acct to either None or TACACS+ and save the configuration while the MAX is running. You change the setting of the Auth parameter in the Ethernet>Mod Config>Auth menufrom RADIUS to RADIUS/LOGOUT. When Auth=RADIUS/LOGOUT, Acct is set to N/A, and RADIUS accounting is disabled.	The Auth parameter is not set to RADIUS/LOGOUT.

Table 8-4. Accounting-specific attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
Ascend-Connect-Progress (196)	Indicates the state of the connection before it disconnects.	The Auth parameter is not set to RADIUS/LOGOUT.
Ascend-Data-Rate (197)	Indicates the data rate of the connection in bits per second.	The Auth parameter is not set to RADIUS/LOGOUT.
Ascend-Disconnect-Cause (195)	Specifies the reason a connection was taken offline.	The Auth parameter is not set to RADIUS/LOGOUT.
Ascend-Event-Type (150)	Indicates a coldstart notification, informing the accounting server that the MAX has started up.	For a coldstart notification, the MAX sends values for NAS-Identifier (4) and Ascend-Event-Type (150) in an Ascend-Event-Request packet (code 33). The RADIUS accounting server must send back an Ascend-Event-Response packet (code 34) with the correct identifier to the MAX.
Ascend-First-Dest (189)	Records the destination IP address of the first packet the MAX received on a connection after authentication.	The Auth parameter is not set to RADIUS/LOGOUT. The session must be authenticated.
Ascend-Multilink-ID (187)	Reports the ID number of the Multilink bundle when the session closes.	The Auth parameter is not set to RADIUS/LOGOUT. The session must be authenticated.
Ascend-Num-In-Multilink (188)	Records the number of sessions remaining in a Multilink bundle when the session closes.	The Auth parameter is not set to RADIUS/LOGOUT. The session must be authenticated.
Ascend-Number-Sessions (202)	Specifies the number of active user sessions of a given class (as specified by the Class attribute). In the case of multichannel calls, such as MP+ calls, each separate connection counts as a session.	The Ascend-Number-Sessions attribute appears in Ascend-Event-Request packets. Only RADIUS daemons you customize to recognize this packet type respond these request packets from the MAX. Other accounting daemons ignore it. Therefore, the standard Livingston RADIUS daemon and the Ascend accounting daemon ignore this attribute.
Ascend-Pre-Input-Octets (190)	Records the number of octets the MAX received before authentication.	The Auth parameter is not set to RADIUS/LOGOUT. The session must be authenticated.

Table 8-4. Accounting-specific attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
Ascend-Pre-Input-packets (192)	Records the number of packets the MAX received before authentication.	The Auth parameter is not set to RADIUS/LOGOUT. The session must be authenticated.
Ascend-Pre-Output-Octets (191)	Records the number of octets the MAX sent before authentication.	The Auth parameter is not set to RADIUS/LOGOUT. The session must be authenticated.
Ascend-Pre-Output-packets (193)	Records the number of packets the MAX sent before authentication.	The Auth parameter is not set to RADIUS/LOGOUT. The session must be authenticated.
Ascend-PreSession-Time (198)	Indicates the length of time in seconds from when a call connected to when it completed authentication.	The Auth parameter is not set to RADIUS/LOGOUT.
Ascend-User-Acct-Base (142)	Specifies whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16.	None.
Ascend-User-Acct-Host (139)	Specifies the IP address of the RADIUS server to use for this connection.	None.
Ascend-User-Acct-Key (141)	Specifies the RADIUS client password as it appears in the clients file.	None.
Ascend-User-Acct-Port (140)	Specifies a UDP port number for the connection.	None.
Ascend-User-Acct-Time (143)	Specifies the number of seconds the MAX waits for a response to a RADIUS accounting request.	None.
Ascend-User-Acct-Type (138)	Specifies the RADIUS accounting server(s) to use for this connection.	None.

Accounting attributes in Failure-to-start records

Failure-to-start records can contain only a subset of the information found in Stop records. These attributes can appear:

- Acct-Delay-Time (41)
- Acct-Session-Id (44)
- Acct-Status-Type (40)
- Ascend-Connect-Progress (196)
- Ascend-Data-Rate (197)
- Ascend-Disconnect-Cause (195)
- Ascend-PreSession-Time (198)

For a brief description of each of these attributes, see Table 8-4 on page 8-18.

Accounting attributes in Checkpoint records

Checkpoint records contain the same group of attributes as the RADIUS Stop record. However, the value for Acct-Status-Type is always the number 3 (checkpoint message).

Call logging records

This section describes:

- Where call logging records are stored
- What kinds of packets call logging uses
- Which attributes appears in each type of packet

Where are call logging records stored?

The call logging server writes each record to a log file. If you run an unmodified Ascend RADIUS daemon, the Ascend RADIUS Call logging file and the Livingston RADIUS Call logging file have the same name:

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

where *`host`* is the RADIUS client. Because the client of the RADIUS call logging server is your MAX, *`host`* is your MAX unit's symbolic host-name, or it's IP address in dotted decimal notation.

What kinds of packets does call logging use?

Call logging uses two kinds of packets: Call logging Start packets and Call logging Stop packets.

Call logging Start packets

Call logging Start packets signal a Start session event. When the MAX begins a terminal-server, bridging, or routing session, and the system authenticates the call or the user logs in, the MAX sends an Call logging Start packet to the call logging server. The packet describes the type of session in use and the name of the user opening the session.

The MAX does not send an Call logging Start packet if a call fails authentication or otherwise fails to log in. In some cases, a session begins with a user login and then authentication follows, such as when a terminal server user chooses PPP or SLIP after login. If User-Service=Login-User, or if User-Service is unspecified, the MAX sends an Call logging Start packet after login.

Information from an Call logging Start packet appears in a Start record in the log file.

Call- logging Stop packets

Call logging Stop packets signal a Stop session or Failure-to-start session event. At the end of a session, including cases in which a user fails authentication, the MAX sends an Call logging Stop packet. Information from an Call logging Stop packet appears in a Stop record or Failure-to-start record in the log file.

Non-call logging attributes in call logging records

- An call logging record can contain attributes that are not call logging specific. The following table lists them. Of the attributes listed in the table, only the NAS-Identifier attribute can appear in a Failure-to-start record.

Table 10. Non-call logging attributes in call logging records

Attribute	Description
Ascend-Dial-Number (227)	Specifies the phone number of the device that originated the connection.
Caller-Id (31)	Specifies the calling-party number, which is the phone number of the user that has connected to the MAX.
Class (25)	Enables access providers to classify their user sessions. The default value for the Class attribute is null.
Client-Port-DNIS (30)	Specifies the called-party number, which is the phone number the user dials to connect to the MAX.
Framed-Address (8)	Specifies the IP address of the user starting the session. The default value is 0.0.0.0.
Framed-IPX-Network (23)	Specifies the network number of the router at the remote end of the connection. The default value is null.
Framed-Protocol (7)	Specifies the kind of protocol the connection uses. By default, the MAX does not restrict the type of protocol a user can access.
NAS-Identifier (4)	Specifies the IP address of the MAX. This attribute does not appear in an Call Logging-Stop packet for a Failure-start-session event.
NAS-Port (5)	Specifies the network port on which the MAX received the call. This attribute does not appear in an Call Logging-Stop packet for a Failure-start-session event.
User-Name (1)	Specifies the name of the user starting the session.

Call logging attributes in Start records

The following table lists the call logging-specific attributes that can appear in a Start record.

Call Logging-specific attributes in Start records

Attribute	Description
Acct-Authentic (45)	Specifies the method the MAX used to authenticate an incoming call: RADIUS (1) specifies that RADIUS authenticated the incoming call. Local (2) specifies that the MAX used a local Connection profile, TACACS profile, or TACACS+ profile, or that the MAX accepted the call without authentication.
Acct-Delay-Time (41)	Specifies the number of seconds the MAX has been trying to send the Call Logging packet. In an Call Logging Start packet, this value is 0 (zero).
Acct-Session-Id (44)	Consists of a unique numeric string identified with the bridging, routing, or terminal-server session reported in the Call Logging packet. The string is a random number of up to seven digits. RADIUS correlates the Call Logging Start packet and Call Logging Stop packet with Acct-Session-Id. Its value can range from 1 to 2,137,383,647.

Call Logging-specific attributes in Start records (continued)

Attribute	Description
Acct-Status-Type (40)	Requests that have Acct-Status-Type=Start are Call Logging Start packets. The information in these packets appears in Start records. Requests that have Acct-Status-Type=Stop are Call Logging Stop packets. The information in these packets appears in Stop or Failure-to-start records. Requests that have Acct-Status-Type=Accounting-On (7) are sent when either of the following occurs • The MAX is booted up and the Acct=RADIUS in the Ethernet > Mod Config > Accounting menu. • You set the Acct parameter RADIUS and save the configuration while the MAX is running. Requests that have Acct-Status-Type=Accounting-Off (8) are sent when one of the following occurs: • You reset the MAX. • You set Acct to either None or TACACS+ and save the configuration while the MAX is running. You change the setting of the Auth parameter in the Ethernet>Mod Config>Auth menufrom RADIUS to RADIUS/LOGOUT. When Auth=RADIUS/ LOGOUT, Acct is set to N/A, and RADIUS accounting is disabled.
Ascend-Session-Svr-Key (151)	Identifies the user session in which a client sends a disconnect or filter-change request to the RADIUS server.
Ascend-User-Acct-Base (142)	Specifies whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16.
Ascend-User-Acct-Host (139)	Specifies the IP address of the RADIUS server to use for the connection.
Ascend-User-Acct-Key (141)	Specifies the RADIUS client password as it appears in the clients file.
Ascend-User-Acct-Port (140)	Specifies a UDP port number for the connection.
Ascend-User-Acct-Time (143)	Specifies the number of seconds the MAX waits for a response to a call logging request.
Ascend-User-Acct-Type (138)	Specifies the call logging server(s) to use for the connection.

Call logging attributes in Stop records

The following table lists the call logging attributes that can appear in a Stop record.

Table 11. Call Logging-specific attributes in Stop records

Attribute	Description	Conditions for inclusion
Acct-Authentic (45)	Specifies the method the MAX used to authenticate an incoming call: RADIUS (1) specifies that RADIUS authenticated the incoming call. Local (2) specifies that the MAX used a local Connection profile, TACACS profile, or TACACS+ profile, or that the MAX accepted the call without authentication.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated.
Acct-Delay-Time (41)	Specifies the number of seconds between the time an event occurred and the time the MAX sent the packet. If RADIUS does not acknowledge the packet, the MAX resends it. The value of Acct-Delay-Time changes to reflect the proper event time.	Auth-Type parameter not set to RADIUS-Logout.
Acct-Input-Octets (42)	Specifies the number of octets the MAX received during the session.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated.
Acct-Input-packets (47)	Specifies the number of packets the MAX received during the session.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated. A framed protocol must be in use.
Acct-Output-Octets (43)	Specifies the number of octets the MAX sent during the session.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated.
Acct-Output-packets (48)	Specifies the number of packets the MAX sent during the session.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated. A framed protocol must be in use.

Table 11. Call Logging-specific attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
Acct-Session-Id (44)	Consists of a unique numeric string identified with the bridging, routing, or terminal-server session reported in the Call Logging packet. The string is a random number of up to seven digits. RADIUS correlates the Call Logging Start packet and Call Logging Stop packet with Acct-Session-Id. Its value can range from 1 to 2,137,383,647.	Auth-Type parameter not set to RADIUS-Logout.
Acct-Session-Time (46)	Specifies the number of seconds the session has been logged in.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated.
Acct-Status-Type (40)	Requests that have Acct-Status-Type=Start are Call Logging Start packets. The information in these packets appears in Start records. Requests that have Acct-Status-Type=Stop are Call Logging Stop packets. The information in these packets appears in Stop or Failure-to-start records. Requests that have Acct-Status-Type=Accounting-On (7) are sent when either of the following occurs • The MAXis booted up and the Acct=RADIUS in the Ethernet > Mod Config > Accounting menu. • You set the Acct parameter RADIUS and save the configuration while the MAX is running. Requests that have Acct-Status-Type=Accounting-Off (8) are sent when one of the following occurs: • You reset the MAX. • You set Acct to either None or TACACS+ and save the configuration while the MAX is running. You change the setting of the Auth parameter in the Ethernet>Mod Config>Auth menufrom RADIUS to RADIUS/LOGOUT. When Auth=RADIUS/LOGOUT, Acct is set to N/A, and RADIUS accounting is disabled.	Auth-Type parameter not set to RADIUS-Logout.

Table 11. Call Logging-specific attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
Ascend-Connect-Progress (196)	Specifies the state of the connection before it disconnects.	Auth-Type parameter not set to RADIUS-Logout.
Ascend-Data-Rate (197)	Specifies the data rate of the connection in bits per second.	Auth-Type parameter not set to RADIUS-Logout.
Ascend-Disconnect-Cause (195)	Specifies the reason a connection was taken offline.	Auth-Type parameter not set to RADIUS-Logout.
Ascend-Event-Type (150)	Specifies a cold-start notification, informing the call logging server that the MAX has started up.	For a cold-start notification, the MAX sends values for NAS-Identifier and Ascend-Event-Type in an Ascend-Event-Request packet (code 33). The call logging server must send back an Ascend-Event-Response packet (code 34), with the correct identifier, to the MAX.
Ascend-First-Dest (189)	Records the destination IP address of the first packet the MAX received on a connection after authentication.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated.
Ascend-Multilink-ID (187)	Reports the ID number of the Multilink bundle when the session closes.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated.
Ascend-Num-In-Multilink (188)	Records the number of sessions remaining in a Multilink bundle when the session closes.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated.
Ascend-Number-Sessions (202)	Specifies the number of active user sessions of a given class (as specified by the Class attribute). In the case of multichannel calls, such as MP+ calls, each separate connection counts as a session.	The MAX sends the Ascend-Number-Sessions attribute in Ascend-Event-Request packets. Only RADIUS daemons you customize to recognize packet code 33 respond to these request packets.
Ascend-Pre-Input-Octets (190)	Records the number of octets the MAX received before authentication.	Auth-Type parameter is not set to RADIUS-Logout. The session must be authenticated.
Ascend-Pre-Input-packets (192)	Records the number of packets the MAX received before authentication.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated.
Ascend-Pre-Output-Octets (191)	Records the number of octets the MAX sent before authentication.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated.

Table 11. Call Logging-specific attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
Ascend-Pre-Output-packets (193)	Records the number of packets the MAX sent before authentication.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated.
Ascend-PreSession-Time (198)	Specifies the length of time, in seconds, from when a call connected to when it completed authentication.	Auth-Type parameter not set to RADIUS-Logout.
Ascend-User-Acct-Base (142)	Specifies whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16.	None.
Ascend-User-Acct-Host (139)	Specifies the IP address of the RADIUS server to use for the connection.	None.
Ascend-User-Acct-Key (141)	Specifies the RADIUS client password as it appears in the clients file.	None.
Ascend-User-Acct-Port (140)	Specifies a UDP port number for the connection.	None.
Ascend-User-Acct-Time (143)	Specifies the number of seconds the MAX waits for a response to a call logging request.	None.
Ascend-User-Acct-Type (138)	Specifies the call logging server(s) to use for the connection.	None.

Call logging attributes in Failure-to-start records

Failure-to-start records can contain only a subset of the information found in Stop records. The following attributes can appear:

- Acct-Delay-Time (41)
- Acct-Session-Id (44)
- Acct-Status-Type (40)
- Ascend-Connect-Progress (196)
- Ascend-Data-Rate (197)
- Ascend-Disconnect-Cause (195)
- Ascend-PreSession-Time (198)

Sample accounting records

This section provides sample Start and Stop records for these scenarios:

- A Pipeline 25 dialing into a MAX
- A modem calling into a MAX

A Pipeline 25 dialing into a MAX 4000

Suppose that a Pipeline 25 dials into a MAX 4000 using PPP. The Start record might look like this one:

```
Tue Feb 25 12:00:41 1997 /* Session startup time */
   User-Name="ht-net" /* The name of the Pipeline 25 */
   NAS-Identifier=206.65.212.46 /* The IP address of the MAX */
   NAS-Port=10114 /* Digital call on line 1, channel 14 */
   Acct-Status-Type=Start /* Start record. */
   Acct-Delay-Time=0 /* Always zero for a Start record */
   Acct-Session-Id="1234567" /* Session identification number */
   Acct-Authentic=RADIUS /* RADIUS authentication in use */
   Client-Port-DNIS="3142" /* Called number */
   Framed-Protocol=PPP /* PPP call */
   Framed-Address=11.0.0.1 /* IP address of the Pipeline 25 */
```

The Stop record might look like this one:

```
Tue Feb 25 12:02:48 1997 /* Session hangup time */
   User-Name="ht-net" /* The name of the Pipeline 25 */
   NAS-Identifier=206.65.212.46 /* The IP address of the MAX */
   NAS-Port=10114 /* Digital call on line 1, channel 14 */
   Acct-Status-Type=Stop /* Stop record */
   Acct-Delay-Time=18 /* MAX tried to send packet for 18 seconds */
   Acct-Session-Id="1234567" /* Session identification number */
   Acct-Authentic=RADIUS /* RADIUS authentication used */
   Acct-Session-Time=128 /* Number of seconds in session */
   Acct-Input-Octets=2421 /* Bytes received from the Pipeline */
   Acct-Output-Octets=1517 /* Bytes sent to the Pipeline */
   Acct-Input-packets=79 /* Packets received from the Pipeline */
   Acct-Output-packets=47 /* Packets sent to the Pipeline */
   Ascend-Disconnect-Cause=100 /* Session timeout */
   Ascend-Connect-Progress=60 /* LAN session up */
   Ascend-Data-Rate=64000 /* Data rate in bits per second */
   Ascend-PreSession-Time=0 /*Secs from connection to authentication*/
   Ascend-Pre-Input-Octets=174 /* Input octets pre-authentication */
   Ascend-Pre-Output-Octets=204 /* Output octets pre-authentication */
   Ascend-Pre-Input-packets=7 /* Input packets pre-authentication */
   Ascend-Pre-Output-packets=8 /* Output packets pre-authentication */
   Ascend-First-Dest=10.81.44.111 /* Dest IP address of 1st packet */
   Ascend-Multilink-ID=64 /* ID number of Multilink bundle */.
   Ascend-Num-In-Multilink=0 /* # of sessions in Multilink bundle */
   Client-Port-DNIS="3142" /* Called number */
   Framed-Protocol=PPP /* PPP call */
   Framed-Address=11.0.0.1 /* IP address of the Pipeline 25 */
```

A modem calling into a MAX 4000

If a modem dials into the MAX to reach its terminal server, the call can only be an unframed call. It cannot be a PPP, MP, or MP+ call. Therefore, the attributes Framed-Protocol and Framed-Address do not appear in the sample records, and Login-Service=Unframed-User.

```
Tue Feb 25 12:00:00 1997 /* Session startup time */
   User-Name="Berkeley" /* The name of the modem caller */
   NAS-Identifier=200.65.212.46 /* The IP address of the MAX */
   NAS-Port=10113 /* Digital call on line 1, channel 13 */
   Acct-Status-Type=Start /* Start record. */
   Acct-Delay-Time=0 /* Always zero for a Start record */
   Acct-Session-Id="3456789" /* Session identification number */
   Acct-Authentic=RADIUS /* RADIUS authentication in use */
   Client-Port-DNIS="3143" /* Called number */
   Login-Service=Unframed-User /* Modem call */
```

The Stop record might look like this one:

```
Tue Feb 25 12:03:00 1997 /* Session hangup time */
   User-Name="Berkeley" /* The name of the modem caller */
   NAS-Identifier=200.65.212.46 /* The IP address of the MAX */
   NAS-Port=10113 /* Digital call on line 1, channel 13 */
   Acct-Status-Type=Stop /* Stop record */
   Acct-Delay-Time=18 /* MAX tried to send packet for 18 seconds */
   Acct-Session-Id="3456789" /* Session identification number */
   Acct-Authentic=RADIUS /* RADIUS authentication used */
   Acct-Session-Time=128 /* Number of seconds in session */
   Acct-Input-Octets=2421 /* Bytes received from the Pipeline */
   Acct-Output-Octets=1517 /* Bytes sent to the Pipeline */
   Acct-Input-packets=79 /* Packets received from the Pipeline */
   Acct-Output-packets=47 /* Packets sent to the Pipeline */
   Ascend-Disconnect-Cause=100 /* Session timeout */
   Ascend-Connect-Progress=60 /* LAN session up */
   Ascend-Data-Rate=64000 /* Data rate in bits per second */
   Ascend-PreSession-Time=0 /*Secs from connection to authentication*/
   Ascend-Pre-Input-Octets=174 /* Input octets pre-authentication */
   Ascend-Pre-Output-Octets=204 /* Output octets pre-authentication */
   Ascend-Pre-Input-packets=7 /* Input packets pre-authentication */
   Ascend-Pre-Output-packets=8 /* Output packets pre-authentication */
   Ascend-First-Dest=10.81.44.111 /* Dest IP address of 1st packet */
   Ascend-Multilink-ID=64 /* ID number of Multilink bundle *.
   Ascend-Num-In-Multilink=0 /* # of sessions in Multilink bundle */
   Client-Port-DNIS="3143" /* Called number */
   Login-Service=Unframed-User /* Modem call */
```

A Pipeline 25 dialing into a MAX

When a Pipeline 25 dials into a MAX with PPP, the Start record might look like the following:

```
Tue Feb 18 12:00:41 1997 /* Session startup time */
   User-Name="ht-net" /* The name of the Pipeline 25 */
   NAS-Identifier=206.65.212.46 /* The IP address of the MAX */
   NAS-Port=1057 /* Call on channel 2, line 2, slot 2, shelf 1 */
   Acct-Status-Type=Start /* Start record. */
   Acct-Delay-Time=0 /* Always zero for a Start record */
   Acct-Session-Id="1234567" /* Session identification number */
   Acct-Authentic=RADIUS /* RADIUS authentication in use */
   Client-Port-DNIS="3142" /* Called-party number */
   Framed-Protocol=PPP /* PPP call */
   Framed-Address=11.0.0.1 /* IP address of the Pipeline 25 */
```

The Stop record might look like the following:

```
Tue Feb 18 12:02:48 1997 /* Session hangup time */
   User-Name="ht-net" /* The name of the Pipeline 25 */
   NAS-Identifier=206.65.212.46 /* The IP address of the MAX */
   NAS-Port=1057 /* Call on channel 2, line 2, slot 2, shelf 1 */
   Acct-Status-Type=Stop /* Stop record */
   Acct-Delay-Time=18 /* MAX tried to send packet for 18 seconds */
   Acct-Session-Id="1234567" /* Session identification number */
   Acct-Authentic=RADIUS /* RADIUS authentication used */
   Acct-Session-Time=128 /* Number of seconds in session */
   Acct-Input-Octets=2421 /* Bytes received from the Pipeline */
   Acct-Output-Octets=1517 /* Bytes sent to the Pipeline */
   Acct-Input-packets=79 /* Packets received from the Pipeline */
   Acct-Output-packets=47 /* Packets sent to the Pipeline */
   Ascend-Disconnect-Cause=100 /* Session timeout */
   Ascend-Connect-Progress=60 /* LAN session up */
   Ascend-Data-Rate=64000 /* Data rate in bits per second */
   Ascend-PreSession-Time=0 /*Secs from connection to authentication*/
   Ascend-Pre-Input-Octets=174 /* Input octets pre-authentication */
   Ascend-Pre-Output-Octets=204 /* Output octets pre-authentication */
   Ascend-Pre-Input-packets=7 /* Input packets pre-authentication */
   Ascend-Pre-Output-packets=8 /* Output packets pre-authentication */
   Ascend-First-Dest=10.81.44.111 /* Dest IP address of 1st packet */
   Ascend-Multilink-ID=64 /* ID number of Multilink bundle */.
   Ascend-Num-In-Multilink=0 /* # of sessions in Multilink bundle */
   Client-Port-DNIS="3142" /* Called-party number */
   Framed-Protocol=PPP /* PPP call */
   Framed-Address=11.0.0.1 /* IP address of the Pipeline 25 */
```

A modem calling into a MAX

If a modem dials into the MAX to reach its terminal server, the call can only be an unframed call. It cannot be a PPP, MP, or MP+ call. Therefore, the attributes Framed-Protocol and Framed-Address do not appear in the sample records, and Login-Service=Unframed-User.

A Start record might look like the following:

```
Tue Feb 18 12:00:00 1997 /* Session startup time */
   User-Name="Berkeley" /* The name of the modem caller */
   NAS-Identifier=200.65.212.46 /* The IP address of the MAX */
   NAS-Port=1057 /* Call on channel 2, line 2, slot 2, shelf 1 */
   Acct-Status-Type=Start /* Start record. */
   Acct-Delay-Time=0 /* Always zero for a Start record */
   Acct-Session-Id="3456789" /* Session identification number */
   Acct-Authentic=RADIUS /* RADIUS authentication in use */
   Client-Port-DNIS="3143" /* Called-party number */
   Login-Service=Unframed-User /* Modem call */
```

The Stop record might look like the following:

```
Tue Feb 18 12:03:00 1997 /* Session hangup time */
   User-Name="Berkeley" /* The name of the modem caller */
   NAS-Identifier=200.65.212.46 /* The IP address of the MAX */
   NAS-Port=1057 /* Call on channel 2, line 2, slot 2, shelf 1 */
   Acct-Status-Type=Stop /* Stop record */
   Acct-Delay-Time=18 /* MAX tried to send packet for 18 seconds */
   Acct-Session-Id="3456789" /* Session identification number */
   Acct-Authentic=RADIUS /* RADIUS authentication used */
   Acct-Session-Time=128 /* Number of seconds in session */
   Acct-Input-Octets=2421 /* Bytes received from the Pipeline */
   Acct-Output-Octets=1517 /* Bytes sent to the Pipeline */
   Acct-Input-packets=79 /* Packets received from the Pipeline */
   Acct-Output-packets=47 /* Packets sent to the Pipeline */
```

```
Ascend-Disconnect-Cause=100 /* Session timeout */
Ascend-Connect-Progress=60 /* LAN session up */
Ascend-Data-Rate=64000 /* Data rate in bits per second */
Ascend-PreSession-Time=0 /*Secs from connection to authentication*/
Ascend-Pre-Input-Octets=174 /* Input octets pre-authentication */
Ascend-Pre-Output-Octets=204 /* Output octets pre-authentication */
Ascend-Pre-Input-packets=7 /* Input packets pre-authentication */
Ascend-Pre-Output-packets=8 /* Output packets pre-authentication */
Ascend-First-Dest=10.81.44.111 /* Dest IP address of 1st packet */
Ascend-Multilink-ID=64 /* ID number of Multilink bundle *.
Ascend-Num-In-Multilink=0 /* # of sessions in Multilink bundle */
Client-Port-DNIS="3143" /* Called-party number */
Login-Service=Unframed-User /* Modem call */
```

Reference to RADIUS Attributes

9

This chapter discusses RADIUS attributes found in user profiles. 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.

Acct-Authentic (45)

Description: The Acct-Authentic attribute specifies the method the MAX used to authenticate a call, or indicates whether the MAX accepted the call without authentication.

The MAX sends Acct-Authentic in an Accounting-Request packet under these conditions:

- At the start of a session (when Acct-Status-Type=Start)
- At the end of an authenticated session (Acct-Status-Type=Stop) when the Auth parameter is not set to RADIUS/LOGOUT

Usage: Acct-Authentic does not appear in a user profile It can have either of the following values:

- RADIUS (1)

  This value indicates that RADIUS authenticated the incoming call. RADIUS is the default.
- Local (2)

  This value indicates that the MAX authenticated the call using a local Connection profile, TACACS profile, or TACACS+ profile, or that the MAX accepted the call without authentication.

Acct-Delay-Time (41)

Description: The Acct-Delay-Time attribute specifies how many seconds the MAX has been trying to send this Accounting packet.

The MAX sends Acct-Delay-Time in an Accounting-Request packet under these conditions:

- At the start of a session (when Acct-Status-Type=Start)
- At the end of a session or when a session fails to authenticate (Acct-Status-Type=Stop) and the Auth parameter is not set to RADIUS/LOGOUT

Usage: Acct-Delay-Time does not appear in a user profile. Its default value is 0 (zero).

Acct-Input-Octets (42)

Description: The Acct-Input-Octets attribute specifies how many octets the MAX has received during the session.

Usage: The MAX sends Acct-Input-Octets in an Accounting-Request packet at the end of a session (Acct-Status-Type=Stop) when both of these conditions are true:

- The session has been authenticated.
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Acct-Input-Octets does not appear in a user profile. Its default value is 0 (zero).

Acct-Input-packets (47)

Description: The Acct-Input-packets attribute specifies how many packets the MAX has received during the session. The MAX sends Acct-Input-packets in an Accounting-Request packet at the end of a session (Acct-Status-Type=Stop) when all of these conditions are true:

- The session has been authenticated.
- The Auth parameter is not set to RADIUS/LOGOUT.
- A framed protocol is in use.

Usage: Acct-Input-packets does not appear in a user profile. Its default value is (zero).

Acct-Output-Octets (43)

Description: The Acct-Output-Octets attribute specifies how many octets the MAX has sent during the session.

The MAX sends Acct-Output-Octets in an Accounting-Request packet at the end of a session (Acct-Status-Type=Stop) when both of these conditions are true:

- The session has been authenticated.
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Acct-Output-Octets does not appear in a user profile. Its default value is (zero).

Acct-Output-packets (48)

Description: The Acct-Output-packets attribute specifies how many packets the MAX has sent during the session. The MAX sends Acct-Output-packets in an Accounting-Request packet at the end of a session (Acct-Status-Type=Stop) when all of these conditions are true:

- The Auth parameter is not set to RADIUS/LOGOUT.

- The session is authenticated.
- A framed protocol is in use.

Usage: Acct-Output-packets does not appear in a user profile. Its default value is (zero).

Acct-Session-Id (44)

Description: The Acct-Session-Id attribute specifies a unique numeric string for the bridging, routing, or terminal server session specified in the Accounting-Request packet. The string is a random number containing up to seven digits. RADIUS correlates the Accounting Start packet and Accounting Stop packet using Acct-Session-Id.

The MAX sends Acct-Session-Id under these conditions:

- At the start of a session (when Acct-Status-Type=Start)
- At the end of a session or when a session failed to authenticate (Acct-Status-Type=Stop) and the Auth parameter is not set to RADIUS/LOGOUT

Usage: Acct-Session-Id does not appear in a user profile. Its value can range from 1 to 2,137,383,647. For every session, RADIUS generates a unique session ID, thereby preventing the same session ID from applying to more than one session.

Dependencies: Keep this additional information in mind:

- When an SNMP accounting session and a RADIUS accounting session have the same ID, they are identical.

  However, SNMP records all calls, while RADIUS records only those calls that result in a successful login or authentication.
- Using the Acct-ID Base parameter in the Ethernet>Mod Config>Accounting menu, you can specify whether the numeric base of the Acct-Session-Id attribute is 10 or 16.

  This parameter controls how the MAX presents Acct-Session-Id attribute to the accounting server. For more information, see the MAX *Reference Guide*.

Acct-Session-Time (46)

Description: The Acct-Session-Time attribute specifies how many seconds the session has been online.

The MAX sends Acct-Session-Time in an Accounting-Request packet at the end of a session (Acct-Status-Type=Stop) when both of these conditions are true:

- The session has been authenticated.
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Acct-Session-Time does not appear in a user profile. Its default value is 0 (zero).

Acct-Status-Type (40)

Description: The Acct-Status-Type attribute specifies whether the Accounting packet the MAX sends to the RADIUS server is the beginning (Start) or end (Stop) of a bridging, routing, or terminal server session, or to indicate whether and when RADIUS accounting is enabled or disabled. The Accounting-Request packet contains these attributes and values:

- NAS-Identifier (4) with the IP address of the MAX
- Acct-Status-Type (40) with the value7
- Acct-Delay-Time(41) with the number of seconds the MAX has been trying to send the packet without receiving an acknowledgement from the accounting server.

The attribute has four possible values:

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

The MAX sends Acct-Status-Type under these conditions:

- At the start of a session (when Acct-Status-Type=Start)
- At the end of a session or when a session fails to authenticate (when Acct-Status-Type=Stop), and only if the Auth parameter is not set to RADIUS/LOGOUT
- You boot the MAX and Acct=RADIUS in the Ethernet > Mod Config > Accounting menu (Acct-Status-Type=Accounting-On.
- You set the Acct parameter RADIUS and save the configuration while the MAX is running (Acct-Status-Type=Accounting-On).

  When Acct-Status-Type=Accounting-On, the MAX retransmits the request until it receives an Accounting-Response packet from the RADIUS accounting server, or until the MAX reaches a limit of ten retries for each accounting server it attempts to reach.
- You reset the MAX.
- You set Acct to either None or TACACS+ and save the configuration while the MAX is running (Accounting-Off).
- You change the setting of the Auth parameter in the Ethernet>Mod Config>Auth menu from RADIUS to RADIUS/LOGOUT (Accounting-Off).
- When Auth=RADIUS/LOGOUT, Acct is set to N/A, and RADIUS accounting is disabled (Accounting-Off).

  When Acct-Status-Type=Accounting-Off, the MAX retransmits the request until it receives an Accounting-Response packet from RADIUS, or until the MAX reaches a limit of ten retries for each accounting server it attempts to reach. If the MAX is being reset, it sends only one Accounting-Request packet, and does not retransmit the request. The MAX does not send an Accounting-Request packet in response to a power failure.

Usage: Acct-Status-Type does not appear in a user profile.

Ascend-Add-Seconds (240)

Description: The Ascend-Add-Seconds attribute specifies the number of seconds that average line utilization (ALU) for transmitted data must exceed the threshold indicated by the Ascend-Target-Util attribute before the MAX begins adding bandwidth to a session. The MAX determines the ALU for a session by using the algorithm specified by the Ascend-History-Weigh-Type attribute.

When utilization exceeds the threshold for a period of time greater than the value of the Ascend-Add-Seconds attribute, the MAX attempts to add the number of channels specified by the Ascend-Inc-Channel-Count attribute. Using the Ascend-Add-Seconds attribute prevents the system from continually adding bandwidth, and can slow down the process of allocating bandwidth.

Usage: Specify a number between 1 and 300. The default value is 5.

Dependencies: Keep this additional information in mind:

- Additional channels must be available, and the number of channels the MAX adds cannot exceed the amount the Ascend-Maximum-Channels attribute specifies.
- Ascend-Add-Seconds and Ascend-Remove-Seconds have little or no effect on a system with a high Ascend-Seconds-Of-History value.

  If the value of Ascend-Seconds-Of-History is low, the Ascend-Add-Seconds and Ascend-Remove-Seconds attributes provide an alternative way to ensure that spikes must persist for a certain period of time before the system responds.

See Also: “Ascend-Base-Channel-Count (172)” on page 9-10
“Ascend-DBA-Monitor (171)” on page 9-33
“Ascend-Dec-Channel-Count (237)” on page 9-34
“Ascend-History-Weigh-Type (239)” on page 9-50
“Ascend-Inc-Channel-Count (236)” on page 9-55
“Ascend-Maximum-Channels (235)” on page 9-61
“Ascend-Minimum-Channels (173)” on page 9-65
“Ascend-Remove-Seconds (241)” on page 9-78
“Ascend-Seconds-Of-History (238)” on page 9-81
“Ascend-Target-Util (234)” on page 9-84

Ascend-Appletalk-Peer-Mode (117)

Description: Specifies whether the connection is for a single dial-in station or for a router.

Usage: Specify one of the following values:

- Appletalk-Peer-Router (0) specifies that the caller is an AppleTalk router, such as an Ascend Pipeline unit.
- Appletalk-Peer-Dialin specifies that the caller is a dial-in AppleTalk client, such as a single Macintosh dialing in over a modem.

Dependencies: Ascend-Route-Appletalk must be set to Ascend-Route-Appletalk-Yes.

Example: The following example shows a RADIUS user profile for a routed connection:

```
pipe50  Password="pipe50"
        User-Service = Framed-User,
        Framed-Protocol = PPP,
        Ascend-Appletalk-Peer-Mode = Appletalk-Peer-Router,
        Ascend-Route-Appletalk = Route-Appletalk-Yes,
        Ascend-Idle-Limit = 0
```

The following is an example of a RADIUS user profile for a dial-in connection:

```
mac1    Password = "mac1"
        User-Service = Framed-User,
        Framed-Protocol = PPP,
        Ascend-Appletalk-Peer-Mode = Appletalk-Peer-Dialin,
        Ascend-Route-Appletalk = Route-Appletalk-Yes,
        Ascend-Idle-Limit = 0
```

Dependencies: Ascend-Route-Appletalk must be set to Yes.

See Also: Ascend-Appletalk-Peer-Mode (117), Ascend-Appletalk-Route (116)

Ascend-Appletalk-Route (116)

Description: Defines a static AppleTalk route. in a RADIUS pseudo-user profile.

Usage: Create a pseudo-user profile with the first line in the following format:

```
appleroute-num Password="ascend’, user-service=Dialout-Framed-User
```

where `num` is a number in a series starting at 1. Then enter one or more static AppleTalk route specifications in the following format:

```
Ascend-Appletalk-Route="net_start net_end zone_name profile_name"
```

Argument	Description
net_start	The lower limit of the network range for this network. A network range is a range of network numbers set into the port descriptor of the router port and then transmitted through RTMP to the other nodes of the network. Each of the numbers within a network range can represent up to 253 devices. The default is blank.
net_end	The upper limit of the network range for this network. This range defines the networks available for packets routed using the static route. Specify a number between 1 and 65199. If there are other AppleTalk routers on the network, you must configure the network ranges to be identical to the ranges specified on the other routers.
zone_name	The name of the AppleTalk zone associated with this network. A zone is a multicast address containing a subset of the AppleTalk nodes on an internet. Each node belongs to only one zone, but a particular extended network can contain nodes belonging to any number of zones. Zones provide departmental or other groupings of network entities that a user can easily understand. In the Ascend AppleTalk router, zone names are case-insensitive. However, because some routers regard zone names as case-sensitive, the spelling of zone names should be consistent when you configure multiple connections or routers. You can use up to 33 alphanumeric characters. The default is blank.
profile_name	The outgoing RADIUS user profile that the route uses. The default is blank.

Each static route must appear in a user profile. User profile entries for Appletalk static routes are identified by the special name `appleroute-#` and have the following format:

```
appleroute-# Password = “ascend” User-Service = Dialout-Framed-User
   Address 1
   Address 2
   ...
   Address n
```

`Address n` is the actual route associated with this entry.

An example of a static route with the associated connection profiles is:

```
appleroute-1  Password = “ascend” User-Service = Dialout-
Framed-User Ascend-Appletalk-Route = “20 25 testzone1 pipe50”


pipe50  Password = “ascend” User-Service = Dialout-Framed-User,
        User-Service = Framed-User,
        Framed-Protocol = MPP,
        Ascend-Appletalk-Peer-Mode = Appletalk-Peer-Router,
        Ascend-Route-Appletalk = Route-Appletalk-Yes,
        Ascend-Dialout-Allowed = Dialout-Allowed,
        Ascend-Dial-Number = “83272”,
        Ascend-Send-Auth = Send-Auth-PAP,
        Ascend-Send-Passwd = “MAX”
```

Dependencies: Ascend-Route-Appletalk must be set to Yes.

See Also: Ascend-Appletalk-Peer-Mode (117)

Ascend-Ara-PW (181)

Description: The Ascend-Ara-PW attribute specifies the password of the incoming caller over an AppleTalk Remote Access (ARA) connection. The ARA software in the MAX uses DES to encrypt and decrypt the password.

Usage: Specify an alphanumeric text string containing up to 20 characters. The default value is null. The password you enter for this attribute must be identical to the password you enter in the first line of the user profile. The MAX requires both entries.

Example: This example sets up a TCP connection through ARA with a dynamic IP address assignment:

```
Emma Password="pwd"

     Framed-Protocol=ARA,

     Ascend-Ara-PW="pwd",

     Ascend-Route-IP=Route-IP-Yes,

     Ascend-Assign-IP-Pool=1
```

See Also: “Password (2)” on page 9-104

Ascend-Assign-IP-Client (144)

Description: In the Radipa-Hosts pseudo-user profile, the Ascend-Assign-IP-Client attribute specifies the IP address of an Ascend unit that can use global IP address pools.

Usage: Specify an IP address in dotted-decimal notation. The default value is 0.0.0.0. You can specify multiple instances of this attribute. At present, the MAX does not use the list of radipad client units.

Dependencies: If no Ascend-Assign-IP-Client attribute is present, the list of client units defaults to those present in the RADIUS clients file.

See Also: “Ascend-Assign-IP-Global-Pool (146)” on page 9-8
“Ascend-Assign-IP-Server (145)” on page 9-9

Ascend-Assign-IP-Global-Pool (146)

Description: In a RADIUS user profile requiring dynamic addressing for dial-in users, the Ascend-Assign-IP-Global-Pool attribute specifies the global address pool from which RADIUS should assign each user an address.

Usage: Specify the name of the pseudo-user profile containing global IP pool definitions. The Ascend unit tries to allocate an address from the pools in order, and chooses an address from the pool with the first available IP address.

Dependencies: Do not set the Framed-Address attribute in the user profile. If you do, the MAX will require the caller to use the static IP address the attribute specifies.

See Also: “Ascend-Assign-IP-Client (144)” on page 9-8
“Ascend-Assign-IP-Server (145)” on page 9-9
“Framed-Address (8)” on page 9-93

Ascend-Assign-IP-Pool (218)

Description: In a user profile, the Ascend-Assign-IP-Pool attribute specifies the MAX-specific address pool from which RADIUS assigns the user an IP address.

A dynamic address comes from the pool of addresses set by the Pool #*n* Start and Pool #*n* Count parameters, by the Ascend-IP-Pool-Definition attribute, or both. An IP address pool you set up in RADIUS overrides an IP address pool you set up in the MAX configuration interface only if you designate the two pools by the same number.

If you need to define more than ten pools of addresses, you must use the RADIUS attribute Ascend-IP-Pool-Definition to configure the IP address pools.

Usage: Specify an integer corresponding to an address pool. The default value is 1. If you set Ascend-Assign-IP-Pool=0, RADIUS chooses an address from any pool that has one available.

Example: In this example, the user requests an address from pool #2:

```
Emma Password="m2dan", User-Service=Framed-User

    Framed-Protocol=PPP,
    Ascend-Route-IP=Route-IP-Yes,

    Ascend-Metric=2,

    Framed-Routing=None,
       Ascend-Assign-IP-Pool=2
```

See Also: “Ascend-IP-Pool-Definition (217)” on page 9-57

Ascend-Assign-IP-Server (145)

Description: In the Radipa-Hosts pseudo-user profile, the Ascend-Assign-IP-Server attribute specifies the IP address of the host running radipad.

Usage: Specify an IP address in dotted decimal notation. The default value is 0.0.0.0. Only one instance of this attribute can appear in the profile. The default value is a placeholder only. You must specify a valid IP address for radipad to work.

See Also: “Ascend-Assign-IP-Client (144)” on page 9-8
“Ascend-Assign-IP-Global-Pool (146)” on page 9-8

Ascend-Authen-Alias (203)

Description: The Ascend-Authen-Alias attribute sets the MAX unit’s login name during PPP authentication.

When the MAX places an outgoing call, it identifies itself by a login name and password. The login name is either its system name (as specified by the Name parameter in the System profile) or the value you specify for the Ascend-Authen-Alias attribute.

Usage: Specify a text string containing up to 16 characters. The default is the value of the Name parameter in the System profile.

Example: This example uses the Ascend-Authen-Alias attribute in an outgoing profile:

```
Homer-Out Password="Ascend", User-Service=Dialout-Framed-User

        User-Name="Homer",

        Ascend-Authen-Alias="myMAXcallingU",

        Ascend-Send-Auth=Send-Auth-PAP,

        Ascend-Send-Secret="passwrd1",

        Ascend-Dial-Number="31",

        Framed-Protocol=PPP,

        Framed-Address=10.0.100.1,

        Framed-Netmask=255.255.255.0,

        Ascend-Metric=2,

        Framed-Routing=None,

        Framed-Route="10.5.0.0/24 10.0.100.1 1",

        Ascend-Idle-Limit=30
```

Ascend-backup (176)

Description: The Ascend-backup attribute specifies the name of a backup profile for a nailed-up link when the physical connection fails on loss of a T1 line or WAN Serial port. The MAX automatically diverts traffic to the backup connection. When the primary connection comes back online, traffic again uses the primary connection.

When you use the backup connection, the MAX does not move routes to the backup profile. Therefore, the IP routes that appear in the terminal server display may be incorrect, although statistical counts reflect the change.

Usage: Specify the name of the profile that you want to act as the backup. The backup connection can be switched or nailed up. The default value is null.

Dependencies: Keep this additional information in mind:

- The Ascend-backup attribute applies to nailed-up connections only (Ascend-Call-Type=Nailed or Nailed/Mpp).
- Do not create nested backup connections.
- Attributes that you define for the primary profile do not automatically apply to the backup profile.

  For example, if you set the primary profile to filter Telnet packets, you must set the backup profile to filter Telnet packets as well. Outgoing Frame Relay packets are the only packets that follow the primary profile definitions. All other packets follow the backup profile definitions.
- If you configure a RADIUS user profile for Frame Relay and for backup, the MAX brings up the backup connection when any one of the DLCIs becomes unusable.
- Do not use the Ascend-backup attribute to provide alternative lines for getting to a single destination.

Ascend-BACP-Enable (134)

Description: The Ascend-BACP-Enable attribute specifies whether Bandwidth Allocation Control Protocol (BACP) is enabled for the link.

BACP is the Internet standard protocol equivalent to the Ascend MP+ bandwidth allocation protocol. BACP functions similarly to MP+ and uses the same attributes as MP+.

Usage: You can specify one of these settings:

- BACP-No (0) disables BACP for the link.

  The default value is BACP-No.
- BACP-Yes (1) enables BACP for the link.

Ascend-Base-Channel-Count (172)

Description: The Ascend-Base-Channel-Count attribute specifies the initial number of channels the MAX sets up when originating calls for a PPP, MP+, MP, or Combinet multichannel link.

Usage: The maximum number of channels you can specify depends upon the nature of the link:

- For a PPP link, the maximum number of channels is always 1.
- For an MP+ or MP link, you can specify any value up to the number of channels available, but the device at the remote end of the link must also support MP+ or MP.
- For a Combinet link, you can specify up to two channels.

The default value is 1.

Dependencies: The Ascend-Base-Channel-Count attribute does not apply when all channels of the link are nailed up (Ascend-Call-Type=Nailed).

For optimum MP+ performance, both sides of a connection must set these values to the same number:

- The base channel count, as specified by Base Ch Count (in the Connection profile) or Ascend-Base-Channel-Count (in RADIUS)
- The minimum channel count, as specified by Min Ch Count (in the Answer profile or Connection profile) or Ascend-Minimum-Channels (in RADIUS)
- The maximum channel count, as specified by Max Ch Count (in the Answer profile or Connection profile) or Ascend-Maximum-Channels (in RADIUS)

See Also: “Ascend-Add-Seconds (240)” on page 9-4
“Ascend-DBA-Monitor (171)” on page 9-33
“Ascend-Dec-Channel-Count (237)” on page 9-34
“Ascend-History-Weigh-Type (239)” on page 9-50
“Ascend-Inc-Channel-Count (236)” on page 9-55
“Ascend-Maximum-Channels (235)” on page 9-61
“Ascend-Minimum-Channels (173)” on page 9-65
“Ascend-Remove-Seconds (241)” on page 9-78
“Ascend-Seconds-Of-History (238)” on page 9-81
“Ascend-Target-Util (234)” on page 9-84

Ascend-Billing-Number (249)

Description: The Ascend-Billing-Number attribute specifies a billing number for charges you incur on the line. If you do not enter a billing number, the telephone company assigns charges to the telephone number associated with the line.

Your carrier determines the billing number, and uses it to sort your bill. If you have several departments, and each department has its own Ascend-Billing-Number, your carrier can separate and tally each department’s usage.

Usage: Specify a telephone number. You can indicate up to ten characters, and you must limit those characters to the following:

```
1234567890()[]!z-*# |
```

Dependencies: The MAX uses the Ascend-Billing-Number attribute differently depending on the type of line you use:

- For a T1 line, the MAX appends the value specified in the Ascend-Billing-Number attribute to the end of each phone number it dials for the call.
- Ascend-Billing-Number for outgoing calls on an ISDN BRI line applies only to installations in Australia.

- For a T1 PRI line, the MAX uses the Ascend-Billing-Number rather than the phone number ID to identify itself to the answering party.

  The Id Auth parameter enables you to require a device to authenticate incoming calls by checking the calling party’s phone number. The device performs Calling Line ID (CLID) authentication before answering an incoming call. The calling party’s phone number must match the Calling # parameter or the Caller-Id attribute. If the MAX cannot authenticate the call when CLID authentication is required, it rejects the call.

  If the calling party uses the Ascend-Billing-Number attribute instead of its phone number as its ID, the CLID the answering side uses is not the true phone number of the caller. This situation presents a security breach if you use Id Auth.

  Further, be aware that if you specify a value for the Ascend-Billing-Number attribute, there is no guarantee that the phone company will send it to the answering device.

See Also: “Caller-Id (31)” on page 9-90

Ascend-Bridge (230)

Description: The Ascend-Bridge attribute enables or disables protocol-independent bridging for the user profile.

Usage: You can specify one of these values:

- Bridge-No (0)

  This setting disables bridging for the link. Bridge-No is the default.

- Bridge-Yes (1)

  This setting enables bridging for the link.

Example: This user profile specifies an IPX bridging link:

```
MAX1 Password="m2dan", User-Service=Framed-User

    Framed-Protocol=PPP,

    Ascend-Route-IPX=Route-IPX-No,

    Ascend-Bridge=Bridge-Yes,
        Ascend-Handle-IPX=Handle-IPX-Client,

    Ascend-Netware-timeout=30
```

See Also: “Ascend-Bridge-Address (168)” on page 9-12

Ascend-Bridge-Address (168)

Description: The Ascend-Bridge-Address attribute specifies the IP address and associated MAC address of a device on a remote LAN to which the MAX can form a bridging connection.

Usage: The Ascend-Bridge-Address attribute has this format:

```
Ascend-Bridge-Address="MAC_address profile_name IP_address"
```

Table 9-1 describes Ascend-Bridge-Address arguments.

Table 9-1. Ascend-Bridge-Address arguments

Argument	Description
MAC_address	Specifies a MAC address in standard 12-digit hexadecimal format (yyyyyyyyyyyy) or in colon-separated format (yy:yy:yy:yy:yy:yy). If the leading digit of a colon-separated pair is 0 (zero), you do not need to enter it. That is, **`:y`** is the same as **`:0y`**. The default value is 000000000000.
profile_name	Specifies the name of the dialout profile the MAX uses to bring up the connection. You can specify either a Connection profile or a RADIUS user profile. The MAX looks for a local profile first.
IP_address	Specifies an IP address in dotted decimal notation. The default value is 0.0.0.0.

When your MAX receives an ARP request for one of the IP addresses you specify, the MAX replies with the corresponding MAC address and uses the specified profile to bring up a connection to that address. Because the MAX replies to these ARP requests as if the IP devices were local, you must have user profiles that bridge IP packets to each device.

Dependencies: Each bridge entry must appear in a pseudo-user profile. You create a pseudo-user to store information that the MAX can query—in this case, in order to store bridging information. For a unit-specific bridge entry, specify the first line of a pseudo-user profile in this format:

```
Bridge-unit_name-num Password="Ascend", User-Service=
Dialout-Framed-User
```

unit_name is the system name of the MAX—that is, the name specified by the Name parameter in the System profile. ***num*** is a number in a sequential series, starting at 1.

In each pseudo-user profile, you specify one or more Ascend-Bridge-Address attributes. Whenever you power on or reset the MAX, or when you select the Upd Rem Cfg command from the Sys Diag menu, RADIUS adds bridging entries to the bridge table in this way:

1. RADIUS looks for profiles having the format Bridge-***unit_name***-***num***, where ***unit_name*** is the system name and ***num*** is a number in a sequential series, starting with 1.
2. RADIUS loads the data to create the bridging tables.

Example: This example creates two bridging table entries.

```
Bridge-Ascend-1 Password="Ascend", User-Service=Dialout-Framed-User

       Ascend-Bridge-Address="2:2:3:10:11:12 Prof1 1.2.3.4 1",

       Ascend-Bridge-Address="2:2:3:13:14:15 Prof2 5.6.7.8 2"
```

See Also: “Ascend-Bridge (230)” on page 9-12

Ascend-Callback (246)

Description: The Ascend-Callback attribute enables or disables callback. Callback occurs when the MAX answers a call and verifies a name and password against a user profile. If Ascend-Callback=Yes, the MAX hangs up and dials back to the caller using these values:

- The phone number specified by Ascend-Dial-Number
- The password specified by Ascend-Send-Secret or Ascend-Send-Passwd
- Any other relevant attributes in the user profile that authenticated the call

Note: If you set up a RADIUS user profile for callback and CLID-only authentication, the MAX never answers the call. The caller can therefore avoid billing charges.

Usage: You can specify one of these values:

- Callback-No (0)

  This value indicates that the MAX answers in the normal manner after authentication.
- Callback-Yes (1)

  This value indicates that the MAX hangs up and calls back the caller after authentication.

Dependencies: The Ascend-Callback attribute applies only to incoming calls and should not appear in dial-out user profiles (when User-Service=Dialout-Framed-User).

Ascend-Call-By-Call (250)

Description: The Ascend-Call-By-Call attribute specifies the T1 PRI service that the MAX uses when placing a PPP call.

Usage: Specify a number corresponding to the type of service the MAX uses. The default value is 6. Table 9-2 lists the services available for each service provider.

Table 9-2. Ascend-Call-By-Call setting

Number	AT&T	Sprint	MCI
0	Disable call-by-call service.	Reserved	N/A
1	SDN (including GSDN)	Private	VNET/Vision
2	Megacom 800	Inwatts	800
3	Megacom	Outwatts	PRISM1, PRISM II, WATS
4	N/A	FX	900
5	N/A	Tie Trunk	DAL
6	ACCUNET Switched Digital Services	N/A	N/A

Table 9-2. Ascend-Call-By-Call setting (continued)

Number	AT&T	Sprint	MCI
7	Long Distance Service (including AT&T World Connect)	N/A	N/A
8	International 800 (I800)	N/A	N/A
16	AT&T MultiQuest	N/A	N/A

Ascend-Call-Filter (243)

Description: The Ascend-Call-Filter attribute defines a call filter.

Unlike the Filter profiles in the MAX configuration interface, RADIUS filters are part of the outgoing or incoming RADIUS user profile. The MAX uses a RADIUS filter only when the MAX places or answers a call with a RADIUS profile that includes the filter specification.

Usage: Filter entries apply on a first-match basis. Therefore, the order in you specify filter entries is significant. If you make changes to a filter in a RADIUS user profile, the changes do not take effect until a call uses that profile.

IP call filter entries

Use the following format for an IP call filter entry:

```
Ascend-Call-Filter="ip dir action
[dstip dest_ipaddr\subnet_mask][srcip src_ipaddr\subnet_mask]
[proto [dstport cmp value] [srcport cmp value] [est]]"
```

Note: A filter definition cannot contain newlines. The syntax appears on multiple lines for printing purposes only.

Table 9-3 describes each element of the syntax. None of the keywords are case sensitive.

Table 9-3. IP call filter syntax elements

Keyword or argument	Description
ip	Indicates an IP filter.
dir	Indicates filter direction. You can specify **in** (to filter packets coming into the MAX) or **out** (to filter packets going out of the MAX).

Table 9-3. IP call filter syntax elements (continued)

Keyword or argument	Description
action	Indicates what action the MAX should take with a packet that matches the filter. You can specify either **`forward`** or **`drop`**.
dstip *dest_ipaddr*	**`dstip`** is a keyword indicating *destination IP address*. The filter applies to packets whose destination address matches the value of ***`dest_ipaddr`***. If a subnet mask portion of the address is present, the MAX compares only the masked bits. If you set ***`dest_ipaddr`*** to 0.0.0.0, or if this keyword and its IP address specification are not present, the filter matches all IP packets.
srcip *src_ipaddr*	**`srcip`** is a keyword indicating *source IP address*. The filter applies to packets whose source address matches the value of ***`src_ipaddr`***. If a subnet mask portion of the address is present, the MAX compares only the masked bits. If you set ***`src_ipaddr`*** to 0.0.0.0, or if this keyword and its IP address specification are not present, the filter matches all IP packets.
proto	Indicates a protocol that you can specify as a name or a number. The filter applies to packets whose protocol field matches this value.The supported names and numbers are icmp (1), tcp (6), udp (17), and ospf (89). If you set ***`proto`*** to 0 (zero), the filter matches any protocol.
dstport *cmp value*	**`dstport`** is a keyword indicating *destination port*. This argument is valid only when the protocol is tcp (6) or udp (17). If you do not specify a destination port, the filter matches any port. ***`cmp`*** is an argument indicating how to compare the specified value to the actual destination port. It can have the value <, =, >, or !=. ***`value`*** can be a number or a name. Supported names and numbers are ftp-data (20), ftp (21), telnet (23), smtp (25), nameserver (42), domain (53), tftp (69), gopher (70), finger (79), www (80), kerberos (88), hostname (101), nntp (119), ntp (123), exec (512), login (513), cmd (514), and talk (517).

Table 9-3. IP call filter syntax elements (continued)

Keyword or argument	Description
srcport *cmp value*	**`srcport`** is a keyword indicating *source port*. It is valid only when the protocol is tcp (6) or udp (17). If you do not specify a source port, the filter matches any port. ***`cmp`*** is an argument indicating how to compare the specified value to the actual source port. It can have the value <, =, >, or !=. ***`value`*** can be a number or a name. Supported names and numbers are ftp-data (20), ftp (21), telnet (23), smtp (25), nameserver (42), domain (53), tftp (69), gopher (70), finger (79), www (80), kerberos (88), hostname (101), nntp (119), ntp (123), exec (512), login (513), cmd (514), and talk (517).
est	If you set this argument to 1, the filter matches a packet only if a TCP session is already established. It is valid only when the ***`proto`*** specification is tcp (6).

IPX call filter entries

Use the following format for an IPX call filter entry:

```
Ascend-Call-Filter="ipx <dir> <action>
   [srcipxnet <srcipxnet> srcipxnode <srcipxnode>
   [srcipxsoc <cmp> <value> ]]
   [dstipxnet <dstipxnet> dstipxnode <dstipxnode>
   [dstipxsoc <cmp> <value> ]]
```

Note: A filter definition cannot contain newlines. The syntax is shown on multiple lines for documentation purposes only.

Table 9-8 lists each keyword and argument.

Table 9-4. IPX filter syntax elements

Syntax element	Description
ipx	Designates an IPX filter.
<dir>	Indicates filter direction. You can specify “in” (to filter packets coming into the MAX) or “out” (to filter packets going out of the MAX).
<action>	Indicates the action the MAX should take with a packet that matches the filter. You can specify either “forward” or “drop”.
srcipxnet	Designates that a source IPX network number appears after this keyword.

Table 9-4. IPX filter syntax elements (continued)

Syntax element	**Description**
<srcipxnet>	Specifies the source IPX network number—the unique internal network number assigned to the NetWare server. You must specify the network number in hexadecimal format. Specifying 0x or 0X is optional.
srcipxnode	Designates that a source IPX node number appears after this keyword.
<srcipxnode>	Specifies the source IPX node number—the node number of the NetWare server. A valid IPX node number must accompany the IPX network number. You must specify the node number in hexadecimal format. Specifying 0x or 0X is optional. The IPX node number 0xffffffffffff is allowed and matches all IPX packets with the same node number.
srcipxsoc	Designates that a source IPX socket number specification appears after this keyword.
<cmp>	Indicates how to compare the socket number specified by <value> to the actual socket number in the packet. The <cmp> argument can have the value <, =, >, or !=.
<value>	Specifies the socket number of the NetWare server. Following the srcipxsoc keyword, the <value> argument specifies the source socket number; following the dstipxsoc keyword, the <value> argument specifies the destination socket number. You must specify the socket number in hexadecimal format. Specifying 0x or 0X is optional.
dstipxnet	Designates that a destination IPX network number appears after this keyword.
<dstipxnet>	Specifies the destination IPX network number—the unique internal network number assigned to the NetWare server. You must specify the network number in hexadecimal format. Specifying 0x or 0X is optional.
dstipxnode	Designates that a destination IPX node number appears after this keyword.
<dstipxnode>	Specifies the destination IPX node number—the node number of the NetWare server. A valid IPX node number must accompany the IPX network number. You must specify the node number in hexadecimal format. Specifying 0x or 0X is optional. The IPX node number 0xffffffffffff is allowed and matches all IPX packets with the same node number.
dstipxsoc	Designates that a source IPX socket number specification appears after this keyword.

Generic call filter entries

Use the following format for a generic call filter entry:

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

Note: A filter definition cannot contain newlines. The syntax appears on multiple lines for printing purposes only.

Table 9-5 describes each element of the syntax. None of the keywords are case sensitive.

Table 9-5. Generic call filter syntax elements

Keyword or argument	Description
generic	Indicates a generic filter.
dir	Indicates filter direction. You can specify **`in`** (to filter packets coming into the MAX) or **`out`** (to filter packets going out of the MAX).
action	Indicates what action the MAX should take with a packet that matches the filter. You can specify either **`forward`** or **`drop`**.
offset	Indicates the number of bytes masked from the start of the packet. The byte position specified by ***`offset`*** is called the byte-offset. Starting at the position specified by ***`offset`***, the MAX applies the value of the ***`mask`*** argument. A mask hides the part of a number that appears behind the binary zeroes in the mask. For example, if you set ***`mask`*** to ffff0000 in hexadecimal format, the filter uses only the first 16 binary digits in the comparison, since f=1111 in binary format. The unit then compares the unmasked portion of the packet with the value specified by the ***`value`*** argument.
mask	Indicates which bits to compare in a segment of the packet. The mask cannot exceed 6 bytes (12 hexadecimal digits). A one-bit in the mask indicates a bit to compare. A zero-bit indicates a bit to ignore. The length of the mask specifies the length of the comparison.
value	Indicates the value to compare to the packet contents at the specified offset in the packet. The length of the value must be the same as the length of the mask. Otherwise, the MAX ignores the filter.
compare	Indicates how the MAX compares a packet's contents to the value specified by ***`value`***. You can specify == (for Equal) or != (for NotEqual). The default value is Equal.

Table 9-5. Generic call filter syntax elements (continued)

Keyword or argument	Description
more	If present, specifies whether the MAX applies the next filter definition in the profile to the current packet before deciding whether to forward or drop the packet. The ***dir*** and ***action*** values for the next entry must be the same as the ***dir*** and ***action*** values for the current entry. Otherwise, the MAX ignores the ***more*** flag.

Example: These are examples of IP call filter entries:

```
Ascend-Call-Filter="ip in drop"
Ascend-Call-Filter="ip out forward tcp"
Ascend-Call-Filter="ip out forward tcp dstip 10.0.200.3/16 srcip
10.0.200.25/16 dstport!=telnet"
Ascend-Call-Filter="ip out forward tcp dstip 10.0.200.3/16 srcip
10.0.200.25/16 icmp"
```

These are examples of generic call filter entries:

```
Ascend-Call-Filter="generic in drop 0 ffff 0080"
Ascend-Call-Filter="generic in drop 0 ffff != 0080 more"
Ascend-Call-Filter="generic in drop 16 ff aa"
```

See Also: “Ascend-Data-Filter (242)” on page 9-24

Ascend-Call-Type (177)

Description: The Ascend-Call-Type attribute specifies the type of nailed-up connection in use.

Usage: You can specify one of these values:

- Nailed (1)

  This setting indicates a link that consists entirely of nailed-up channels. Nailed (1) is the default.

- Nailed/Mpp (2)

  This setting indicates a link that consists of both nailed-up and switched channels. The MAX establishes this connection whenever any of its nailed-up or switched channels are linked end-to-end. If a Nailed/Mpp link is down and the nailed-up channels are down, the link cannot re-establish itself until the MAX brings up one or more of the nailed-up channels, or dials one or more switched channels.

  Typically, the MAX dials a call when it receives a packet whose destination is the unit at the remote end of the Nailed/Mpp connection. The packet initiating the switched call must come from the caller side of the connection.

  If a failed channel is in the group specified by the Ascend-Group attribute, the MAX replaces that channel with a switched channel, even if the call is online with more than the minimum number of channels. The MAX replaces failed nailed-up channels with switched channels, regardless of the Min Ch Count setting.

- Perm/Switched (3)

  This setting indicates a permanent switched connection—an outbound call that attempts to remain up at all times. If the unit or central switch resets, or if the link goes down, the permanent switched connection attempts to restore the link at ten-second intervals.

  Use this setting if your telephone company charges for each incoming and outgoing connection attempt, but does not charge for connection time on local calls. Ascend's regular bandwidth-on-demand feature conserves connection time but causes many connection attempts. A permanent switched connection performs the opposite function—it conserves connection attempts but causes a long connection time.

  For the answering device at the remote end of the permanent switched connection, we recommend that you configure the Connection profile to answer calls but not to originate them. If the remote device initiates a call, the MAX simply does not answer it. This situation could result in repeated charges for calls that have no purpose. To keep the remote device from originating calls, set AnsOrig=Ans Only for that device.

Dependencies: The MAX adds or subtracts switched channels on a Nailed/Mpp connection as the settings on either side of the connection require. Each side makes its calculations based on the traffic it receives at that side. If the two sides of the connection disagree on the number of channels needed, the side requesting the greater number prevails.

The DO Hangup command works only from the caller side of the connection when you choose Nailed/Mpp.

Ascend-CBCP-Enable (112)

Description: Specifies how the MAX responds to requests by callers to support CBCP.

Note: Make sure you set CBCP Enable=Yes in the Ethernet > Answer > PPP Options menu.

Usage: Specify one of the following settings:

- CBCP-Enabled (0)—Specifies that the MAX will positively acknowledge, during LCP negotiations, support for CBCP.
- CBCP-Not-Enabled (1)—Specifies that the MAX will reject any request to support CBCP.

See Also: Ascend-CBCP-Mode, Ascend-CBCP-Trunk-Group

Ascend-CBCP-Mode (113)

Description: Specifies what method of callback the MAX offers the incoming caller.

Note: Make sure you set CBCP Enable=Yes in the Ethernet > Answer > PPP Options menu.

Usage: Specify one of the following values:

- CBCP-No-Callback (1)—Applies for Windows NT or Windows 95 clients who must not be called back. Because CBCP has been negotiated initially, the Windows clients must have validation from the MAX that no callback is used for this connection.
- CBCP-User-Callback (2)—Specifies that the caller will supply the number the MAX uses for the callback.
- CBCP-Profile-Callback (3)—Specifies that the MAX will use the number in Ascend-Dial-Number for the callback

- CBCP-User-Or-No (7)—Specifies that the caller has the option of either supplying the number to dial or specifying that no callback is used for the call. If no callback is chosen, the call will not be disconnected by the MAX.

Dependencies: Ascend-CBCP-Mode applies only if CBCP is successfully negotiated for a connection.

See Also: Ascend-CBCP-Enable, Ascend-CBCP-Trunk-Group

Ascend-CBCP-Trunk-Group (115)

Description: Assigns the callback to a MAX trunk group. This attribute is used only when the caller is specifying the phone number the MAX uses for the callback. The value in Ascend-CBCP-Trunk-Group is prepended to the caller-supplied number when the MAX calls back.

Note: Make sure you set CBCP Enable=Yes in the Ethernet > Answer > PPP Options menu.

Usage: You can specify a number between 4 and 9, inclusive. The default is 9.

Dependencies: Ascend-CBCP-Trunk-Group applies only if CBCP is negotiated for a connection.

See Also: Ascend-CBCP-Enable, Ascend-CBCP-Mode

Ascend-Client-Gateway (132)

Description: The Ascend-Client-Gateway attribute specifies the default route for IP packets coming from the user on this connection.

Usage: Specify the IP address of the next hop router in dotted decimal notation. The default value is 0.0.0.0. If you accept this value, the Ascend unit routes packets as specified in the routing table, using the system-wide default route if it cannot find a more specific route.

The Ascend unit must have a direct route to the address you specify. The direct route can take place via a profile or an Ethernet connection. If the Ascend unit does not have a direct route, it drops the packets on the connection. When you diagnose routing problems with a profile using this feature, an error in a per-user gateway address is not apparent from inspection of the global routing table.

Example: If you specify Ascend-Client-Gateway=10.0.0.3 in the RADIUS user profile Berkeley, IP packets from the user with destinations through the default route goes through the router at 10.0.0.3.

Ascend-Connect-Progress (196)

Description: The Ascend-Connect-Progress attribute specifies the state of the connection before it disconnects.

The MAX includes Ascend-Connect-Progress in an Accounting-Request packet when both of these conditions are true:

- The session has ended or has failed to authenticate (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-Connect-Progress can have any one of values specified in Table 9-6.

Table 9-6. Ascend-Connect-Progress codes

Code	Explanation
0	No progress.
1	Not applicable.
2	The progress of the call is unknown.
10	The call is up.
30	The modem is up.
31	The modem is waiting for DCD.
32	The modem is waiting for result codes.
40	The terminal server session has started up.
41	The MAX is establishing the TCP connection.
42	The MAX is establishing the immediate Telnet connection.
43	The MAX has established a raw TCP session with the host. This code does not imply that the user has logged into the host.
44	The MAX has established an immediate Telnet connection with the host. This code does not imply that the user has logged into the host.
45	The MAX is establishing an Rlogin session.
46	The MAX has established an Rlogin session with the host. This code does not imply that the user has logged into the host.
60	The LAN session is up.
61	LCP negotiations are allowed.
62	CCP negotiations are allowed.
63	IPNCP negotiations are allowed.
64	Bridging NCP negotiations are allowed.
65	LCP is in the Open state.
66	CCP is in the Open state.
67	IPNCP is in the Open state.
68	Bridging NCP is in the Open state.
69	LCP is in the Initial state.

Table 9-6. Ascend-Connect-Progress codes (continued)

Code	Explanation
70	LCP is in the Starting state.
71	LCP is in the Closed state.
72	LCP is in the Stopped state.
73	LCP is in the Closing state.
74	LCP is in the Stopping state.
75	LCP is in the Request Sent state.
76	LCP is in the ACK Received state.
77	LCP is in the ACK Sent state.
80	IPXNCP is in the Open state.
90	V.110 is up.
91	V.110 is in the Open state.
92	V.110 is in the Carrier state.
93	V.110 is in the Reset state.
94	V.110 is in the Closed state.

Ascend-Data-Filter (242)

Description: The Ascend-Data-Filter attribute defines a data filter.

Unlike the Filter profiles in the MAX configuration interface, RADIUS filters are part of the outgoing or incoming RADIUS user profile. The MAX uses a RADIUS filter only when the MAX places or answers a call with a RADIUS profile that includes the filter specification.

Usage: Filter entries apply on a first-match basis. Therefore, the order in you specify filter entries is significant. If you make changes to a filter in a RADIUS user profile, the changes do not take effect until a call uses that profile.

IP data filter entries

Use the following format for an IP data filter entry:

```
Ascend-Data-Filter="ip dir action
[dstip dest_ipaddr\subnet_mask][srcip src_ipaddr\subnet_mask]
[proto [dstport cmp value] [srcport cmp value] [est]]"
```

Note: A filter definition cannot contain newlines. The syntax appears on multiple lines for printing purposes only.

Table 9-7 describes each element of the syntax. None of the keywords are case sensitive.

Table 9-7. IP data filter syntax elements

Keyword or argument	Description
ip	Indicates an IP filter.
dir	Indicates filter direction. You can specify **`in`** (to filter packets coming into the MAX) or **`out`** (to filter packets going out of the MAX).
action	Indicates what action the MAX should take with a packet that matches the filter. You can specify either **`forward`** or **`drop`**.
dstip *dest_ipaddr*	**`dstip`** is a keyword indicating *destination IP address*. The filter applies to packets whose destination address matches the value of ***`dest_ipaddr`***. If a subnet mask portion of the address is present, the MAX compares only the masked bits. If you set ***`dest_ipaddr`*** to 0.0.0.0, or if this keyword and its IP address specification are not present, the filter matches all IP packets.
srcip *src_ipaddr*	**`srcip`** is a keyword indicating *source IP address*. The filter applies to packets whose source address matches the value of ***`src_ipaddr`***. If a subnet mask portion of the address is present, the MAX compares only the masked bits. If you set ***`src_ipaddr`*** to 0.0.0.0, or if this keyword and its IP address specification are not present, the filter matches all IP packets.
proto	Indicates a protocol that you can specify as a name or a number. The filter applies to packets whose protocol field matches this value.The supported names and numbers are icmp (1), tcp (6), udp (17), and ospf (89). If you set ***`proto`*** to 0 (zero), the filter matches any protocol.
dstport *cmp value*	**`dstport`** is a keyword indicating *destination port*. This argument is valid only when the protocol is tcp (6) or udp (17). If you do not specify a destination port, the filter matches any port. ***`cmp`*** is an argument indicating how to compare the specified value to the actual destination port. It can have the value <, =, >, or !=. ***`value`*** can be a number or a name. Supported names and numbers are ftp-data (20), ftp (21), telnet (23), smtp (25), nameserver (42), domain (53), tftp (69), gopher (70), finger (79), www (80), kerberos (88), hostname (101), nntp (119), ntp (123), exec (512), login (513), cmd (514), and talk (517).

Table 9-7. IP data filter syntax elements (continued)

Keyword or argument	Description
srcport *cmp value*	**`srcport`** is a keyword indicating *source port*. It is valid only when the protocol is tcp (6) or udp (17). If you do not specify a source port, the filter matches any port. ***`cmp`*** is an argument indicating how to compare the specified value to the actual source port. It can have the value <, =, >, or !=. ***`value`*** can be a number or a name. Supported names and numbers are ftp-data (20), ftp (21), telnet (23), smtp (25), nameserver (42), domain (53), tftp (69), gopher (70), finger (79), www (80), kerberos (88), hostname (101), nntp (119), ntp (123), exec (512), login (513), cmd (514), and talk (517).
est	If you set this argument to 1, the filter matches a packet only if a TCP session is already established. It is valid only when the ***`proto`*** specification is tcp (6).

IPX data filter entries

Use the following format for an IPX data filter entry:

```
Ascend-Data-Filter="ipx <dir> <action>
   [srcipxnet <srcipxnet> srcipxnode <srcipxnode>
   [srcipxsoc <cmp> <value> ]]
   [dstipxnet <dstipxnet> dstipxnode <dstipxnode>
   [dstipxsoc <cmp> <value> ]]
```

Note: A filter definition cannot contain newlines. The syntax is shown on multiple lines for documentation purposes only.

Table 9-8 lists each keyword and argument.

Table 9-8. IPX filter syntax elements

Syntax element	Description
ipx	Designates an IPX filter.
<dir>	Indicates filter direction. You can specify “in” (to filter packets coming into the MAX) or “out” (to filter packets going out of the MAX).
<action>	Indicates the action the MAX should take with a packet that matches the filter. You can specify either “forward” or “drop”.
srcipxnet	Designates that a source IPX network number appears after this keyword.

Table 9-8. IPX filter syntax elements (continued)

Syntax element	**Description**
<srcipxnet>	Specifies the source IPX network number—the unique internal network number assigned to the NetWare server. You must specify the network number in hexadecimal format. Specifying 0x or 0X is optional.
`srcipxnode`	Designates that a source IPX node number appears after this keyword.
<srcipxnode>	Specifies the source IPX node number—the node number of the NetWare server. A valid IPX node number must accompany the IPX network number. You must specify the node number in hexadecimal format. Specifying 0x or 0X is optional. The IPX node number 0xffffffffffff is allowed and matches all IPX packets with the same node number.
srcipxsoc	Designates that a source IPX socket number specification appears after this keyword.
<cmp>	Indicates how to compare the socket number specified by <value> to the actual socket number in the packet. The <cmp> argument can have the value <, =, >, or !=.
<value>	Specifies the socket number of the NetWare server. Following the srcipxsoc keyword, the <value> argument specifies the source socket number; following the dstipxsoc keyword, the <value> argument specifies the destination socket number. You must specify the socket number in hexadecimal format. Specifying 0x or 0X is optional.
dstipxnet	Designates that a destination IPX network number appears after this keyword.
<dstipxnet>	Specifies the destination IPX network number—the unique internal network number assigned to the NetWare server. You must specify the network number in hexadecimal format. Specifying 0x or 0X is optional.
dstipxnode	Designates that a destination IPX node number appears after this keyword.
<dstipxnode>	Specifies the destination IPX node number—the node number of the NetWare server. A valid IPX node number must accompany the IPX network number. You must specify the node number in hexadecimal format. Specifying 0x or 0X is optional. The IPX node number 0xffffffffffff is allowed and matches all IPX packets with the same node number.
dstipxsoc	Designates that a source IPX socket number specification appears after this keyword.

Generic data filter entries

Use the following format for a generic data filter entry:

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

Note: A filter definition cannot contain newlines. The syntax appears on multiple lines for printing purposes only.

Table 9-9 describes each element of the syntax. None of the keywords are case sensitive.

Table 9-9. Generic data filter syntax elements

Keyword or argument	Description
generic	Indicates a generic filter.
dir	Indicates filter direction. You can specify **`in`** (to filter packets coming into the MAX) or **`out`** (to filter packets going out of the MAX).
action	Indicates what action the MAX should take with a packet that matches the filter. You can specify either **`forward`** or **`drop`**.
offset	Indicates the number of bytes masked from the start of the packet. The byte position specified by ***`offset`*** is called the byte-offset. Starting at the position specified by ***`offset`***, the MAX applies the value of the ***`mask`*** argument. A mask hides the part of a number that appears behind the binary zeroes in the mask. For example, if you set ***`mask`*** to ffff0000 in hexadecimal format, the filter uses only the first 16 binary digits in the comparison, since f=1111 in binary format. The unit then compares the unmasked portion of the packet with the value specified by the ***`value`*** argument.
mask	Indicates which bits to compare in a segment of the packet. The mask cannot exceed 6 bytes (12 hexadecimal digits). A one-bit in the mask indicates a bit to compare. A zero-bit indicates a bit to ignore. The length of the mask specifies the length of the comparison.
value	Indicates the value to compare to the packet contents at the specified offset in the packet. The length of the value must be the same as the length of the mask. Otherwise, the MAX ignores the filter.
compare	Indicates how the MAX compares a packet's contents to the value specified by ***`value`***. You can specify == (for Equal) or != (for NotEqual). The default value is Equal.

Table 9-9. Generic data filter syntax elements (continued)

Keyword or argument	Description
more	If present, specifies whether the MAX applies the next filter definition in the profile to the current packet before deciding whether to forward or drop the packet. The ***dir*** and ***action*** values for the next entry must be the same as the ***dir*** and ***action*** values for the current entry. Otherwise, the MAX ignores the ***more*** flag.

Example: These are examples of IP data filter entries:

```
Ascend-Data-Filter="ip in drop"
```

```
Ascend-Data-Filter="ip out forward tcp"
```

```
Ascend-Data-Filter="ip out forward tcp dstip 10.0.200.3/16 srcip
10.0.200.25/16 dstport!=telnet"
```

```
Ascend-Data-Filter="ip out forward tcp dstip 10.0.200.3/16 srcip
10.0.200.25/16 icmp"
```

These are examples of generic data filter entries:

```
Ascend-Data-Filter="generic in drop 0 ffff 0080"
```

```
Ascend-Data-Filter="generic in drop 0 ffff != 0080 more"
```

```
Ascend-Data-Filter="generic in drop 16 ff aa"
```

See Also: “Ascend-Call-Filter (243)” on page 9-15

Ascend-Data-Rate (197)

Description: The Ascend-Data-Rate attribute specifies the receive baud rate of the connection in bits per second.

The MAX includes Ascend-Data-Rate in an Accounting-Request packet when both of these conditions are true:

- The session has ended or has failed to authenticate (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-Data-Rate does not appear in a user profile. Its default value is 0 (zero).

Ascend-Data-Svc (247)

Description: The Ascend-Data-Svc attribute specifies the type of data service the link uses for outgoing calls.

Usage: The data service you specify must be available end-to-end. You can set the Ascend-Data-Svc attribute to one of the values listed in Table 9-10.

Table 9-10.Ascend-Data-Svc settings

Setting	Description
Switched-Voice-Bearer (0)	This value applies only to calls made over an ISDN BRI or T1 PRI line. When you specify this setting, the MAX enables the network to place an end-to-end digital voice call for transporting data when a switched data service is not available.
Switched-56KR (1)	The call contains restricted data, guaranteeing that the data the MAX transmits meets the density restrictions of D4-framed T1 lines. D4 specifies the D4 format, also known as the Superframe format, for framing data at the physical layer. This format consists of 12 consecutive frames, separated by framing bits. The call connects to the Switched-56 data service. The only services available to lines using inband signaling (T1 access lines containing one or more switched channels, and Switched-56 lines) are Switched-56K and Switched-56KR.
Switched-64K (2)	The call contains any type of data and connects to the Switched-64 data service.
Switched-64KR (3)	The call contains restricted data and connects to the Switched-64 data service.
Switched-56K (4)	The call contains any type of data and connects to the Switched-56 data service. The only services available to lines using inband signaling (T1 access lines containing one or more switched channels, and Switched-56 lines) are Switched-56K and Switched- 56KR. For most T1 PRI lines, select Switched-56K.
Nailed-56KR (1)	The call contains restricted data and connects to the Nailed-56 data service.
Nailed-64K (2)	The call contains any type of data and connects to the Nailed-64 data service.
Switched-384KR (5)	The call contains restricted data, and connects to MultiRate or GloBanD data services at 384 kbps.
Switched-384K (6)	The call contains any type of data and connects to the Switched-384 data service. This AT&T data service does not require MultiRate or GloBanD.

Table 9-10.Ascend-Data-Svc settings (continued)

Setting	**Description**
Switched-1536K (7)	The call contains any type of data and connects to the Switched-1536 data service at 1536 kbps. This setting is valid only for a MAX that supports ISDN D-channel signaling, and that connects to two or more T1 PRI lines using Non-Facility Associated Signaling (NFAS).
Switched-1536KR (8)	The call contains restricted data, and connects to the Switched-1536 data service at 1536 kbps. This setting is valid only for a MAX that supports ISDN D-channel signaling, and that connects to two or more T1 PRI lines using Non-Facility Associated Signaling (NFAS).
Switched-128K (9)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-192K (10)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-256K (11)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-320K (12)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-384K-MR (13)	This value is available on a T1 PRI line with the MultiRate data service.
Switched-448K (14)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-512K (15)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-576K (16)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-640K (17)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-704K (18)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-768K (19)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-832K (20)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.

Table 9-10.Ascend-Data-Svc settings (continued)

Setting	Description
Switched-896K (21)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-960K (22)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1024K (23)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1088K (24)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1152K (25)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1216K (26)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1280K (27)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1344K (28)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1408K (29)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1472K (30)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1600K (31)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1664K (32)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1728K (33)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1792K (34)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1856K (35)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1920K (36)	This value is available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-inherited (37)	This setting applies to calls placed by a device connected to a local ISDN BRI line supplied by a Host/ BRI module. The call connects with the data service as requested by the caller on the local ISDN BRI line.

Table 9-10.Ascend-Data-Svc settings (continued)

Setting	Description
Switched-restricted-bearer-x30 (38)	This setting specifies the 56-kbps X.30 switched data service available from DPNSS and DASS 2 switches.
Switched-clear-bearer-v110 (39)	This setting specifies the 64-kbps V.110 switched data service available from DPNSS and DASS 2 switches.
Switched-restricted-64-x30 (40)	This setting specifies the 64-kbps X.30 switched data service available from DPNSS and DASS 2 switches. For most DASS 2 and DPNSS installations, select Switched-restricted-64-x30.
Switched-clear-56-v110 (41)	This setting specifies the 56-kbps V.110 switched data service available from DPNSS and DASS 2 switches.
Switched-modem (42)	This setting places an outgoing call on any available digital modem. If no digital modems are available, the MAX does not place the call. The data rate depends upon the quality of the connections between modems and the types of modems in use. The Switched-modem setting requires that your MAX have digital modems. Modem applies only for PPP, MP+, and X.25/PAD calls. Currently, the MAX does not support multichannel modem calls. When you need to set up a dial-out profile in RADIUS for the MAX 4000, MAX 2000, MAX 1800, or Pipeline 400, set Ascend-Data-Svc=Switched-modem.
Switched-atmodem (43)	This setting applies only to the MAX 200 and is equivalent to Switched-modem.

Dependencies: Keep this additional information in mind:

- You can determine the base bandwidth of a call by multiplying the value of the Ascend-Base-Channel-Count attribute by the value of the Ascend-Data-Svc attribute.
- Either party can request a data service that is unavailable.
  In this case, the MAX cannot connect the call.

Ascend-DBA-Monitor (171)

Description: The Ascend-DBA-Monitor attribute specifies how the Ascend calling unit monitors the traffic on an MP+ call. The Ascend unit can use this information to add or subtract bandwidth as necessary.

Usage: You can specify one of these values:

- DBA-Transmit (0)
  This setting indicates that the MAX adds or subtracts bandwidth based on the amount of data it transmits.

DBA-Transmit is the default.

- DBA-Transmit-Recv (1)

  This setting indicates that the MAX adds or subtracts bandwidth based on the amount of data it transmits *and* receives.

- DBA-None (2)

  This setting indicates that the MAX does not monitor traffic over the link.

Dependencies: Keep this additional information in mind:

- The MAX supports Ascend-DBA-Monitor only on MP+ calls.
- If both sides of the link have Ascend-DBA-Monitor set to DBA-None, Dynamic Bandwidth Allocation is disabled.

See Also: "Ascend-Add-Seconds (240)" on page 9-4
"Ascend-Base-Channel-Count (172)" on page 9-10
"Ascend-Dec-Channel-Count (237)" on page 9-34
"Ascend-History-Weigh-Type (239)" on page 9-50
"Ascend-Inc-Channel-Count (236)" on page 9-55
"Ascend-Maximum-Channels (235)" on page 9-61
"Ascend-Minimum-Channels (173)" on page 9-65
"Ascend-Remove-Seconds (241)" on page 9-78
"Ascend-Seconds-Of-History (238)" on page 9-81
"Ascend-Target-Util (234)" on page 9-84

Ascend-Dec-Channel-Count (237)

Description: The Ascend-Dec-Channel-Count attribute specifies the number of channels the MAX removes when bandwidth changes either manually or automatically during a call.

Usage: Specify a number between 1 and 32. The default value is 1.

Dependencies: Keep this additional information in mind:

- Ascend-Dec-Channel-Count does not apply if all channels of a link are nailed up (Ascend-Call-Type=Nailed).
- Ascend-Dec-Channel-Count applies only when the link is using MP+ encapsulation (Framed-Protocol=MPP).
- You cannot clear a call by decrementing channels.

See Also: "Ascend-Add-Seconds (240)" on page 9-4
"Ascend-Base-Channel-Count (172)" on page 9-10
"Ascend-DBA-Monitor (171)" on page 9-33
"Ascend-History-Weigh-Type (239)" on page 9-50
"Ascend-Inc-Channel-Count (236)" on page 9-55
"Ascend-Maximum-Channels (235)" on page 9-61
"Ascend-Minimum-Channels (173)" on page 9-65
"Ascend-Remove-Seconds (241)" on page 9-78
"Ascend-Seconds-Of-History (238)" on page 9-81
"Ascend-Target-Util (234)" on page 9-84

Ascend-DHCP-Maximum-Leases

Description: The Ascend-DHCP-Maximum-Leases attribute specifies the maximum number of dynamic addresses the MAX can assign to Network Address Translation (NAT) for LAN clients using this connection.

Usage: Specify a value between 1 and 254. The default is 4.

See Also: "Ascend-DHCP-Pool-Number (148)" on page 9-35
"Ascend-DHCP-Reply (147)" on page 9-35

Ascend-DHCP-Pool-Number (148)

Description: The Ascend-DHCP-Pool-Number attribute indicates the address pool from which the MAX assigns a dynamic IP address to the Dynamic Host Configuration Protocol (DHCP) client.

Usage: Specify an integer between 1 and the number of address pools defined on the MAX. The default value is 0 (zero), which specifies that the MAX uses the first defined IP address pool.

Dependencies: When the DHCP client requests an address, the MAX allocates an IP address from one of its IP address pools and assigns it to the client for 30 minutes. The client must renew the IP address assignment after the 30-minute period expires.

In its local memory, the MAX keeps track of all the IP addresses it has assigned. Therefore, it loses the entries for current, unexpired IP address assignments when you reset it. If a client holds an unexpired IP address assignment when you reset the MAX, the MAX may assign the same address to a new client. These duplicate IP addresses cause network problems until the first assignment expires or one of the clients reboots.

See Also: "Ascend-DHCP-Maximum-Leases" on page 9-35
"Ascend-DHCP-Reply (147)" on page 9-35

Ascend-DHCP-Reply (147)

Description: The Ascend-DHCP-Reply attribute specifies whether the MAX processes DHCP packets and acts as a DHCP server on this connection.

Usage: You can specify one of these settings:

- DHCP-Reply-Yes indicates that the MAX processes DHCP packets.
  - For a bridged connection, the MAX responds to all DHCP requests.
  - For a non-bridged connection, the MAX responds only to Network Address Translation (NAT) for LAN DHCP packets.
- DHCP-Reply-No indicates that the MAX does not process DHCP packets, but routes or bridges DHCP packets as any other packet.

  The default value is DHCP-Reply-No.

See Also: "Ascend-DHCP-Maximum-Leases" on page 9-35
"Ascend-DHCP-Pool-Number (148)" on page 9-35

Ascend-Dialout-Allowed (131)

Description: The Ascend-Dialout-Allowed attribute specifies whether the user associated with an outgoing RADIUS user profile can dial out using one of the MAX unit's digital modems.

Usage: You can specify one of these settings:

- Dialout-Not-Allowed (0) indicates that the RADIUS user profile does not allow modem dialout.

  The default value is Dialout-Not Allowed.
- Dialout-Allowed (1) indicates that the RADIUS user profile allows modem dialout.

Ascend-Dial-Number (227)

Description: The Ascend-Dial-Number attribute specifies the phone number the MAX dials to reach the bridge, router, or node at the remote end of the link.

Usage: Specify a telephone number. You can enter up to 21 characters, and you must limit those characters to the following:

```
1234567890()[]!z-*#|
```

The MAX sends only the numeric characters to place a call. The default value is null.

If Use Trunk Grps=Yes in the System>Sys Config menu, the first digits in the Ascend-Dial-Number attribute have the meanings listed in Table 9-11.

Table 9-11.Ascend-Dial-Number digits

Digit	Explanation
First digit is between 4 and 9.	The MAX places the call over the corresponding trunk group listed in the Ch *n* Trnk Grp, B1 Trnk Grp, or B2 Trnk Grp parameters in the Line profile. If Dial Plan=Trunk Grp, the digits following the first digit constitute an ordinary phone number. If Dial Plan=Extended, the next two digits specify the Dial Plan profile containing the parameters the MAX uses when making the call. These parameters constitute the extended dial plan. An ordinary phone number follows these two digits.
First digit is 3.	The MAX places the call to a destination listed in a Destination profile. In this case, the second and third digits indicate the number of the Destination profile.

Table 9-11.Ascend-Dial-Number digits (continued)

Digit	Explanation
First digit is 2.	The MAX places the call between host ports on the same MAX, or between Terminal Equipment (TEs) on a local ISDN BRI line on the same MAX. The first type of call is a port-to-port call. The latter type of call is a TE-to-TE call. In a port-to-port call, the second digit indicates the slot of an AIM/6 module. In a TE-to-TE call, the second digit indicates the slot of a Host/BRI module. If you enter 0 (zero) for the second digit, the call connects to any available AIM port and ignores the third digit. If you enter a nonzero value for the second digit, the third digit selects the AIM port (for a port-to-port call) or a local ISDN BRI port (for a TE-to-TE call). If you enter 0 (zero) for the third digit, the call connects to any available AIM port or local ISDN BRI line in the module selected by the second digit.

Ascend-Disconnect-Cause (195)

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

The MAX includes Ascend-Disconnect-Cause in an Accounting-Request packet when both of these conditions are true:

- The session has ended or has failed to authenticate (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-Disconnect-Cause can return any of the values listed in Table 9-12.

Table 9-12.Ascend-Disconnect-Cause codes

Code	Description
0	No reason.
1	The event was not a disconnect.
2	The reason for the disconnect is unknown. This code can appear when the remote connection goes down.
3	The call has disconnected.
4	CLID authentication has failed.
These codes can appear if a disconnect occurs during the initial modem connection.	
10	The modem never detected DCD.
11	The modem detected DCD, but became inactive.

Table 9-12.Ascend-Disconnect-Cause codes (continued)

Code	Description
12	The result codes could not be parsed.
These codes are related to immediate Telnet and raw TCP disconnects during a terminal server session.	
20	The user exited normally from the terminal server.
21	The user exited from the terminal server because the idle timer expired.
22	The user exited normally from a Telnet session.
23	The user could not switch to SLIP or PPP because the remote host had no IP address or because the dynamic pool could not assign one.
24	The user exited normally from a raw TCP session.
25	The login process ended because the user failed to enter a correct password after three attempts.
26	The raw TCP option is not enabled.
27	The login process ended because the user typed Ctrl-C.
28	The terminal server session has ended.
29	The user closed the virtual connection
30	The virtual connection has ended.
31	The user exited normally from an Rlogin session
32	The user selected an invalid Rlogin option.
33	The MAX has insufficient resources for the terminal server session.
These codes concern PPP connections.	
40	PPP LCP negotiation timed out while waiting for a response from a peer.
41	There was a failure to converge on PPP LCP negotiations.
42	PPP PAP authentication failed.
43	PPP CHAP authentication failed.
44	Authentication failed from the remote server.
45	The peer sent a PPP Terminate Request.

Table 9-12.Ascend-Disconnect-Cause codes (continued)

Code	**Description**
46	LCP got a close request from the upper layer while LCP was in an open state.
47	LCP closed because no NCPs were open.
48	LCP closed because it could not determine to which MP bundle it should add the user.
49	LCP closed because the MAX could not add any more channels to an MP session.
These codes are related to immediate Telnet and raw TCP disconnects, and contain more specific information than the Telnet and TCP codes listed earlier in this table.	
50	The Raw TCP or Telnet internal session tables are full.
51	Internal resources are full.
52	The IP address for the Telnet host is invalid.
53	The MAX could not resolve the hostname.
54	The MAX detected a bad or missing port number.
The TCP stack can return these disconnect codes during an immediate Telnet or raw TCP session.	
60	The host reset the TCP connection.
61	The host refused the TCP connection.
62	The TCP connection timed out.
63	A foreign host closed the TCP connection.
64	The TCP network was unreachable.
65	The TCP host was unreachable.
66	The TCP network was administratively unreachable.
67	The TCP host was administratively unreachable.
68	The TCP port was unreachable.
These are additional disconnect codes.	
100	The session timed out because there was no activity on a PPP link.
101	The session failed for security reasons.
102	The session ended for callback.

Table 9-12.Ascend-Disconnect-Cause codes (continued)

Code	Description
120	One end refused the call because the protocol was disabled or unsupported.
150	RADIUS requested the disconnect.
160	The allowed retries for V.110 synchronization have been exceeded.
170	PPP authentication has timed out.
180	The call disconnected as the result of a local hangup.
185	The call disconnected because the remote end hung up.
190	The call disconnected because the T1 line that carried it was quiesced.
195	The call disconnected because the call duration exceeded the maximum amount of time allowed by the Max Call Mins or Max DS0 Mins parameter on the MAX.

Ascend-Event-Type (150)

Description: The Ascend-Event-Type attribute indicates a coldstart notification, informing the accounting server that the MAX has started up, or a session event, informing the authentication server that a session has begun.

In a coldstart notification, the MAX sends values for NAS-Identifier, Ascend-Event-Type, and Ascend-Number-Sessions in an Ascend-Event-Request packet (code 33). The RADIUS accounting server must send back an Ascend-Event-Response packet (code 34) with the correct identifier to the MAX.

In a session event, the MAX sends values for Password, NAS-Identifier, Ascend-Event-Type, and Ascend-Number-Sessions in an Ascend-Event-Request packet (code 33) when Auth=RADIUS/LOGOUT in Ethernet>Mod Config>Auth. The authentication server must send back an Ascend-Event-Response packet (code 34) with the correct identifier to the MAX.

Usage: For a coldstart notification, Ascend-Event-Type=Ascend-Coldstart (1). For a session event, Ascend-Event-Type=Ascend-Session-Event (2)

See Also: “Ascend-Number-Sessions (202)” on page 9-68
“NAS-Identifier (4)” on page 9-102

Ascend-Expect-Callback (149)

Description: The Ascend-Expect-Callback attribute specifies whether a user dialing out should expect the remote end to call back.

When the remote device is set to call back (Ascend-Callback=Callback-Yes or Callback=Yes) and CLID authentication is not required, the remote device answers the call, verifies a name and password against a user profile, hangs up, and dials back to the caller using these values:

- The phone number specified by Ascend-Dial-Number
- The password specified by Ascend-Send-Secret or Ascend-Send-Passwd
- Any other relevant attributes in the user profile that authenticated the call

If the remote RADIUS user profile is set up for callback, and the remote unit requires CLID-only authentication (Id Auth=Require), the remote device never answers the call. The caller can therefore avoid billing charges. However, a problem can also occur. To the caller, it appears as though the call never got through at all. This is a special problem for Ping and Telnet, because these processes continuously try to open a connection and reject any callback.

When you set Ascend-Expect-Callback=Expect-Callback-Yes, calls that dial out and do not connect (for any reason) appear on a list that disallows any further calls to that destination for 90 seconds. This delay gives the remote device an opportunity to complete the callback.

Usage: You can specify one of these values:

- Expect-Callback-No (0) indicates that the caller does not wait for a callback after placing a call that does not connect.
- Expect-Callback-Yes (1) indicates that the caller waits 90 seconds after placing a call that does not connect before attempting to place another call to the same number.

See Also: “Ascend-Callback (246)” on page 9-14

Ascend-First-Dest (189)

Description: The Ascend-First-Dest attribute records the destination IP address of the first packet the MAX receives on a link after RADIUS authenticates the connection.

The MAX includes Ascend-First-Dest in an Accounting-Request packet when all of these conditions are true:

- The session has been authenticated.
- The session has ended (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-First-Dest does not appear in a user profile and has no default value.

Dependencies: This attribute only applies if the session routes IP.

Ascend-Force-56 (248)

Description: The Ascend-Force-56 attribute specifies whether the MAX uses only the 56-kbps portion of a channel, even when all 64 kbps appear to be available:

Usage: You can specify one of these values:

- Force-56-No

  This setting indicates that the MAX should use the entire 64 kbps (when available). Force-56-No is the default.
- Force-56-Yes

  This setting specifies that the MAX should use only the 56-kbps portion of a channel.

Set Ascend-Force-56=Force=56-Yes when you place calls to European or Pacific Rim countries from within North America and the complete path cannot distinguish between the Switched-56 and Switched-64 data services. This feature is not required if you are placing calls only within North America.

Ascend-FR-Circuit-Name (156)

Description: The Ascend-FR-Circuit-Name attribute specifies the Permanent Virtual Connection (PVC) for which the user profile is an endpoint. A circuit specification defines two DLCI endpoints of a PVC, with one endpoint specified in each RADIUS user profile or Connection profile.

Usage: Specify a text string containing up to 15 characters. The default value is null.

Dependencies: Keep this additional information in mind:

- You can specify Ascend-FR-Circuit-Name only when Framed-Protocol=FR-CIR.
- The MAX requires two profiles for a single PVC.

  You can use two RADIUS user profiles, two Connection profiles, or one RADIUS user profile and one Connection profile. The two DLCIs can use the same Frame Relay profile or different ones.
- The MAX switches pairs of links with matching Ascend-FR-Circuit-Name attributes to each other.

  Therefore, make sure that you specify the exact same name for Ascend-FR-Circuit-Name (in RADIUS) or Circuit (in a Connection profile) for the profiles that supply the endpoints of the PVC.

See Also: "Ascend-FR-Direct (219)" on page 9-43

Ascend-FR-DCE-N392 (162)

Description: The Ascend-FR-DCE-N392 attribute specifies the number of errors during Ascend-FR-DCE-N393-monitored events that cause the network side to declare the user side's procedures inactive.

Usage: Specify an integer between 1 and 10. The default value is 3.

Dependencies: Keep this additional information in mind:

- Set Ascend-FR-DCE-N392 to a value less than Ascend-FR-DCE-N393.
- Ascend-FR-DCE-N392 does not apply if Ascend-FR-Type=Ascend-FR-DTE.

See Also: "Ascend-FR-DCE-N393 (164)" on page 9-42
"Ascend-FR-Type (159)" on page 9-47

Ascend-FR-DCE-N393 (164)

Description: The Ascend-FR-DCE-N393 attribute indicates the DCE-monitored event count. The MAX always considers a link active if the value of Ascend-FR-DCE-N393 is not reached.

Usage: Specify a number between 1 and 10. The default value is 4.

Dependencies: This attribute does not apply if Ascend-FR-Type=Ascend-FR-DTE.

See Also: "Ascend-FR-Type (159)" on page 9-47

Ascend-FR-Direct (219)

Description: The Ascend-FR-Direct attribute specifies whether the MAX uses a redirect connection for Frame Relay packets.

When the MAX receives IP packets from a caller that has a redirect specified in its local Connection profile or RADIUS user profile, it simply forwards the data stream out to the Frame Relay switch using the specified DLCI, effectively passing on the responsibility of routing those packets to a later hop on the Frame Relay network. The MAX never examines the destination address of redirect packets. This feature enables you to accept traffic from one link and send all traffic to a predetermined destination, eliminating any user concerns over security.

Usage: You can specify one of these values:

- FR-Direct-No (0) indicates that the MAX does not use a redirect connection.
  FR-Direct-No is the default.
- FR-Direct-Yes (1) indicates that the MAX uses a redirect connection.

See Also: "Ascend-FR-Direct-DLCI (221)" on page 9-43
"Ascend-FR-DLCI (179)" on page 9-44

Ascend-FR-Direct-DLCI (221)

Description: The Ascend-FR-Direct-DLCI attribute specifies the Data Link Connection Indicator (DLCI) for the user profile in a Frame Relay redirect connection. The DLCI identifies the user profile to the Frame Relay switch as a logical link on a physical circuit.

Usage: Specify an integer between 16 and 991. The default value is 16. Many redirect connections can use the same DLCI.

Dependencies: Ascend-FR-Direct-DLCI applies only if Ascend-FR-Direct=FR-Direct-Yes.

Example: This portion of a user profile shows a redirect connection that uses DLCI 21 and the Frame Relay profile called Montgomery.

```
Permconn-MAX-1 Password="Ascend", User-Service=Dialout-Framed-User
    User-Name="Matt",
    Ascend-FR-Direct=FR-Direct-Yes,
    Ascend-FR-Direct-Profile="Montgomery",
    Ascend-FR-Direct-DLCI=21,
    Metric=2,
    ...
```

See Also: "Ascend-FR-Direct (219)" on page 9-43
"Ascend-FR-Direct-Profile (220)" on page 9-44

Ascend-FR-Direct-Profile (220)

Description: The Ascend-FR-Direct-Profile attribute specifies the name of the Frame Relay profile that carries the redirect connection.

Usage: Indicate the name of a Frame Relay profile that connects to the Frame Relay switch handling the Data Link Connection Indicator (DLCI) specified by Ascend-FR-Direct-DLCI. You can specify up to 15 alphanumeric characters. The default value is null. Make sure that you enter the name exactly as it appears in the Name parameter of the Frame Relay profile.

Dependencies: Ascend-FR-Direct-Profile applies only if Ascend-FR-Direct=FR-Direct-Yes.

Example: This portion of a user profile shows a redirect connection that uses DLCI 21 and the Frame Relay profile called Montgomery.

```
Permconn-MAX-1 Password="Ascend", User-Service=Dialout-Framed-User
    User-Name="Matt",
    Ascend-FR-Direct=FR-Direct-Yes,
    Ascend-FR-Direct-Profile="Montgomery",
    Ascend-FR-Direct-DLCI=21,
    Metric=2,
    ...
```

See Also: “Ascend-FR-Direct (219)” on page 9-43
“Ascend-FR-Direct-DLCI (221)” on page 9-43

Ascend-FR-DLCI (179)

Description: The Ascend-FR-DLCI attribute specifies the Data Link Connection Indicator (DLCI) for the user profile in a Frame Relay gateway connection. The DLCI identifies the user profile to the Frame Relay switch as a logical link on a physical circuit.

Usage: Specify an integer between 16 and 991. The default value is 16. You must assign each gateway connection its own DLCI.

Dependencies: Ascend-FR-DLCI applies only if Ascend-FR-Direct=FR-Direct-No.

Example: This portion of a user profile shows a gateway connection that uses DLCI 21 and the Frame Relay profile called Florence.

```
Permconn-MAX-1 Password="Ascend", User-Service=Dialout-Framed-User
    User-Name="Matt",
Ascend-FR-Direct=FR-Direct-No,
Ascend-FR-Profile-Name="Florence",
Ascend-FR-DLCI=21,
Metric=2,
...
```

See Also: “Ascend-FR-Direct (219)” on page 9-43
“Ascend-FR-Profile-Name (180)” on page 9-46

Ascend-FR-DTE-N392 (163)

Description: The Ascend-FR-DTE-N392 attribute specifies the number of errors during Ascend-FR-DTE-N393-monitored events that cause the user side to declare the network side's procedures inactive.

Usage: Specify an integer between 1 and 10. The default value is 3.

Dependencies: Keep this additional information in mind:

- Set Ascend-FR-DTE-N392 to a value less than Ascend-FR-DTE-N393.
- Ascend-FR-DTE-N392 does not apply if Ascend-FR-Type=Ascend-FR-DCE.

See Also: "Ascend-FR-DTE-N393 (165)" on page 9-45
"Ascend-FR-Type (159)" on page 9-47

Ascend-FR-DTE-N393 (165)

Description: The Ascend-FR-DTE-N393 attribute indicates the DTE-monitored event count. The MAX always considers a link active if the value of Ascend-FR-DTE-N393 is not reached.

Usage: Specify a number between 1 and 10. The default value is 4.

Dependencies: This attribute does not apply if Ascend-FR-Type=Ascend-FR-DCE.

See Also: "Ascend-FR-Type (159)" on page 9-47

Ascend-FR-Link-Mgt (160)

Description: In a Frame Relay profile, the Ascend-FR-Link Mgt attribute specifies the link management protocol in use between the MAX and the Frame Relay switch.

Usage: You can specify one of these values:

- Ascend-FR-No-Link-Mgt (0)

  This setting indicates no link management, and is the default. The MAX always considers a link active if no link management functions are performed.
- Ascend-FR-T1-617D (1)

  This setting indicates T1.617 Annex D link management.
- Ascend-FR-Q-933A (2)

  This setting indicates Q.933 Annex A link management.

Ascend-FR-LinkUp (157)

Description: In a Frame Relay profile, the Ascend-FR-LinkUp attribute specifies whether the Frame Relay link comes up automatically.

Usage: You can specify one of these values:

- Ascend-LinkUp-Default (0)

  This setting indicates that the datalink does not come up unless a DLCI brings it up, and shuts down after the last DLCI has been removed. This value is the default.
- Ascend-LinkUp-AlwaysUp (1)

This setting indicates that the datalink comes up automatically and stays up even when the last DLCI has been removed.

Dependencies: You can start and drop Frame Relay connections by using the DO DIAL and DO HANGUP commands. DO DIAL brings up a connection. DO HANGUP closes the link and any DLCIs on it. If Ascend-FR-LinkUp=Ascend-LinkUp-AlwaysUp, DO HANGUP brings the link down, but the link automatically restarts. A restart also occurs if a DLCI brings up the datalink.

Ascend-FR-N391 (161)

Description: In a Frame Relay profile, the Ascend-FR-N391 attribute specifies the interval in seconds at which the MAX requests a Full Status Report.

If you configure the Frame Relay link for link management, it regularly request updates on the status of the link. The Frame Relay unit at the other end of the link must respond to these requests. Otherwise, the MAX considers the link inactive. Furthermore, if the response to these requests indicates a DLCI failure, the MAX considers the link inactive.

Usage: Specify an integer between 1 and 255. The default value is 6.

Dependencies: This attribute does not apply if Ascend-FR-Type=Ascend-FR-DCE.

See Also: "Ascend-FR-Type (159)" on page 9-47

Ascend-FR-Nailed-Grp (158)

Description: The Ascend-FR-Nailed-Grp attribute associates a group of nailed-up channels with the Frame Relay profile.

Usage: Specify a number between 1 and the maximum number of nailed-up channels that your MAX allows. The default value is 1.

Dependencies: Do not associate a group with more than one active Frame Relay profile.

Ascend-FR-Profile-Name (180)

Description: The Ascend-FR-Profile-Name attribute specifies the name of the Frame Relay profile that carries the gateway connection.

Usage: Indicate the name of a Frame Relay profile that connects to the Frame Relay switch handling the Data Link Connection Indicator (DLCI) specified by Ascend-FR-DLCI. You can specify up to 15 alphanumeric characters. The default value is null. Make sure that you enter the name exactly as it appears in the Name parameter of the Frame Relay profile.

Dependencies: Ascend-FR-Profile-Name applies only if Ascend-FR-Direct=FR-Direct-No.

Example: This portion of a user profile shows a gateway connection that uses DLCI 21 and the Frame Relay profile called Florence.

```
Permconn-MAX-1 Password="Ascend", User-Service=Dialout-Framed-User
    User-Name="Matt",
    Ascend-FR-Direct=FR-Direct-No,
    Ascend-FR-Profile-Name="Florence",
    Ascend-FR-DLCI=21,
    Metric=2,
    ...
```

See Also: “Ascend-FR-Direct (219)” on page 9-43
“Ascend-FR-DLCI (179)” on page 9-44

Ascend-FR-T391 (166)

Description: The Ascend-FR-T391 attribute indicates the Link Integrity Verification polling timer.

Usage: You can specify a number of seconds between 5 and 30. The default value is 10.

Dependencies: This attribute does not apply if Ascend-FR-Type=Ascend-FR-DCE.

See Also: “Ascend-FR-Type (159)” on page 9-47

Ascend-FR-T392 (167)

Description: The Ascend-FR-T392 attribute indicates the timer for the verification of the polling cycle— the length of time the unit should wait between Status Enquiry messages. The MAX records an error if it does not receive a Status Enquiry within the number seconds this attribute specifies.

Usage: Specify a number of seconds between 5 and 30. The default value is 10.

Dependencies: This attribute does not apply if Ascend-FR-Type=Ascend-FR-DTE.

See Also: “Ascend-FR-Type (159)” on page 9-47

Ascend-FR-Type (159)

Description: The Ascend-FR-Type attribute specifies the type of Frame Relay connection the Frame Relay profile uses.

Usage: You can specify one of these values:

- Ascend-FR-DTE (0)

  This setting indicates a UNI-DTE interface (the default). When you specify this value, the MAX acts as a DTE that can connect to a Frame Relay switch.
- Ascend-FR-DCE (1)

  This setting indicates a UNI-DCE interface. When you specify this value, the MAX acts as a DCE that can connect to a Frame Relay DTE unit—that is, to the user’s Customer Premises Equipment (CPE).
- Ascend-FR-NNI (2)

  This setting indicates an NNI interface. When you specify this value, the MAX can connect to another NNI unit (a Frame Relay switch).

Ascend-FT1-Caller (175)

Description: The Ascend-FT1-Caller attribute specifies whether the MAX initiates an FT1-AIM or an FT1-B&O call, or whether it waits for the remote end to initiate these types of calls.

Usage: You can specify one of these values:

- FT1-No (0) specifies that the MAX waits for the remote end to initiate the call.

  FT1-No is the default.
- FT1-Yes (1) specifies that the MAX initiates the call.

  If you choose this setting, the MAX dials to bring online any switched circuits that are part of the call.

Dependencies: Keep this additional information in mind:

- If the remote end has set Ascend-FT1-Caller=FT1-No in a RADIUS user profile (or FT1 Caller=No in a Connection profile), set Ascend-FT1-Caller=FT1-Yes for the local MAX.
- If the remote end has set Ascend-FT1-Caller=FT1-Yes in a RADIUS user profile (or FT1 Caller=Yes in a Connection profile), set Ascend-FT1-Caller=FT1-No for the local MAX.

Ascend-Group (178)

Description: The Ascend-Group attribute points to the nailed-up channels the profile’s WAN link uses.

If you set the Ascend-Group attribute to a value that matches the settings of a Ch *n* Prt/Grp, B1 Prt/Grp, or B2 Prt/Grp parameter in a Line profile, the MAX uses the specified channels for this profile’s link across the WAN. Similarly, if Ascend-Group has the same value as Nailed Grp in the Serial WAN profile, the MAX uses the serial WAN circuit for this profile’s link.

Usage: Your usage depends upon the value you specify for the Ascend-Call-Type attribute:

- If you set Ascend-Call-Type=Nailed, you can specify a number between 1 and 60 for Ascend-Group.

  The default value is 1.
- If you set Ascend-Call-Type=Nailed/Mpp, you can use the Ascend-Group attribute to assign multiple nailed-up groups to the profile.

  Specify a single number, or specify a list of numbers between 1 and 60, separated by commas. Do not include spaces. The default value is 1.

Dependencies: Keep this additional information in mind:

- The Ascend-Group attribute does not apply if the link consists entirely of switched channels.
- If you add channels for the Ascend-Group attribute, the MAX adds the additional channels to any online connection that uses the group.
- Do not duplicate group numbers in active profiles—that is, choose a value for Ascend-Group that no active Connection profile, Call profile, Frame Relay profile, or RADIUS user profile is using.
- Although you can assign multiple groups to a user profile, do not mix the Serial WAN circuit with nailed-up BRI or T1/E1 channels.

Example: If Ascend-Call-Type=Nailed/Mpp, setting the Ascend-Group attribute to “1,3,5,7” assigns four nailed-up groups to the profile.

Ascend-Handle-IPX (222)

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

Usage: You can specify one of these values:

- Handle-IPX-None (0)

  This setting indicates that special IPX behavior does not take place. Choose this setting when the LAN on each side of the bridge has one or more IPX servers.

  Handle-IPX-None is the default.

- Handle-IPX-Client (1)

  This setting indicates that the MAX discards Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) periodic broadcasts at its WAN interface, but forwards RIP and SAP queries.

  The WAN interface is the port on the MAX that connects to a WAN line. RIP and SAP queries enable a client workstation to locate a NetWare server across the network. Choose Handle-IPX-Client when both these conditions are true:

  - The local LAN has IPX clients but no servers.
  - The MAX is acting as a bridge to another LAN containing only IPX servers, or a combination of IPX servers and clients.

- Handle-IPX-Server (2)

  This setting indicates that the MAX discards all Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) periodic broadcasts and queries at its WAN interface.

  This mode enables the MAX to bring down calls during idle periods without breaking client/server or peer-to-peer connections.

  Ordinarily, when a NetWare server does not receive a reply to the watchdog session keepalive packets it sends to a client, it closes the connection. When you specify Handle-IPX-Server, however, the MAX replies to NCP watchdog requests on behalf of clients on the other side of the bridge. In other words, the MAX tricks the server watchdog process into believing that the link is still active. This process is called watchdog spoofing.

  Choose this setting when both these conditions are true:

  - The MAX is acting as a bridge to a remote LAN with IPX clients, but no servers.
  - The local LAN contains only IPX servers, or a combination of IPX clients and servers.

Dependencies: Keep this additional information in mind:

- If you specify Ascend-Handle-IPX=Handle-IPX-Server, you must also specify a value for the Ascend-Netware-timeout attribute, indicating the maximum length of idle time during which the MAX performs watchdog spoofing for NetWare connections.
- If the connection does not bridge (Ascend-Bridge=Bridge-No), the Ascend-Handle-IPX attribute does not apply.
- If the MAX on one LAN sets Ascend-Handle-IPX=Handle-IPX-Server, and the LAN on the other side of the connection has only NetWare clients, the MAX on the client-only LAN should set Ascend-Handle IPX=Handle-IPX-Client.

If both LANs contain servers, both sides of the connection should set Ascend-Handle-IPX=Handle-IPX-None.

- Although Ascend-Handle-IPX does not apply if Ascend-Bridge=Bridge-No, the MAX automatically performs watchdog spoofing just as though you had set Ascend-Handle-IPX=Handle-IPX-Server.

  However, the MAX does not filter as though you had set Ascend-Handle-IPX=Handle-IPX-Server.

Example: This user profile specifies an IPX bridging link in which the local Ethernet supports NetWare clients, and the remote network supports both NetWare servers and clients:

```
MAX1 Password="m2dan", User-Service=Framed-User

    Framed-Protocol=PPP,

    Ascend-Route-IPX=Route-IPX-No,

    Ascend-Bridge=Bridge-Yes,
        Ascend-Handle-IPX=Handle-IPX-Client,

    Ascend-Netware-timeout=30
```

See Also: “Ascend-Bridge (230)” on page 9-12
“Ascend-Netware-timeout (223)” on page 9-68

Ascend-History-Weigh-Type (239)

Description: The Ascend-History-Weigh-Type attribute specifies which Dynamic Bandwidth Allocation (DBA) algorithm to use for calculating average line utilization (ALU) of transmitted data. DBA enables you to specify that the MAX uses ALU as the basis for automatically adding or subtracting bandwidth from a switched connection without terminating the link.

Usage: Figure 9-1 illustrates the differences among the algorithms you can choose.

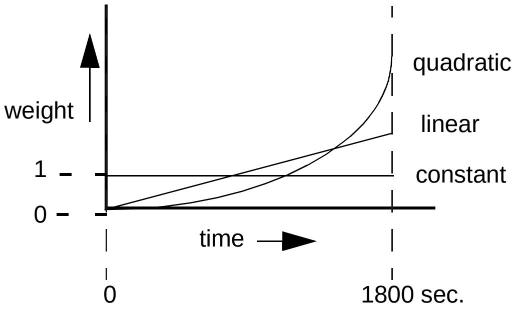

Figure 9-1. Bandwidth algorithms for MP+ calls

- History-Constant (0) gives equal weight to all samples taken during the historical time period specified by Ascend-Seconds-Of History.

  When you select this option, older historical samples have as much impact on the decision to change bandwidth allocation as more recent samples.

- History-Linear (1) gives more weight to recent samples of bandwidth usage than to older samples taken during the historical period specified by Ascend-Seconds-Of-History.

  The weighting grows at a linear rate.
- History-Quadratic (2) gives more weight to recent samples of bandwidth usage than to older samples taken during the historical period specified by Ascend-Seconds-Of-History.

  The weighting grows at a quadratic rate. History-Quadratic is the default.

See Also: "Ascend-Add-Seconds (240)" on page 9-4
"Ascend-Base-Channel-Count (172)" on page 9-10
"Ascend-DBA-Monitor (171)" on page 9-33
"Ascend-Dec-Channel-Count (237)" on page 9-34
"Ascend-Inc-Channel-Count (236)" on page 9-55
"Ascend-Maximum-Channels (235)" on page 9-61
"Ascend-Minimum-Channels (173)" on page 9-65
"Ascend-Remove-Seconds (241)" on page 9-78
"Ascend-Seconds-Of-History (238)" on page 9-81
"Ascend-Target-Util (234)" on page 9-84

Ascend-Home-Agent-IP-Addr

Description: Indicates the IP address of the home agent used for this mobile ATMP client in a RADIUS Stop record.

Example: The following is an example of a RADIUS accounting STOP record that includes the Ascend-Home-Agent-IP-Addr attribute:

```
Mon Apr 21 02:41:38 1997

User-Name = "JacobP75"
NAS-Identifier = 1.1.1.1
NAS-Port = 10105
Acct-Status-Type = Stop
Acct-Delay-Time = 0
Acct-Session-Id = "111111111"
Acct-Authentic = RADIUS
Acct-Session-Time = 0
Acct-Input-Octets = 215
Acct-Output-Octets = 208
Acct-Input-Packets = 10
Acct-Output-Packets = 10
Ascend-Disconnect-Cause = 1
Ascend-Connect-Progress = 60
Ascend-Data-Rate = 56000
Ascend-PreSession-Time = 1
Ascend-Pre-Input-Octets = 215
Ascend-Pre-Output-Octets = 208
Ascend-Pre-Input-Packets = 10
Ascend-Pre-Output-Packets = 10
Framed-Protocol = PPP
Framed-Address = 2.2.2.2
Tunneling-Protocol = ATMP
Ascend-Home-Agent-IP-Addr = 3.3.3.3
```

```
Ascend-Home-Agent-UDP-Port = 5150
Ascend-Home-Network-Name = homenet
```

Dependencies: Accounting-Request packets, generated by the foreign agent, send the Ascend-Home-Agent-IP-Addr attribute at the end of a session, under the following conditions:

- The Accounting-Request packet includes Acct-Status-Type=Stop.
- The session was authenticated and encapsulated by means of Ascend Tunnel Management Protocol (ATMP).

Ascend-Home-Agent-Password (184)

Description: In a mobile node’s RADIUS user profile, the Ascend-Home-Agent-Password attribute specifies the password that the foreign agent sends to the home agent in order to authenticate itself during Ascend Tunnel Management Protocol (ATMP) operation. This password must match the value of the Password parameter in Ethernet>Mod Config>ATMP Options menu for the home agent. All mobile nodes accessing a single home agent must specify the same password.

The RADIUS server passes the attributes in the mobile node’s RADIUS user profile to the foreign agent. The foreign agent sends these attributes when connecting with the home agent.

A mobile node can also connect directly to the home agent. An ATMP-based RADIUS profile that is local to the home agent enables the mobile node to bypass a foreign agent connection, but does not preclude a foreign agent. If both the home agent and the foreign agent have local RADIUS profiles for the mobile node, the node can choose between a direct connection or a tunneled connection through the foreign agent.

Usage: Specify a text string containing up to 20 characters. The default value is null.

Example: The following RADIUS profile authenticates a mobile NetWare client that connects directly to the home agent. In this example, the home agent is in gateway mode. It forwards packets from the mobile node across a nailed-up WAN link to the home IPX network.

```
Mobile-IPX Password="unit"
     User-Service=Framed-User,
     Ascend-Route-IPX=Route-IPX-Yes,
     Framed-Protocol=PPP,
     Ascend-IPX-Peer-Mode=IPX-Peer-Dialin,
     Framed-IPX-Network=40000000,
     Ascend-IPX-Node-Addr=12345678,
     Ascend-Primary-Home-Agent="max1.home.com:6001",
     Ascend-Secondary-Home-Agent="max2.home.com:6001",
     Ascend-Home-Network-Name="Dave’s MAX",
     Ascend-Home-Agent-Password="Pipeline"
```

See Also: “Ascend-Home-Agent-UDP-Port (186)” on page 9-53
“Ascend-Home-Network-Name (185)” on page 9-53
“Ascend-Primary-Home-Agent (129)” on page 9-73
“Ascend-Secondary-Home-Agent (130)” on page 9-80

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

Description: In a mobile node's RADIUS user profile, the Ascend-Home-Agent-UDP-Port attribute specifies the UDP port number on the home agent to which the foreign agent directs Ascend Tunnel Management Protocol (ATMP) messages.

Usage: Specify a UDP port number between 0 and 65535. The default value is 5150.

Dependencies: If you specify a value for the ***udp_port*** argument of Ascend-Primary-Home-Agent or Ascend-Secondary-Home-Agent, or if you accept the default of 5150 for ***udp_port***, you need not specify the Ascend-Home-Agent-UDP-Port attribute.

See Also: "Ascend-Home-Agent-Password (184)" on page 9-52
"Ascend-Home-Network-Name (185)" on page 9-53
"Ascend-Primary-Home-Agent (129)" on page 9-73
"Ascend-Secondary-Home-Agent (130)" on page 9-80

Ascend-Home-Network-Name (185)

Description: In a mobile node's RADIUS user profile, the Ascend-Home-Network-Name attribute specifies the name of the Connection profile on which the home agent sends all packets it receives from the mobile node during Ascend Tunnel Management Protocol (ATMP) operation.

The RADIUS server passes the attributes in the mobile node's RADIUS user profile to the foreign agent. The foreign agent sends these attributes when connecting with the home agent.

A mobile node can also connect directly to the home agent. An ATMP-based RADIUS profile that is local to the home agent enables the mobile node to bypass a foreign agent connection, but does not preclude a foreign agent. If both the home agent and the foreign agent have local RADIUS profiles for the mobile node, the node can choose between a direct connection or a tunneled connection through the foreign agent.

Usage: Specify the name of the home agent's Connection profile. The default value is null.

Dependencies: You must specify a value for this attribute only if the home agent is a gateway (that is, only if Type=Gateway in the Ethernet>Mod Config>ATMP Options menu).

Example: The following RADIUS profile authenticates a mobile NetWare client that connects directly to the home agent. In this example, the home agent is in gateway mode. It forwards packets from the mobile node across a nailed-up WAN link to the home IPX network.

```
Mobile-IPX Password="unit"
     User-Service=Framed-User,
     Ascend-Route-IPX=Route-IPX-Yes,
     Framed-Protocol=PPP,
     Ascend-IPX-Peer-Mode=IPX-Peer-Dialin,
     Framed-IPX-Network=40000000,
     Ascend-IPX-Node-Addr=12345678,
     Ascend-Primary-Home-Agent="max1.home.com:6001",
     Ascend-Secondary-Home-Agent="max2.home.com:6001",
     Ascend-Home-Network-Name="Dave’s MAX",
     Ascend-Home-Agent-Password="Pipeline"
```

See Also: “Ascend-Home-Agent-Password (184)” on page 9-52
“Ascend-Home-Agent-UDP-Port (186)” on page 9-53
“Ascend-Primary-Home-Agent (129)” on page 9-73
“Ascend-Secondary-Home-Agent (130)” on page 9-80

Ascend-Host-Info (252)

Description: The Ascend-Host-Info attribute specifies a list of hosts to which a user can establish a Telnet session.

Usage: You can specify up to 10 Ascend-Host-Info entries in a user profile. Enter your attribute settings in this format:

`Ascend-Host-Info="`*`IP_address text`***`"`**

- ***`IP_address`*** specifies the IP address of each host.

  Specify an IP address in dotted decimal notation. An IP address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0.

- ***`text`*** describes each host.

  You can enter up to 31 characters for ***`text`***. The default value is null. The RADIUS server assigns the text a number. When the user selects the number, the terminal server initiates a Telnet session with the host at the specified IP address.

Dependencies: If you specify a value for the Ascend-Host-Info attribute, you must also make these settings in the Ethernet>Mod Config>TServ Options menu:

- Set Initial Scrn=Menu or Toggle Scrn=Yes.
- Set Remote Conf=Yes.

Example: Here is an example for a MAX named Cal:

```
Initial-Banner-Cal Password="Ascend", User-Service=Dialout-Framed-User
     Reply-Message="Up to 16 lines of up to 80 characters each",
     Reply-Message="will be accepted. Long lines will be
truncated",
     Reply-Message="Additional lines will be ignored.",
     Reply-Message="",

  Ascend-Host-Info="1.2.3.4 Berkeley",

  Ascend-Host-Info="1.2.3.5 Alameda",

  Ascend-Host-Info="1.2.36 San Francisco",

  ...
```

See Also: “Reply-Message (18)” on page 9-105

Ascend-Idle-Limit (244)

Description: The Ascend-Idle-Limit attribute specifies the number of seconds the MAX waits before clearing a call when a session is inactive.

Usage: Specify a number between 0 and 65535. If you specify 0 (zero), the MAX always clears a call when a session is inactive. The default value is 120 seconds. If you accept the default and an existing Answer profile specifies a value for the analogous Idle parameter, the MAX ignores the Idle value and uses the Ascend-Idle-Limit default.

Dependencies: Keep this additional information in mind:

- If the time set by the Ascend-Idle-Limit expires, the call disconnects whether or not bandwidth utilization falls below the Ascend-MPP-Idle-Percent setting.
- When bandwidth utilization falls below the Ascend-MPP-Idle-Percent setting, the call disconnects regardless of whether the time specified by the Ascend-Idle-Limit attribute has expired.
- Because the Ascend-MPP-Idle-Percent attribute is dependent on traffic levels on both sides of the connection, we recommend that you use the Ascend-Idle-Limit attribute in preference to it.
- The Ascend-Idle-Limit attribute does not apply to nailed-up links.

See Also: "Ascend-MPP-Idle-Percent (254)" on page 9-66
"Ascend-Preempt-Limit (245)" on page 9-72

Ascend-IF-Netmask (154)

Description: The Ascend-IF-Netmask attribute specifies the subnet mask in use for the local numbered interface.

Usage: Specify a subnet mask consisting of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0.

Ascend-Inc-Channel-Count (236)

Description: The Ascend-Inc-Channel-Count attribute specifies the number of channels the MAX adds when bandwidth changes either manually or automatically during a call.

Usage: Specify a number between 1 and 32. The default value is 1.

Dependencies: Keep this additional information in mind:

- Ascend-Inc-Channel-Count does not apply if all channels of a link are nailed up (Ascend-Call-Type=Nailed).
- Ascend-Inc-Channel-Count applies only if the link is using MP+ encapsulation (Framed-Protocol=MPP).
- MP+ calls cannot exceed 32 channels.
- The sum of Ascend-Base-Channel-Count and Ascend-Inc-Channel-Count cannot exceed the maximum number of channels available.

See Also: "Ascend-Add-Seconds (240)" on page 9-4
"Ascend-Base-Channel-Count (172)" on page 9-10

“Ascend-DBA-Monitor (171)” on page 9-33
“Ascend-Dec-Channel-Count (237)” on page 9-34
“Ascend-History-Weigh-Type (239)” on page 9-50
“Ascend-Maximum-Channels (235)” on page 9-61
“Ascend-Minimum-Channels (173)” on page 9-65
“Ascend-Remove-Seconds (241)” on page 9-78
“Ascend-Seconds-Of-History (238)” on page 9-81
“Ascend-Target-Util (234)” on page 9-84

Ascend-IP-Direct (209)

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

Usage: Specify an IP address in dotted decimal notation. An IP address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0. If you accept the default, the MAX does not redirect IP traffic.

Dependencies: Keep this additional information in mind:

- You can specify the Ascend-IP-Direct attribute only under these conditions:
  - IP routing is in use.
  - The user profile contains the specification Ascend-Bridge=Bridge-No.
  - Framed-Protocol is not set to COMB or FR.
- Do not set Ascend-IP-Direct and Ascend-FR-Direct in the same user profile.

  If you do, an error occurs.
- Ascend-IP-Direct connections typically turn off RIP.

  If you configure the connection to receive RIP, the MAX keeps all RIP packets from the remote end and forwards them to the IP address you specify. To turn off RIP, set Framed-Routing=None.

Example: This user profile specifies that the MAX redirects incoming packets to the host at IP address 10.2.3.11:

```
Emma Password="m2dan", User-Service=Framed-User
     Framed-Protocol=PPP,
     Framed-Address=10.8.9.10,

  Framed-Netmask=255.255.252.0,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Bridge=Bridge-No,
     Ascend-IP-Direct=10.2.3.11,
     Ascend-Metric=2,
     Framed-Routing=None,
     ...
```

See Also: "Framed-Routing (10)" on page 9-100

Ascend-IP-Pool-Definition (217)

Description: The Ascend-IP-Pool-Definition attribute specifies the first IP address in a MAX-specific IP address pool, and indicates the number of addresses in the pool.

Usage: The Ascend-IP-Pool-Definition attribute has this format:

```
Ascend-IP-Pool-Definition="num first_ipaddr max_entries"
```

Table 9-13 describes each Ascend-IP-Pool-Definition argument.

Table 9-13.Ascend-IP-Pool-Definition arguments

Argument	Description
num	Indicates the number of the pool. The default value is 1. Specify pool numbers starting with 1, unless you have defined pools in the MAX interface using the Pool #*n* Start and Pool #*n* Count parameters and do not wish to override these settings. In this case, for the ***num*** argument, specify the highest number of an address pool on the MAX + 1. For example, if you have set up address pools 1 through 5 on the MAX, specify pool numbers starting with 6 in RADIUS.
first_ipaddr	Specifies the first IP address in the address pool. The address you indicate should not accept a subnet mask, because it always becomes a host route. The default value is 0.0.0.0.
max_entries	Specifies the maximum number of IP addresses in the pool. The MAX assigns addresses sequentially, from ***first_ipaddr*** on, up to the limit of addresses specified by ***max_entries***. The default value is 0 (zero).

Dependencies: You specify one or more Ascend-IP-Pool-Definition attributes in a pseudo-user profile. You create a pseudo-user to store information that the MAX can query—in this case, in order to store IP address pool information. Specify the first line of a pseudo-user profile in this format:

```
Pools-unit_name Password="Ascend", User-Service=Dialout-Framed-User
```

unit_name is the system name of the MAX—that is, the name specified by the Name parameter in the System profile. On the next lines of the profile, specify one or more Ascend-IP-Pool-Definition attributes.

Example: In this example, the pseudo-user profile creates two IP address pools for the MAX to use. Address pool #1 contains a block of 7 IP addresses from 10.1.0.1 to 10.1.0.7. Address pool #2 contains a block of 48 IP addresses from 10.2.0.1 to 10.2.0.48.

```
Pools-MAX Password="Ascend", User-Service=Dialout-Framed-User
    Ascend-IP-Pool-Definition="1 10.1.0.1 7",
    Ascend-IP-Pool-Definition="2 10.2.0.1 48"
```

See Also: "Ascend-Assign-IP-Pool (218)" on page 9-8

Ascend-IPX-Alias (224)

Description: The Ascend-IPX-Alias attribute specifies an IPX network number to use when connecting to IPX routers that require numbered interfaces.

Usage: Specify an IPX network number. The default value is 0 (zero). RADIUS requires that this attribute have a decimal value (base 10), but IPX network numbers generally have hexadecimal values (base 16). In order to give this attribute a value, you must convert the hexadecimal IPX network number to a decimal value for use in the user profile.

See Also: "Ascend-IPX-Peer-Mode (216)" on page 9-58
"Ascend-IPX-Route (174)" on page 9-59
"Ascend-Route-IPX (229)" on page 9-80

Ascend-IPX-Node-Addr (182)

Description: The Ascend-IPX-Node-Addr attribute specifies a unique IPX node address on the network specified by Framed-IPX-Network. This value completes the IPX address of a mobile node.

Usage: Specify a 12-digit ASCII string enclosed in double-quotes. The RADIUS server passes the attributes in the mobile node's profile to the foreign agent. The foreign agent sends these attributes when connecting with the home agent.

See Also: "Framed-IPX-Network (23)" on page 9-94

Ascend-IPX-Peer-Mode (216)

Description: The Ascend-IPX-Peer-Mode attribute specifies whether the caller is a dial-in PPP client or an Ethernet client with its own IPX network address.

Dial-in clients do not belong to an IPX network, so you must assign them an IPX network number. When you do so, a dial-in client can establish a routing connection with the MAX. To provide an IPX network number, you must define a virtual IPX network using the IPX Pool# parameter in the MAX configuration interface. The MAX advertises the route to this virtual network and assigns it as the network address for dial-in clients.

Usage: For the Ascend-IPX-Peer-Mode attribute, you can specify one of these values:

- IPX-Peer-Router (0) indicates that the caller is on the Ethernet network and has its own IPX address.

  IPX-Peer-Router is the default.
- IPX-Peer-Dialin (1) indicates that the caller is a dial-in NetWare client that incorporates PPP software and dial-out hardware, but does not have an Ethernet interface.

  This setting causes the MAX to assign the caller an IPX address derived from the value of IPX Pool#. If the client does not supply its own unique node number, the MAX assigns a unique node number to the client as well. The MAX does not send IPX RIP and SAP advertisements across the connection, and ignores IPX RIP and SAP advertisements it receives from the remote end. However, it does respond to IPX RIP and SAP queries it receives from dial-in clients.

See Also: “Ascend-IPX-Route (174)” on page 9-59
“Ascend-Route-IPX (229)” on page 9-80

Ascend-IPX-Route (174)

Description: The Ascend-IPX-Route attribute enables you to configure a static IPX route.

Usage: To configure a static IPX route to an internal network, use the following format:

```
Ascend-IPX-Route="profile_name network# [node#] [socket#]
[server_type] [hop_count] [tick_count] [server_name]"
```

Table 9-14 describes each Ascend-IPX-Route argument.

Table 9-14.Ascend-IPX-Route arguments

Argument	Description
profile_name	Specifies the RADIUS user profile used to reach the network. The default value is null.
network#	Indicates the unique internal network number of the NetWare server. The default value is 00000000.
node#	Specifies the node number of the NetWare server. The default value is 000000000001—the typical node number for a NetWare file server.
socket#	Indicates the socket number of the NetWare server. Typically, NetWare file servers use socket 0451. The default value is 0000. The number you specify must be a well-known socket number. Services that use dynamic socket numbers may use a different socket each time they load. To bring up a connection to a remote service that uses a dynamic socket number, specify a master server that uses a well-known socket number.
server_type	Specifies the SAP service type of the NetWare server. NetWare file servers have SAP service type 0004. The default value is 0000.
hop_count	Indicates the distance to the destination network in hops. The default value is 1.
tick_count	Specifies the distance to the destination network in IBM PC clock ticks (one-eighteenth of a second). This value is for round-trip timer calculation and for determining the nearest server of a given type.The default value is 12.
server_name	Indicates the name of an IPX server. The default value is null.

When you define a static route to an external network, the Ascend-IPX-Route attribute has the following format:

```
Ascend-IPX-Route="route-only [network #] [transit_network #]"
```

Table 9-15 describes each Ascend-IPX-Route argument.

Table 9-15.Ascend-IPX-Route arguments

Argument	Description
network #	Indicates the unique external network number. The default value is 00000000.
transit_network #	Indicates an intermediate network: • Between the MAX and the destination network. • To which the MAX knows how to route.

Dependencies: Each static route must appear in a pseudo-user profile. You create a pseudo-user to store information that the MAX can query—in this case, in order to store IPX routing information. You can configure pseudo-users for both global and MAX-specific configuration control of IPX dialout routes. The MAX loads the unit-specific dialout routes in addition to the global dialout routes.

For a unit-specific IPX dialout route, specify the first line of a pseudo-user profile in this format:

```
IPXRoute-unit_name-num Password="Ascend", User-Service=Dialout-Framed-
User
```

For a global IPX dialout route, specify the first line of a pseudo-user profile in this format:

```
IPXRoute-num Password="Ascend", User-Service=Dialout-Framed-User
```

unit_name is the system name of the MAX—that is, the name specified by the Name parameter in the System profile. ***num*** is a number in a sequential series, starting at 1.

In each pseudo-user profile, you can specify one or more routes using the Ascend-IPX-Route attribute. Limit each pseudo-user profile to about 25 routes. The MAX fetches information from each pseudo-user profile in order to gather routing information. Whenever you power on or reset the MAX, or when you select the Upd Rem Cfg command from the Sys Diag menu, RADIUS adds IPX dialout routes to the routing table in this way:

1. RADIUS looks for profiles having the format IPXRoute-***unit_name***-1, where ***unit_name*** is the system name.
2. If at least one profile exists, RADIUS loads all existing profiles having the format IPXRoute-***unit_name***-***num*** to initialize the IPX routing table.

   The variable ***num*** is a number in a sequential series, starting with 1.
3. The MAX queries IPXRoute-***unit_name***-1, then IPXRoute-***unit_name***-2, and so on, until it receives an authentication reject from RADIUS.
4. RADIUS loads the global configuration profiles.

   These configurations have the form IPXRoute-***num***.
5. The MAX queries IPXRoute-1, then IPXRoute-2, and so on, until it receives an authentication reject from RADIUS.

Example: This example defines a unit-specific IPX route:

```
IPXRoute-CA-1 Password="Ascend", User-Service=Dialout-Framed-User
```

```
        Ascend-IPX-Route="def 6 7 8 9 10"
```

This example defines a global IPX route:

```
IPXRoute-1 Password="Ascend", User-Service=Dialout-Framed-User
        Ascend-IPX-Route="abc 1 2 3 4 5 "
```

See Also: “Ascend-IPX-Alias (224)” on page 9-58
“Ascend-IPX-Peer-Mode (216)” on page 9-58
“Ascend-Route-IPX (229)” on page 9-80

Ascend-Link-Compression (233)

Description: The Ascend-Link-Compression attribute turns data compression on or off for a PPP link.

Usage: You can specify one of these values:

- Link-Comp-None (0) disables data compression.

  Link-Comp-None in the default.
- Link-Comp-Stac (1) enables Ascend’s modified version of the STACKER LZS compression/decompression algorithm.
- Link-Comp-Stac-Draft-9 (2) enables STACKER LZS compression/decompression algorithm, as specified in draft 9 of the IETF draft “PPP Stac LZS Compression Protocol”.
- Link-Comp-MS-Stac (3) enables Microsoft’s modified version of the STACKER LZS compression/decompression algorithm.

Dependencies: Both sides of the link must set either the Ascend-Link-Compression attribute or the Link Comp parameter to turn on data compression.

See Also: “Framed-Compression (13)” on page 9-94

Ascend-Maximum-Call-Duration (125)

Description: The Ascend-Maximum-Call-Duration attribute specifies the maximum number of minutes an incoming call can remain connected.

Usage: You can specify an integer between 0 and 1440. The MAX checks the connection once per minute, so the actual time the call is connected is slightly longer than the actual time you set.

The default value is 0 (zero). If you accept the default, the MAX does not set a limit on the duration of an incoming call.

Ascend-Maximum-Channels (235)

Description: The Ascend-Maximum-Channels attribute specifies the maximum number of channels the MAX allows on an MP+ call.

Usage: Specify an integer between 1 and the maximum number of channels your system supports. The default value is 1.

Dependencies: This attribute applies only to MP+ calls.

For optimum MP+ performance, both sides of a connection must set these values to the same number:

- The base channel count, as specified by Base Ch Count (in the Connection profile) or Ascend-Base-Channel-Count (in RADIUS)
- The minimum channel count, as specified by Min Ch Count (in the Answer profile or Connection profile) or Ascend-Minimum-Channels (in RADIUS)
- The maximum channel count, as specified by Max Ch Count (in the Answer profile or Connection profile) or Ascend-Maximum-Channels (in RADIUS)

See Also: "Ascend-Add-Seconds (240)" on page 9-4
"Ascend-Base-Channel-Count (172)" on page 9-10
"Ascend-DBA-Monitor (171)" on page 9-33
"Ascend-Dec-Channel-Count (237)" on page 9-34
"Ascend-History-Weigh-Type (239)" on page 9-50
"Ascend-Inc-Channel-Count (236)" on page 9-55
"Ascend-Minimum-Channels (173)" on page 9-65
"Ascend-Remove-Seconds (241)" on page 9-78
"Ascend-Seconds-Of-History (238)" on page 9-81
"Ascend-Target-Util (234)" on page 9-84

Ascend-Maximum-Time (194)

Description: The Ascend-Maximum-Time attribute specifies the maximum length of time in seconds that any session is allowed. Once a session reaches the time limit, its connection is taken offline.

Usage: Specify an integer between 0 and 4,294,967,295. The default value is 0 (zero). When you accept the default, the MAX does not enforce a time limit.

Ascend-Menu-Item (206)

Description: The Ascend-Menu-Item attribute defines a single terminal server 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 a profile to give the terminal server user a custom menu of items from which to choose. The server uses the custom menu to present the user with a subset of terminal server commands. The user does not have access to the regular menu or to the terminal server command line.

Usage: Enter your specifications using this format:

`Ascend-Menu Item=`*`command`***`;`***`text`***`;`***`match`*

- ***`command`*** is the string that the MAX sends to the terminal server when the user selects the menu item.
- ***`text`*** is the text that displays to the user.
- ***`match`*** is the pattern the user must type to select the item.
- The first semi-colon (;) that appears acts as the delimiter between ***`command`*** and ***`text`***.

- The second semi-colon that appears acts as the delimiter between ***text*** and ***match***.

By default, the MAX uses the standard terminal server menu.

Example: Suppose you set these attributes:

```
Emma Password="m2dan", 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:
```

Now, suppose you also enter specifications for the ***match*** option, as in this profile:

```
Emma Password="m2dan", User-Service=Login-User
  Ascend-Menu-Item="show ip stats;ip=Display ip stats;ip",
  Ascend-Menu-Item="ping 1.2.3.4;p=Ping server. Ctrl-C stops ping;p",
  Ascend-Menu-Item="telnet 10.2.4.5;t=Telnet to Ken’s machine;t",
  Ascend-Menu-Item="show arp;dsp=Display arp table;dsp ",
   Ascend-Menu-Selector="               Option:",
   ...
```

The terminal server displays this text:

```
ip=Display ip stats         p=Ping server. Ctrl-C stops ping
t=Telnet to Ken’s machine   dsp=Display arp table
               Option:
```

Note that you cannot combine numeric menu selections with pattern matching. This example shows what you should not do:

```
Emma Password="m2dan", User-Service=Login-User
  Ascend-Menu-Item="show ip stats;ip=Display ip stats",
  Ascend-Menu-Item="ping 1.2.3.4;p=Ping server. Ctrl-C stops ping;p",
  Ascend-Menu-Item="telnet 10.2.4.5;t=Telnet to Ken’s machine;t",
  Ascend-Menu-Item="show arp;dsp=Display arp table;dsp ",
 Ascend-Menu-Selector="            Option:",
 ...
```

If you mix numbered selections and pattern matching, as in this example, the terminal server screen displays the following text:

```
1. ip=Display ip stats            3. t=Telnet to Ken's machine
2. p=Ping server. Ctrl-C stops ping  4. dsp=Display arp table
          Option:
```

See Also: "Ascend-Menu-Selector (205)" on page 9-64

Ascend-Menu-Selector (205)

Description: The Ascend-Menu-Selector attribute specifies a string as a prompt for user input in the terminal server menu interface.

By default, when you create a custom menu with the Ascend-Menu-Item attribute, the terminal server displays this string when prompting the user to make a selection:

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

The *num* argument represents the last number in the list. The terminal server code automatically determines the value of *num* by determining the number of items in the menu. The only valid user input is in the range 1 through *num*, and q to quit.

However, you can specify a different string for prompting the user to make a selection. The Ascend-Menu-Selector attribute enables you to specify a string that the terminal server displays when prompting a user for a menu selection. If you define this attribute, its value overrides the default of `Enter Selection (1-num, q)`.

Usage: Specify a text string containing up to 31 characters. The terminal server displays this string when prompting the user for a menu selection.

Example: Suppose you set these attributes:

```
Emma Password="m2dan", 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.

See Also: "Ascend-Menu-Item (206)" on page 9-62

Ascend-Metric (225)

Description: The Ascend-Metric attribute enables you to specify the virtual hop count of an IP route.

If there are two routes available to a single destination network, you can ensure that the MAX uses any available nailed-up channel before using a switched channel. Simply set the Ascend-Metric attribute to a value higher than the metric of any nailed-up route. The higher the value you enter, the less likely that the MAX will bring the link online. The MAX uses the lowest metric.

Usage: You can specify a number between 1 and 15. This value is the virtual hop count. The default value is 7.

Dependencies: Keep this additional information in mind:

- The Ascend-Metric attribute does not apply to bridged connections, such as Combinet links.
- The hop count includes the metric of each switched link in the route.

Example: If a route to a station takes three hops over nailed-up lines, and Ascend-Metric=4 in a user profile that reaches the same station, the MAX does not bring the user's link online. However, if the link is already online, the MAX does not use the nailed-up line.

See Also: "Ascend-Route-IP (228)" on page 9-80
"Framed-Route (22)" on page 9-97

Ascend-Minimum-Channels (173)

Description: The Ascend-Minimum-Channels attribute specifies the minimum number of channels an MP+ call maintains.

Usage: You can specify a number between 1 and 32. The default value is 1.

Dependencies: This attribute applies only to MP+ calls.

For optimum MP+ performance, both sides of a connection must set these values to the same number:

- The base channel count, as specified by Base Ch Count (in the Connection profile) or Ascend-Base-Channel-Count (in RADIUS)
- The minimum channel count, as specified by Min Ch Count (in the Answer profile or Connection profile) or Ascend-Minimum-Channels (in RADIUS)
- The maximum channel count, as specified by Max Ch Count (in the Answer profile or Connection profile) or Ascend-Maximum-Channels (in RADIUS)

See Also: "Ascend-Add-Seconds (240)" on page 9-4
"Ascend-Base-Channel-Count (172)" on page 9-10
"Ascend-DBA-Monitor (171)" on page 9-33
"Ascend-Dec-Channel-Count (237)" on page 9-34
"Ascend-History-Weigh-Type (239)" on page 9-50

"Ascend-Inc-Channel-Count (236)" on page 9-55
"Ascend-Maximum-Channels (235)" on page 9-61
"Ascend-Remove-Seconds (241)" on page 9-78
"Ascend-Seconds-Of-History (238)" on page 9-81
"Ascend-Target-Util (234)" on page 9-84

Ascend-Modem-PortNo (120)

Description: Specifies, for inclusion in an accounting Stop record, the modem used for the call.

Usage: The MAX sends Ascend-Modem-PortNo as part of an accounting Stop record. The attribute does no appear in a user profile.

Dependencies: Because the MAX designates a modem by slot card and port, you must consider the value of Ascend-Modem-SlotNo.

See Also: Ascend-Modem-SlotNo

Ascend-Modem-SlotNo (Attribute 121)

Description: Specifies, for inclusion in an accouting Stop record, the slot containing the modem used for the call.

Usage: The MAX sends Ascend-Modem-SlotNo as part of an accounting Stip record. The attribute does not appear in a user profile.

Dependencies: Because the MAX designates a modem by slot card and port, you must consider the value of Ascend-Modem-PortNo

See Also: Ascend-Modem-PortNo

Ascend-MPP-Idle-Percent (254)

Description: The Ascend-MPP-Idle-Percent attribute specifies a percentage of bandwidth utilization below which the MAX clears a single-channel MP+ call.

Usage: Specify an integer between 0 and 99. The default value is 0 (zero). This setting causes the MAX to ignore bandwidth utilization when determining whether to clear a call.

Dependencies: Keep this additional information in mind:

- MP+ must be the selected encapsulation method for the profile (Framed-Protocol=MPP).
- If either end of a connection sets the Ascend-MPP-Idle-Percent attribute or Idle Pct parameter to 0 (zero), the MAX ignores bandwidth utilization when determining when to clear a call.
- Bandwidth utilization must fall below this percentage *on both sides of the connection* before the MAX clears the call.
- If the device at the remote end of the link enters an Ascend-MPP-Idle-Percent setting lower than the value you specify, the MAX does not clear the call until bandwidth utilization falls below the lower percentage.

- If the time set by the Ascend-Idle-Limit expires, the call disconnects whether or not bandwidth utilization falls below the Ascend-MPP-Idle-Percent setting.
- When bandwidth utilization falls below the Ascend-MPP-Idle-Percent setting, the call disconnects regardless of whether the time specified by the Ascend-Idle-Limit attribute has expired.
- Because the Ascend-MPP-Idle-Percent attribute is dependent on traffic levels on both sides of the connection, we recommend that you use the Ascend-Idle-Limit attribute in preference to it.

See Also: "Ascend-Idle-Limit (244)" on page 9-55
"Ascend-Preempt-Limit (245)" on page 9-72

Ascend-Multicast-Client (152)

Description: The Ascend-Multicast-Client attribute specifies when the user is a multicast client of the MAX.

Usage: You can specify one of these values:

- Multicast-No (0)

  This setting indicates that the user is not a multicast client of the MAX.
- Multicast-Yes (1)

  This setting indicates that the user is a multicast client of the MAX.

Dependencies: This attribute applies solely to the IP-only release of the MAX 4000.

See Also: "Ascend-Multicast-Rate-Limit (153)" on page 9-67

Ascend-Multicast-Rate-Limit (153)

Description: The Ascend-Multicast-Rate-Limit attribute specifies how many seconds the MAX waits before accepting another packet from a multicast client. To prevent multicast clients from creating response storms to multicast transmissions, you configure the user profile to limit the rate at which the MAX accepts packets from clients.

Usage: Specify an integer. If you set the attribute to 0 (zero), the MAX does not apply rate limiting. The default value is 100. The MAX discards any subsequent packets it receives in the window you specify.

Dependencies: This attribute applies solely to the IP-only release of the MAX 4000.

See Also: "Ascend-Multicast-Client (152)" on page 9-67

Ascend-Multilink-ID (187)

Description: The Ascend-Multilink-ID attribute specifies the ID number of the Multilink bundle when the session closes. A Multilink bundle is a multichannel MP or MP+ call. Each online channel of the MP or MP+ call is a session.

The MAX sends Ascend-Multilink-ID in an Accounting-Request packet when all of these conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-Multilink-ID does not appear in a user profile and has no default value.

See Also: "Ascend-Num-In-Multilink (188)" on page 9-69

Ascend-Netware-timeout (223)

Description: The Ascend-Netware-Timeout attribute specifies how long in minutes the MAX responds to NCP watchdog requests on behalf of IPX clients on the other side of an offline IPX bridging connection. Responding to watchdog requests on behalf of clients is commonly called watchdog spoofing.

Usage: Specify an integer between 0 and 65535. The default value is 0 (zero). This default allows the MAX to respond to watchdog requests without a time limit.

The timer begins counting down as soon as the WAN bridging link goes offline. At the end of the selected time, the MAX releases the client-server connections. If there is a reconnection of the WAN session, the MAX cancels the timeout.

Dependencies: Ascend-Netware-timeout applies to IPX bridging connections when the MAX is on the server LAN and not on the client LAN—that is, when Ascend-Handle-IPX= Handle-IPX-Server.

See Also: "Ascend-Handle-IPX (222)" on page 9-49

Ascend-Number-Sessions (202)

Description: The Ascend-Number-Sessions attribute specifies the number of active user sessions of a given class (as specified by the Class attribute). In the case of multichannel calls, such as MP+ calls, each separate connection counts as a session.

Usage: The Ascend-Number-Sessions attribute has a compound value. The first part specifies a user-session class. The second part reports the number of active sessions in that class.

In the MAX, you can set the Sess Timer parameter in the Ethernet>Mod Config>Accounting menu to send accounting requests at regular intervals. At the specified interval, the MAX reports the number of open sessions by sending an Ascend-Event-Request packet (code 33). This packet contains an NAS-Identifier attribute, an Ascend-Event-Type attribute, and one or more Ascend-Number-Sessions attributes. The authentication server must send back an Ascend-Event-Response packet (code 34) with the correct identifier to the MAX.

In addition, you can set the Sess Timer parameter in the Ethernet>Mod Config>Auth menu to send requests to the authentication server at regular intervals. In a session event when Auth=RADIUS/LOGOUT, the MAX sends values for Password, NAS-Identifier, Ascend-Event-Type, and Ascend-Number-Sessions in an Ascend-Event-Request packet (code 33). The authentication server must send back an Ascend-Event-Response packet (code 34) with the correct identifier to the MAX.

Dependencies: The MAX sends the Ascend-Number-Sessions attribute in Ascend-Event-Request packets. Only RADIUS daemons you customize to recognize this packet code respond these request packets from the MAX. Other daemons ignore it. Therefore, both the standard Livingston RADIUS daemon and the Ascend daemon ignore this attribute.

When modifying the daemon, make sure that it recognizes an Ascend-Event-Request packet in this format:

```
Code (8-bit)=33

Identifier (8-bit)

Length (16-bit)

Authenticator (48-bit for an accounting server, 64-bit for an
authentication server)

List of attributes
```

Example: Suppose that the MAX has three classes of clients: Class-1, Class-2, and Class-3. At the time of the sessions report, there are eight active sessions: three Class-1 sessions, four Class-2 sessions, and one Class-3 session. The accounting packet the MAX sends back to the RADIUS accounting server has three Ascend-Number-Session attributes, one for each of these class/session pairs.

See Also: “Ascend-Event-Type (150)” on page 9-40
“Class (25)” on page 9-91

Ascend-Num-In-Multilink (188)

Description: The Ascend-Num-In-Multilink attribute specifies the number of sessions remaining in a Multilink bundle when the session closes. A Multilink bundle is a multichannel MP or MP+ call. Each online channel of the MP or MP+ call is a session.

The MAX sends Ascend-Num-In-Multilink in an Accounting-Request packet when all of these conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-Num-In-Multilink does not appear in a user profile and has no default value.

See Also: “Ascend-Multilink-ID (187)” on page 9-67

Ascend-PPP-Address (253)

Description: The Ascend-PPP-Address attribute specifies the MAX unit’s IP address reported to the calling unit during PPP IPCP negotiations.

Usage: Specify an IP address in dotted decimal notation. An IP address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0. If you accept the default, IPCP negotiates with the value of the IP Adrs parameter in the Ethernet>Mod Config>Ether Options menu.

If you specify a valid IP address, IPCP negotiates with that IP address. If you specify 255.255.255.255, IPCP negotiates with the address 0.0.0.0.

Dependencies: You can assign Ascend-PPP-Address a value different from the MAX unit's true IP address, as long as the user requesting access understands that limitation.

Ascend-PPP-Async-Map (212)

Description: The Ascend-PPP-Async-Map attribute gives the Ascend PPP code the async control character map for the PPP session. The control characters pass through the PPP link as data. Only applications running over the link use this data.

Usage: Specify a 4-byte bitmap to one or more control characters. The async control character map is defined in RFC 1548 and specifies that each bit position represents its ASCII equivalent. The bits are ordered with the lowest bit of the lowest byte being 0. For example, bit 19 corresponds to Control-S (DC3) or ASCII 19.

Example: Your specification might look like this one:

```
Emma Password="m2dan", 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.

Ascend-PPP-VJ-1172 (211)

Description: The Ascend-PPP-VJ-1172 attribute instructs the Ascend PPP code to use the 0x0037 value for the VJ compression type. The MAX uses this value only during IPNCP negotiation. The MAX accepts incoming 1172 type options without your setting this option.

RFC 1172 section 5.2 contains an erroneous statement that the VJ compression type value is 0x0037. It should be 0x002d. However, many older PPP implementations use the 0x0037 value when negotiating VJ compression. If you do not specify a value for Ascend-PPP-VJ-1172, the VJ compression type is 0x002d.

Usage: Enter your specification using this format:

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

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

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

When you turn on VJ compression, the MAX removes the TCP/IP header, and associates a TCP/IP packet with a connection by giving it a slot ID. The first packet coming into a connection must have a slot ID, but succeeding packets need not have one. If the packet does not have a slot ID, the MAX assumes that it uses the last slot ID. This scenario uses slot ID compression, because the slot ID does not appear in any packet but the first in a stream.

However, there may be times when you want each VJ-compressed packet to have a slot ID. The Ascend-PPP-VJ-Slot-Comp attribute exists for this purpose.

Usage: To specify that no slot compression occurs, set the Ascend-PPP-VJ-Slot-Comp attribute to VJ-Slot-Comp-No (1). If you do not specify a value for Ascend-PPP-VJ-Slot-Comp, and Framed-Compression=Van-Jacobson-TCP-IP, slot compression occurs.

See Also: "Framed-Compression (13)" on page 9-94

Ascend-Pre-Input-Octets (190)

Description: The Ascend-Pre-Input-Octets attribute indicates the number of input octets before authentication.

The MAX includes Ascend-Pre-Input-Octets in an Accounting-Request packet when all of these conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-Pre-Input-Octets does not appear in a user profile. Its default value is 0 (zero).

Ascend-Pre-Input-packets (192)

Description: The Ascend-Pre-Input-packets attribute indicates the number of input packets before authentication.

The MAX includes Ascend-Pre-Input-packets in an Accounting-Request packet when all of these conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-Pre-Input-packets does not appear in a user profile. Its default value is 0 (zero).

Ascend-Pre-Output-Octets (191)

Description: The Ascend-Pre-Output-Octets attribute indicates the number of output octets before authentication.

The MAX includes Ascend-Pre-Output-Octets in an Accounting-Request packet when all of these conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-Pre-Output-Octets does not appear in a user profile. Its default value is 0 (zero).

Ascend-Pre-Output-packets (193)

Description: The Ascend-Pre-Output-packets attribute indicates the number of output packets before authentication.

The MAX includes Ascend-Pre-Output-packets in an Accounting-Request packet when all of these conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-Pre-Output-packets does not appear in a user profile. Its default value is 0 (zero).

Ascend-Preempt-Limit (245)

Description: The Ascend-Preempt-Limit attribute specifies the number of idle seconds the MAX waits before using one of the channels of an idle link for a new call.

Usage: Specify an integer between 0 and 65535. The MAX never preempts a call if you enter 0 (zero). The default value is 60.

Dependencies: The Ascend-Preempt-Limit attribute does not apply to nailed-up links.

See Also: "Ascend-Idle-Limit (244)" on page 9-55
"Ascend-MPP-Idle-Percent (254)" on page 9-66

Ascend-Preference (126)

Description: This attribute specifies the preference for a route defined by the Framed-Address attribute in a dial-in or dial-out user profile. Every RADIUS user profile that specifies an explicit IP address using the Framed-Address attribute indicates a static route.

Usage: Specify an integer. The default value is 60. We recommend that you accept this default for dial-in and dial-out user profiles.

Dependencies: Make sure that more desirable routes have a lower preference number. In particular, make sure that routes for connections that are down have a higher preference number than routes for connections that are up. The following table lists the factory default values for route preferences.

Route type	**Default value**
Interface	0
ICMP	30
RIP	100
OSPF ASE	150
OSPF Internal	10
Static	60
Down-WAN	120

Route type	Default value
Infinite	225

Ascend-PreSession-Time (198)

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

The MAX includes Ascend-PreSession-Time in an Accounting-Request packet when both of these conditions are true:

- The session has ended or has failed to authenticate (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Usage: Ascend-PreSession-Time does not appear in a user profile. Its default value is 0 (zero).

Ascend-Primary-Home-Agent (129)

Description: The Ascend-Primary-Home-Agent attribute specifies the first home agent the foreign agent tries to reach when setting up an ATMP tunnel, and indicates the UDP port the foreign agent uses for the link.

The RADIUS server passes the attributes in the mobile node's RADIUS user profile to the foreign agent. The foreign agent sends these attributes when connecting with the home agent.

A mobile node can also connect directly to the home agent. An ATMP-based RADIUS profile that is local to the home agent enables the mobile node to bypass a foreign agent connection, but does not preclude a foreign agent. If both the home agent and the foreign agent have local RADIUS profiles for the mobile node, the node can choose between a direct connection or a tunneled connection through the foreign agent.

Usage: Specify the primary home agent using this syntax:

```
Ascend-Primary-Home-Agent="hostname | ip_address [:udp_port]"
```

- The ***hostname*** argument indicates the home agent's symbolic hostname.
- The ***ip_address*** argument indicates the home agent's IP address in dotted decimal notation.

  Specify an IP address if a DNS server is not set up for the home agent. You can specify a hostname or an IP address, but not both.
- The optional ***udp_port*** argument indicates the UDP port on which the foreign agent communicates with the home agent.

  The default value is 5150.
- The colon (:) separates the hostname or IP address from the UDP port specification.

Example: To specify the home agent max1.home.com at IP address 10.0.0.1, and indicate that the foreign agent should use UDP port 6001, specify one of these lines in the RADIUS user profile:

```
Ascend-Primary-Home-Agent="max1.home.com:6001"
```

```
Ascend-Primary-Home-Agent="10.0.0.1:6001"
```

The following RADIUS profile authenticates a mobile NetWare client that connects directly to the home agent. In this example, the home agent is in gateway mode. It forwards packets from the mobile node across a nailed-up WAN link to the home IPX network.

```
Mobile-IPX Password="unit"
     User-Service=Framed-User,
     Ascend-Route-IPX=Route-IPX-Yes,
     Framed-Protocol=PPP,
     Ascend-IPX-Peer-Mode=IPX-Peer-Dialin,
     Framed-IPX-Network=40000000,
     Ascend-IPX-Node-Addr=12345678,
     Ascend-Primary-Home-Agent="max1.home.com:6001",
     Ascend-Secondary-Home-Agent="max2.home.com:6001",
     Ascend-Home-Network-Name="Dave’s MAX",
     Ascend-Home-Agent-Password="Pipeline"
```

Dependencies: Keep this additional information in mind:

- If you specify the Ascend-Home-Agent-UDP-Port attribute on the line immediately following the Ascend-Primary-Home-Agent attribute, you need not specify a value for ***udp_port***.

  By the same token, if you specify a value for the ***udp_port*** argument of Ascend-Secondary-Home-Agent, or if you accept the default of 5150, you need not specify the Ascend-Home-Agent-UDP-Port attribute.
- It is preferable to use Ascend-Primary-Home-Agent in place of the Ascend-Home-Agent-IP-Addr attribute in the RADIUS user profile. However, the Stop record will include Ascend-Home-Agent-IP-Addr and not Ascend-Primary-Home-Agent.
- To specify a secondary home agent for use if the primary home agent is unavailable, use the Ascend-Secondary-Home-Agent attribute.

Note: The RADIUS accounting Stop record will include Ascend-Home-Agent-IP-Addr when Ascend-Primary-Home-Agent is present in the user profile.

See Also: “Ascend-Home-Agent-Password (184)” on page 9-52
“Ascend-Home-Agent-UDP-Port (186)” on page 9-53
“Ascend-Home-Network-Name (185)” on page 9-53
“Ascend-Secondary-Home-Agent (130)” on page 9-80

Ascend-PRI-Number-Type (226)

Description: The Ascend-PRI-Number-Type attribute specifies the type of phone number the MAX dials.

Usage: You can specify one of these values:

- Unknown-Number (0)

  This setting indicates that the MAX can dial any type of number.
- Intl-Number (1)

  This setting indicates that the MAX dials a number outside the U.S.

- National-Number (2)

  This setting indicates that the MAX dials a number inside the U.S. National-Number is the default.
- Local-Number (4)

  This setting indicates that the MAX dials a number within your Centrex group.
- Abbrev-Number (5)

  This setting indicates that the MAX dials an abbreviated phone number.

Ascend-PW-Expiration (21)

Description: The Ascend-PW-Expiration attribute specifies an expiration date for a user's password in a user profile.

When the MAX makes an authentication request, the RADIUS server checks the current date against the value of 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.

Usage: Specify a month, day, and year.

- For the month specification, enter the first three letters of the month in which you want the password to expire, or 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.

  The values 2, 02, 002, and 0021 are all valid, but 32 is not.
- For the year specification, enter a four-digit year.

  The year must start with the number 19.
- Separate each part of the date specification using one or more spaces, tabs, or commas.

The default value is 00/00/00.

Dependencies: Keep this additional information in mind:

- If a password expires and the user resets it, the RADIUS server adds the value of Ascend-PW-Lifetime to the date on which the user resets the password.

  The resulting date becomes the new value for Ascend-PW-Expiration.

  For example, suppose that Ascend-PW-Lifetime=30, Ascend-PW-Expiration=January 1, 1997, and today's date is March 1, 1997. If the user resets the password today, the value of Ascend-PW-Expiration becomes today's date + Ascend-PW-Lifetime, or March 31, 1997.
- If the password has not expired, the value of Ascend-PW-Expiration overrides the value of Ascend-PW-Lifetime.

  For example, if on January 1, 1997 you set Ascend-PW-Lifetime=30 and Ascend-PW-Expiration=January 15, 1997, the password expires on January 15, 1997. In other words, if the password has not expired, the value of Ascend-PW-Lifetime is irrelevant.

Example: Your specification might look like this one:

```
Emma Password="m2dan", User-Service=Login-User, Ascend-PW-
Expiration="January 1, 1997"
...
```

See Also: "Ascend-PW-Lifetime (208)" on page 9-76

Ascend-PW-Lifetime (208)

Description: The Ascend-PW-Lifetime attribute specifies the number of days that a password is valid.

Usage: Specify an integer to indicate the number of days for which the user's password is valid. You can set the Ascend-PW-Lifetime attribute on any line other than the first line of the user profile.

Dependencies: Keep this additional information in mind:

- If a password expires and the user resets it, the RADIUS server adds the value of Ascend-PW-Lifetime to the date on which the user resets the password.

  The resulting date becomes the new value for Ascend-PW-Expiration. For example, suppose that Ascend-PW-Lifetime=30, Ascend-PW-Expiration=January 1, 1997, and today's date is March 1, 1997. If the user resets the password today, the value of Ascend-PW-Expiration becomes today's date + Ascend-PW-Lifetime, or March 31, 1997.
- If the password has not expired, the value of Ascend-PW-Expiration overrides the value of Ascend-PW-Lifetime.

  For example, if on January 1, 1997 you set Ascend-PW-Lifetime=30 and Ascend-PW-Expiration=January 15, 1997, the password expires on January 15, 1997. In other words, if the password has not expired, the value of Ascend-PW-Lifetime is irrelevant.
- If Ascend-PW-Lifetime is absent, the value of Lifetime-In-Days determines the password duration.

  The Lifetime-In-Days value in the RADIUS dictionary is the default value for Ascend-PW-Lifetime. By default, Lifetime-In-Days is 0 (zero). This value means that passwords do not expire.

Example: You might make this specification:

```
Emma Password="m2dan", User-Service=Login-User, Ascend-PW-
Expiration="Jan 1, 1997"
     Ascend-PW-Lifetime=30
```

See Also: "Ascend-PW-Expiration (21)" on page 9-75

Ascend-Receive-Secret (215)

Description: The Ascend-Receive-Secret attribute specifies a value that must match the password that the RADIUS server sends it to your MAX from the calling unit.

Usage: You can use the Ascend-Receive-Secret attribute for CACHE-TOKEN or PAP-TOKEN-CHAP authentication. In either case, you can specify up to 20 characters. The default value is null.

- CACHE-TOKEN authentication uses a shared secret, and simplifies the authentication process by caching the user's token for the fixed length of time specified by the Ascend-Token-Expiry attribute.

  During the lifetime of the token, subsequent calls by the user require only CHAP authentication without the use of a hand-held security card. For this type of authentication, set the Ascend-Receive-Secret attribute to the same password as the Send PW parameter in the Connection profile that places the incoming call. The RADIUS server uses this value to authenticate incoming calls from a user while his or her token is cached and alive. The cached token resides on the MAX during the initial security-card authentication process.

- PAP-TOKEN-CHAP authentication uses an encrypted CHAP password with which the answering unit authenticates second and subsequent channels of an MP+ call.

  For this type of authentication, set Ascend-Receive-Secret to the value of the Aux Send PW parameter in the Connection profile at the remote end.

  In PAP-TOKEN-CHAP authentication, you need to verify only the initial connection using a hand-held security card. CHAP verifies any additional channels. That is, whenever the MAX adds channels to a PPP or MP+ call using PAP-TOKEN-CHAP, the calling unit sends the encrypted value of Aux Send PW, and the answering unit checks this password against Ascend-Receive-Secret. The answering unit receives Ascend-Receive-Secret from the RADIUS server when the first channel of the call connects.

Example: This example shows the settings necessary for a user called John to use an Enigma Logic server. The MAX sends the password to the security server for authentication.

```
John   Password="SAFEWORD", Ascend-Token-Expiry=90, Ascend-
Token-Idle=80, Ascend-Token-Immediate=Tok-Imm-Yes

       Ascend-Receive-Secret="shared-secret",

       User-Service=Framed-User,

       Framed-Protocol=MPP,

       Framed-Address=200.0.5.1,

       Framed-Netmask=255.255.255.0
```

This example shows the settings necessary for a user called Emma to use an Enigma Logic server. Because this profile includes the attribute Ascend-Receive-Secret, the MAX can authenticate additional channels through CHAP without having to go to the SAFEWORD server for authentication.

```
Emma   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"
```

See Also: "Ascend-Token-Expiry (204)" on page 9-85
"Ascend-Token-Idle (199)" on page 9-85
"Ascend-Token-Immediate (200)" on page 9-86

Ascend-Remote-Addr (155)

Description: The Ascend-Remote-Addr attribute specifies the IP address of the numbered interface at the remote end of a link.

Usage: Specify the IP address of the numbered interface. An IP address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0.

Dependencies: For Ascend-Remote-Addr to apply, you must enable IP for the user profile (Ascend-Route-IP=Route-IP-Yes).

See Also: “Ascend-Route-IP (228)” on page 9-80

Ascend-Remove-Seconds (241)

Description: The Ascend-Remove-Seconds attribute specifies the number of seconds that average line utilization (ALU) for transmitted data must fall below the threshold indicated by the Ascend-Target-Util attribute before the MAX begins removing bandwidth from a session. The MAX determines the ALU for a session by using the algorithm specified by the Ascend-History-Weigh-Type attribute.

When utilization falls below the threshold for a period of time greater than the value of the Ascend-Remove-Seconds attribute, the MAX attempts to remove the number of channels specified by the Ascend-Dec-Channel-Count attribute. Using the Ascend-Remove-Seconds attribute prevents the system from continually subtracting bandwidth, and can slow down the process of removing bandwidth.

Usage: Specify a number between 1 and 300. The default value is 10.

Dependencies: Keep this additional information in mind:

- One channel must be up at all times.
- Removing bandwidth cannot cause the ALU to exceed the threshold specified by the Ascend-Target-Util attribute.
- The number of channels remaining cannot fall below the amount specified by the Ascend-Minimum-Channels attribute.
- Ascend-Add-Seconds and Ascend-Remove-Seconds have little or no effect on a system with a high Ascend-Seconds-Of-History value.

  If the value of Ascend-Seconds-Of-History is low, the Ascend-Add-Seconds and Ascend-Remove-Seconds attributes provide an alternative way to ensure that spikes must persist for a certain period of time before the system responds.

See Also: “Ascend-Add-Seconds (240)” on page 9-4
“Ascend-Base-Channel-Count (172)” on page 9-10
“Ascend-DBA-Monitor (171)” on page 9-33
“Ascend-Dec-Channel-Count (237)” on page 9-34
“Ascend-History-Weigh-Type (239)” on page 9-50
“Ascend-Inc-Channel-Count (236)” on page 9-55
“Ascend-Maximum-Channels (235)” on page 9-61
“Ascend-Minimum-Channels (173)” on page 9-65
“Ascend-Seconds-Of-History (238)” on page 9-81
“Ascend-Target-Util (234)” on page 9-84

Ascend-Require-Auth (201)

Description: The Ascend-Require-Auth attribute specifies whether the MAX requires additional authentication after Calling Line ID (CLID) or called-number authentication. Called-number authentication is also known as Dialed Number Information Service (DNIS) authentication.

Usage: You can specify one of these values:

- Not-Require-Auth (0) specifies that additional authentication is not required.

  Not-Require-Auth is the default.
- Require-Auth (1) specifies that additional authentication is required.

  If you require additional authentication, you must configure a two-tiered dial-in setup.

  For additional authentication after CLID authentication, the first-tier dial-in user profile has the following two-line format:

```
phonenum Password="Ascend-CLID"
            Ascend-Require-Auth=Require-Auth
```

For additional authentication after called-number authentication, the first-tier dial-in user profile has the following two-line format:

```
phonenum Password="Ascend-DNIS"
            Ascend-Require-Auth=Require-Auth
```

- For calls involving CLID authentication, ***phonenum*** represents the calling party's phone number.
- For calls involving called-number authentication, ***phonenum*** represents the called number.
- The Password setting specifies that RADIUS authenticates the caller by caller ID or called number, depending on your authentication setup.
- The Ascend-Require-Auth setting specifies that after CLID or called-number authentication, additional authentication is required.

When you set Ascend-Require-Auth=Require-Auth, you should not include any other attributes in the user profile. You must specify the characteristics of the call in the second-tier user profile.

Example: This example shows a two-tiered approach. The first user profile specifies CLID authentication, and indicates that additional authentication will follow. Because Recv Auth=CHAP in the Answer profile, CHAP authentication will follow CLID authentication. The second user profile sets up other attributes for the call.

```
5551212   Password="Ascend-CLID"
          Ascend-Require-Auth=Require-Auth
Emma   Password="pwd" Caller-Id="5551212"
       User-Service=Framed-User,
       Framed-Protocol=PPP,
       Framed-Address=200.11.12.10,
       Framed-Netmask=255.255.255.248,
       Ascend-Send-Secret="pwd",
       ...
```

Ascend-Route-Appletalk (118)

Description: Specifies whether AppleTalk routing is enabled for the connection. When AppleTalk routing is enabled, the connection can forward AppleTalk packets.

Usage: Specify one of the following values:

- Route-Appletalk-No (0) disables AppleTalk routing for this user profile.
  The default is No (0).
- Route-Appletalk-Yes (1) enables AppleTalk routing for this user profile.

Dependencies: If you specify Route-Appletalk-Yes, you must set the Ascend- Appletalk-Peer-Mode attribute.

Ascend-Route-IP (228)

Description: The Ascend-Route-IP attribute specifies whether the MAX enables IP routing for the user profile.

Usage: You can specify one of these values:

- Route-IP-No (0) disables IP routing.
- Route-IP-Yes (1) enables IP routing.
  Route-IP-Yes is the default.

See Also: “Framed-Route (22)” on page 9-97

Ascend-Route-IPX (229)

Description: The Ascend-Route-IPX attribute indicates whether the MAX enables IPX routing for the user profile. For PPP and MP+ calls, both ends of the connection must have matching settings to route IPX.

Usage: You can specify one of these values:

- Route-IPX-No (0) disables IPX routing.
  Route-IPX-No is the default.
- Route-IPX-Yes (1) enables IPX routing.

See Also: “Ascend-IPX-Alias (224)” on page 9-58
“Ascend-IPX-Peer-Mode (216)” on page 9-58
“Ascend-IPX-Route (174)” on page 9-59

Ascend-Secondary-Home-Agent (130)

Description: The Ascend-Secondary-Home-Agent attribute specifies the secondary home agent the foreign agent tries to reach when the primary home agent (specified by Ascend-Primary-Home-Agent) is unavailable. The attribute also indicates the UDP port the foreign agent uses for the link.

Usage: Specify the secondary home agent using this syntax:

```
Ascend-Secondary-Home-Agent="hostname | ip_address [:udp_port]"
```

- The ***hostname*** argument indicates the home agent's symbolic hostname.
- The ***ip_address*** argument indicates the home agent's IP address in dotted decimal notation.

  Specify an IP address if a DNS server is not set up for the home agent. You can specify a hostname or an IP address, but not both.
- The optional ***udp_port*** argument indicates the UDP port on which the foreign agent communicates with the home agent.

  The default value is 5150.
- The colon (:) separates the hostname or IP address from the UDP port specification.

Example: To specify max2.home.com at IP address 10.0.0.2 as the secondary home agent, and indicate that the foreign agent should use UDP port 6002, specify one of these lines in the RADIUS user profile:

```
Ascend-Secondary-Home-Agent="max2.home.com:6002"
```

```
Ascend-Secondary-Home-Agent="10.0.0.2:6002"
```

To specify a primary home agent and a secondary home agent, enter these lines in the RADIUS user profile:

```
Ascend-Primary-Home-Agent="max1.home.com:6001"

Ascend-Secondary-Home-Agent="max2.home.com:6002"
```

The foreign agent first tries max1.home.com on UDP port 6001. If the name cannot be resolved, or if max1.home.com does not respond, the foreign agent then tries max2.home.com on UDP port 6002.

The RADIUS accounting Stop record will include Ascend-Home-Agent-IP-Addr when Ascend-Secondary-Home-Agent is present in the user profile.

Dependencies: If you specify the Ascend-Home-Agent-UDP-Port attribute on the line immediately following the Ascend-Secondary-Home-Agent attribute, you need not specify a value for ***udp_port***. By the same token, if you specify a value for the ***udp_port*** argument of Ascend-Secondary-Home-Agent, or if you accept the default of 5150, you need not specify the Ascend-Home-Agent-UDP-Port attribute.

See Also: "Ascend-Home-Agent-Password (184)" on page 9-52
"Ascend-Home-Agent-UDP-Port (186)" on page 9-53
"Ascend-Home-Network-Name (185)" on page 9-53
"Ascend-Primary-Home-Agent (129)" on page 9-73

Ascend-Seconds-Of-History (238)

Description: The Ascend-Seconds-Of-History attribute specifies the number of seconds the MAX uses as a sample for calculating average line utilization (ALU) of transmitted data. The MAX arrives at this average using the algorithm specified by the Ascend-History-Weigh-Type attribute.

The number of seconds you choose for the Ascend-Seconds-Of-History attribute depends on your device's traffic patterns. For example, if you want to average spikes with normal traffic flow, you may want the MAX to establish a longer historical time period. If, on the other hand, traffic patterns consist of many spikes that are short in duration, you may want to specify a shorter period of time. Doing so assigns less weight to the short spikes.

Usage: Specify a number between 1 and 300. The default value is 15 seconds.

Dependencies: Keep this additional information in mind:

- Ascend-Seconds-Of-History applies only to MP+ calls (Framed-Protocol=MPP).
- If you specify a small value for the Ascend-Seconds-Of-History attribute, and increase the values of the Ascend-Add-Seconds attribute and the Ascend-Remove-Seconds attribute relative to the value of Ascend-Seconds-Of-History, the system becomes less responsive to quick spikes.

  The easiest way to determine the proper values for all these attributes is to observe usage patterns. If the system is not responsive enough, the value of Ascend-Seconds-Of-History is too high.

See Also: “Ascend-Add-Seconds (240)” on page 9-4
“Ascend-Base-Channel-Count (172)” on page 9-10
“Ascend-DBA-Monitor (171)” on page 9-33
“Ascend-Dec-Channel-Count (237)” on page 9-34
“Ascend-History-Weigh-Type (239)” on page 9-50
“Ascend-Inc-Channel-Count (236)” on page 9-55
“Ascend-Maximum-Channels (235)” on page 9-61
“Ascend-Minimum-Channels (173)” on page 9-65
“Ascend-Remove-Seconds (241)” on page 9-78
“Ascend-Target-Util (234)” on page 9-84

Ascend-Send-Auth (231)

Description: The Ascend-Send-Auth attribute specifies the authentication protocol that the MAX requests when initiating a connection using PPP or MP+ encapsulation. The answering side of the connection determines which authentication protocol, if any, the connection uses.

Usage: You can specify one of these values:

- Send-Auth-None (0) indicates that the MAX does not request an authentication protocol for outgoing calls.

  Send-Auth-None is the default.
- Send-Auth-PAP (1) indicates that the MAX requests Password Authentication Protocol (PAP).

  PAP is a PPP authentication protocol that provides a simple method for the MAX to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment, and does not use encryption. The remote device must support PAP.

  If you specify this setting, the MAX requests PAP authentication, but uses CHAP authentication if the called unit requires CHAP. Choose this setting for non-token card authentication if you want to send your password unencrypted.
- Send-Auth-CHAP (2) indicates that the MAX requests Challenge Handshake Authentication Protocol (CHAP).

  CHAP is a PPP authentication protocol that is more secure than PAP. CHAP provides a way for the remote device to periodically verify the identity of the MAX using a three-way handshake and encryption. Authentication takes place upon initial link establishment. A device can repeat the authentication process any time after the connection is made. The remote device must support CHAP.

If you specify this setting, the MAX does not bring up the connection using PAP. Choose this setting for non-token card authentication if you do not wish to send your password unencrypted—that is, if you do not wish to use PAP authentication.

Dependencies: Keep this additional information in mind:

- Ascend-Send-Auth is applicable only to outgoing user profiles in RADIUS.
- The link must use PPP or MP+ encapsulation.
- If you request PAP or CHAP authentication, you must also specify a password using Ascend-Send-Secret or Ascend-Send-Passwd.

See Also: “Ascend-Send-Passwd (232)” on page 9-83
“Ascend-Send-Secret (214)” on page 9-83

Ascend-Send-Passwd (232)

Description: The Ascend-Send-Passwd attribute specifies the password that the RADIUS server sends to the remote end of a connection on an outgoing call.

Usage: Specify a text string containing up to 20 characters. The default value is null.

Dependencies: In a user profile, you can specify either Ascend-Send-Passwd or Ascend-Send-Secret, but not both. Use Ascend-Send-Passwd only if your version of the MAX does not support Ascend-Send-Secret.

See Also: “Ascend-Send-Auth (231)” on page 9-82
“Ascend-Send-Secret (214)” on page 9-83

Ascend-Send-Secret (214)

Description: The Ascend-Send-Secret attribute specifies the password that the RADIUS server sends to the remote end of a connection on an outgoing call. It is encrypted when passed between the RADIUS server and the MAX.

Usage: Specify a text string containing up to 20 characters. The default value is null.

Dependencies: In a user profile, you can specify either Ascend-Send-Passwd or Ascend-Send-Secret, but not both. Use Ascend-Send-Passwd only if your version of the MAX does not support Ascend-Send-Secret.

See Also: “Ascend-Send-Auth (231)” on page 9-82
“Ascend-Send-Passwd (232)” on page 9-83

Ascend-Session-Svr-Key (151)

Description: The Ascend-Session-Svr-Key attribute enables the MAX to match a user session with a client request to perform certain operations, such as disconnecting a session or changing a session’s filters.

The client sends Ascend-Session-Svr-Key to the RADIUS server in a Disconnect-Request or Change-Filter-Request packet when it initiates an operation. In addition, Ascend-Session-Svr-Key appears in a RADIUS Accounting-Start packet when a session starts.

Usage: Specify up to 16 characters. The default value is null.

Dependencies: The client sends the Ascend-Session-Svr-Key attribute only if Session Key=Yes in the Ethernet>Mod Config>RADIUS Server menu.

Ascend-Shared-Profile-Enable (128)

Description: Enables or disables sharing of a RADIUS user file for multiple incoming users.

Note: To apply Shared Profiles on a per RADIUS user profile basis, you have to disable profile sharing on a system-wide basis by setting Ethernet > Mod Config > Shared Prof = No on the MAX

Usage: You can specify one of the following settings:

- Ascend-Shared-Profile-Enable = Shared-Profile-Yes specifies that multiple incoming calls can share this RADIUS user profile.
- Ascend-Shared-Profile-Enable = Shared-Profile-No specifies that multiple incoming calls cannot share a local Connection Profile.

  The default value is Shared-Profile-No

Dependencies: For the Ascend-Shared-Profile-Enable attribute to apply, you must disable shared profiles for the MAX as a whole with Ethernet > Mod Config > Shared Prof = No.

Ascend-Target-Util (234)

Description: The Ascend-Target-Util attribute specifies the percentage of bandwidth use at which the MAX adds or subtracts bandwidth.

Usage: Specify an integer between 0 and 100. The default value is 70.When the value is 70%, the device adds bandwidth when it exceeds a 70 percent utilization rate, and subtracts bandwidth when it falls below that number.

Dependencies: Keep this additional information in mind:

- When selecting a target utilization value, monitor how the application behaves when using different bandwidths. For example, an application might be able to use 88% of a 64-kbps link, but only 70% of a 256-kbps link. Also, monitor the application at different loads.
- Ascend-Target-Util applies only if the link is using MP+ encapsulation (Framed-Protocol=MPP).

See Also: “Ascend-Add-Seconds (240)” on page 9-4
“Ascend-Base-Channel-Count (172)” on page 9-10
“Ascend-DBA-Monitor (171)” on page 9-33
“Ascend-Dec-Channel-Count (237)” on page 9-34
“Ascend-History-Weigh-Type (239)” on page 9-50
“Ascend-Inc-Channel-Count (236)” on page 9-55
“Ascend-Maximum-Channels (235)” on page 9-61
“Ascend-Minimum-Channels (173)” on page 9-65

"Ascend-Remove-Seconds (241)" on page 9-78
"Ascend-Seconds-Of-History (238)" on page 9-81

Ascend-Third-Prompt (213)

Description: In the MAX configuration interface, the 3rd Prompt parameter enables you to specify an additional prompt for user input in the terminal server interface after the login and password prompts. The MAX passes the information the user enters to the RADIUS server as the Ascend-Third-Prompt attribute.

Usage: The Ascend-Third-Prompt attribute can contain up to 80 characters and does not appear in a user profile. If the user enters more than 80 characters, the MAX truncates the input to 80. If the user does enter any characters, the MAX sets the attribute to null.

Ascend-Token-Expiry (204)

Description: The Ascend-Token-Expiry attribute specifies the lifetime in minutes of a cached token.

CACHE-TOKEN authentication uses a shared secret, and simplifies the authentication process by caching the user's token for the fixed length of time specified by the Ascend-Token-Expiry attribute.When the cached token is still alive, CHAP authenticates subsequent CACHE-TOKEN access requests from the same user without the use of a hand-held security card. When the cached token has expired, the ACE or SAFEWORD server authenticates CACHE-TOKEN access requests.

Usage: On the first line of the user profile, specify an integer representing the lifetime of the cached token in minutes. The default value is 0 (zero). If you accept the default, the MAX rejects subsequent CACHE-TOKEN requests from the same user.

Example: The following two-line example sets up CACHE-TOKEN authentication with a 90-minute token cache. Notice that the Ascend-Token-Expiry attribute must appear on the first line of the profile, along with the user name and ACE or SAFEWORD password:

```
Connor  Password="ACE", Ascend-Token-Expiry=90

    Ascend-Receive-Secret="shared-secret",

    ...
```

See Also: "Ascend-Token-Idle (199)" on page 9-85
"Ascend-Token-Immediate (200)" on page 9-86

Ascend-Token-Idle (199)

Description: The Ascend-Token-Idle attribute specifies the maximum length of time in minutes a cached token can remain alive between authentications.

Usage: On the first line of the user profile, specify an integer representing the maximum length of time in minutes that a cached token can remain alive. The default value is o (zero). If you accept this default, the cached token remains alive until the value of the Ascend-Token-Expiry attribute causes it to expire.

Dependencies: Typically, the value of Ascend-Token-Idle is lower than the value of Ascend-Token-Expiry.

Example: The following two-line example sets up CACHE-TOKEN authentication with a 90-minute token cache and an 80-minute idle limit. Notice that the Ascend-Token-Idle attribute must appear on the first line of the profile:

Jim Password="ACE", Ascend-Token-Expiry=90, Ascend-Token-Idle=80

Ascend-Receive-Secret="shared secret"

See Also: "Ascend-Token-Expiry (204)" on page 9-85
"Ascend-Token-Immediate (200)" on page 9-86

Ascend-Token-Immediate (200)

Description: The Ascend-Token-Immediate attribute specifies how RADIUS treats the password it receives from a login user when the user profile specifies a hand-held security card server. Use this attribute in an ACE or SAFEWORD user profile that contains the setting User-Service=Login-User.

Usage: You can specify one of these values:

- Tok-Imm-No (0) indicates that the MAX ignores the password.

  Choose this value for a security server that requires that a user enter a challenge using a security card before the security server derives a password.

  Tok-Imm-No is the default.
- Tok-Imm-Yes (1) specifies that the MAX sends the password to the security server for authentication.

Dependencies: The Ascend-Token-Immediate attribute does not work with CHAP authentication.

Example: This example shows a portion of a user profile that requires the MAX to send the password to the ACE server. The login-user derives the password from a hand-held security card:

```
Connor  Password="ACE", Ascend-Token-Immediate=Tok-Imm-Yes
        Ascend-Receive-Secret="shared-secret",
        User-Service=Login-User,
        ...
```

See Also: "Ascend-Token-Expiry (204)" on page 9-85
"Ascend-Token-Idle (199)" on page 9-85

Ascend-Transit-Number (251)

Description: The Ascend-Transit-Number attribute specifies the U.S Interexchange Carrier (IEC) you use for long distance calls over a T1 PRI line.

Usage: Specify the same digits you use to prefix a phone number you dial over an ISDN BRI line, T1 access line, or voice interface:

- 288 selects AT&T.
- 222 selects MCI.
- 333 selects Sprint.

The default value is null. If you accept the default, the MAX uses any available IEC for long-distance calls.

Ascend-TS-Idle-Limit (169)

Description: The Ascend-TS-Idle-Limit attribute specifies the number of seconds that a terminal server connection must be idle before the MAX disconnects the session.

Usage: You can specify a value between 0 and 65535.The default value is 120. A setting of 0 (zero) means that the line can be idle indefinitely.

Dependencies: Ascend-TS-Idle-Limit does not apply if you are using a Frame Relay or raw TCP connection, or if Ascend-TS-Idle-Mode=TS-Idle-None.

See Also: “Ascend-TS-Idle-Mode (170)” on page 9-87

Ascend-TS-Idle-Mode (170)

Description: The Ascend-TS-Idle-Mode attribute specifies whether the MAX uses a terminal server idle timer and, if so, whether both the user and host must be idle before the MAX disconnects the session.

Usage: You can specify one of these settings:

- TS-Idle-None (0)

  This setting indicates that the MAX does not disconnect the session no matter how long the line is idle. This setting disables the idle timer.
- TS-Idle-Input (1)

  This setting indicates that the MAX disconnects the session if the user is idle for a length of time greater than the value of the Ascend-TS-Idle-Limit attribute.

  TS-Idle-Input is the default.
- TS-Idle-Input-Output (2)

  This setting indicates that the MAX disconnects the session if both the user and the host are idle for a length of time greater than the value of the Ascend-TS-Idle-Limit attribute.

Example: This profile specifies that the user must be idle for 90 seconds before the MAX disconnects the session.

```
Default Password="UNIX"
        User-Service=Login-User,
        Ascend-TS-Idle-Limit=90,
        Ascend-TS-Idle-Mode=TS-Idle-Input
```

Dependencies: Ascend-TS-Idle-Mode does not apply if you are using a Frame Relay or raw TCP connection.

See Also: “Ascend-TS-Idle-Limit (169)” on page 9-87

Ascend-User-Acct-Base (142)

Description: The Ascend-User-Acct-Base attribute specifies whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16.

Usage: Specify one of these settings:

- Ascend-User-Acct-Base-10 indicates that the numeric base is 10.
  The default is 10.
- Ascend-User-Acct-Base-16 indicates that the numeric base is 16.

For example, when you set Ascend-User-Acct-Base=Ascend-User-Acct-Base-10, the MAX presents a typical session ID to the accounting server in this way:

"1234567890"

When you set Ascend-User-Acct-Base=Ascend-User-Acct-Base-16, the MAX presents the same session ID in this way:

"499602D2"

Dependencies: Changing the value of Ascend-User-Acct-Base while sessions are active results in inconsistent reporting between the Start and Stop records.

See Also: “Ascend-User-Acct-Host (139)” on page 9-88
“Ascend-User-Acct-Key (141)” on page 9-88
“Ascend-User-Acct-Port (140)” on page 9-89
“Ascend-User-Acct-Time (143)” on page 9-89
“Ascend-User-Acct-Type (138)” on page 9-89

Ascend-User-Acct-Host (139)

Description: The Ascend-User-Acct-Host attribute specifies the IP address of the RADIUS accounting server to use for this connection.

Usage: Specify an IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0.

See Also: “Ascend-User-Acct-Base (142)” on page 9-88
“Ascend-User-Acct-Key (141)” on page 9-88
“Ascend-User-Acct-Port (140)” on page 9-89
“Ascend-User-Acct-Time (143)” on page 9-89
“Ascend-User-Acct-Type (138)” on page 9-89

Ascend-User-Acct-Key (141)

Description: The Ascend-User-Acct-Key attribute specifies the RADIUS client password as it appears in the clients file.

Usage: Specify a text string. The default value is null.

See Also: “Ascend-User-Acct-Base (142)” on page 9-88
“Ascend-User-Acct-Host (139)” on page 9-88
“Ascend-User-Acct-Port (140)” on page 9-89

"Ascend-User-Acct-Time (143)" on page 9-89
"Ascend-User-Acct-Type (138)" on page 9-89

Ascend-User-Acct-Port (140)

Description: The Ascend-User-Acct-Port attribute specifies a UDP port number for the connection between the user and the RADIUS accounting server.

Usage: Specify the UDP port number you indicated for the authentication process of the daemon in /etc/services. Or, if you used the `incr` keyword to the –A option when starting the daemon, specify the number of the UDP port for authentication services +1. You can specify a number between 1 and 32767.

See Also: "Ascend-User-Acct-Base (142)" on page 9-88
"Ascend-User-Acct-Host (139)" on page 9-88
"Ascend-User-Acct-Key (141)" on page 9-88
"Ascend-User-Acct-Time (143)" on page 9-89
"Ascend-User-Acct-Type (138)" on page 9-89

Ascend-User-Acct-Time (143)

Description: The Ascend-User-Acct-Time attribute specifies the number of seconds the MAX waits for a response to a RADIUS accounting request from the RADIUS accounting server for this connection.

Usage: Specify an integer between 1 and 10. The default value is 0 (zero).

See Also: "Ascend-User-Acct-Base (142)" on page 9-88
"Ascend-User-Acct-Host (139)" on page 9-88
"Ascend-User-Acct-Key (141)" on page 9-88
"Ascend-User-Acct-Port (140)" on page 9-89
"Ascend-User-Acct-Type (138)" on page 9-89

Ascend-User-Acct-Type (138)

Description: The Ascend-User-Acct-Type attribute specifies the RADIUS accounting server(s) to use for this connection.

Usage: You can specify one of these settings:

- Ascend-User-Acct-None (0)

  This setting indicates the MAX sends accounting information to the RADIUS server specified by the Acct Host #1, Acct Host #2, or Acct Host #3 parameter in the Ethernet>Mod Config>Accounting menu, depending on which server is available. This server is known as the default server.

  The default value is Ascend-User-Acct-None (0).
- Ascend-User-Acct-User (1)

  This setting indicates that the MAX sends accounting information to the RADIUS server specified by the Ascend-User-Acct-Host attribute in the RADIUS user profile.
- Ascend-User-Acct-User-Default (2)

This setting indicates that the MAX sends accounting information both to the RADIUS server specified by the Ascend-User-Acct-Host attribute in the RADIUS user profile and to the default server.

See Also: "Ascend-User-Acct-Base (142)" on page 9-88
"Ascend-User-Acct-Host (139)" on page 9-88
"Ascend-User-Acct-Key (141)" on page 9-88
"Ascend-User-Acct-Port (140)" on page 9-89
"Ascend-User-Acct-Time (143)" on page 9-89

Ascend-Xmit-Rate (255)

Description: Specifies the transmit baud rate for the connection.

Dependencies: The Ascend-Xmit-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 attribute is still sent with the Accounting-Request packet whether the connection is authenticated or not.

Caller-Id (31)

Description: The Caller-Id attribute specifies the calling party number for Calling Line ID (CLID) authentication, indicating the phone number of the user that wants to connect to the MAX.

- If you set Id Auth=Prefer in the Ethernet>Answer menu, the MAX checks the calling party's phone number against the value of the Caller-Id attribute whenever CLID authentication is available.

  If a match is found, and no further authentication is required, the MAX accepts the call.
- If you set Id Auth=Require in the Ethernet>Answer menu, the calling party's phone number must match the value of the Caller-Id attribute before the MAX can answer the call.

  If CLID is not available, the MAX does not answer the call.

Usage: Specify a telephone number. You can indicate up to 37 characters, limited to the following: **1234567890()[]!z-*#|**

The default value is null.

Example: This user profile specifies CLID authentication using name, password, and caller ID:

```
Emma  Password="test", Caller-Id="123456789"
      User-Service=Framed-User,
      Framed-Protocol=PPP,
      Framed-Address=255.255.255.254,
      Framed-Netmask=255.255.255.255,
      Ascend-Assign-IP-Pool=1,
      Ascend-Route-IP=Route-IP-Yes,
      Ascend-Idle-Limit=30
```

Challenge-Response (3)

Description: The Challenge-Response attribute specifies the value that a Challenge Handshake Authentication Protocol (CHAP) user provides in response to the password challenge.

Usage: The MAX sets the Challenge-Response value and sends it in Access-Request packets. The default value is null.

Change-Password (17)

Description: The MAX and the RADIUS server use the Change-Password attribute to change an expired password.

When a user specifies an expired password, RADIUS prompts the user for a new password. When the user enters the new password, the MAX sends an Access-Password-Request packet that contains both the old password (as the value of the Change-Password attribute), and the new password (as the value of the Password attribute).

If the RADIUS server accepts the new password, it tries to edit the users file and replace the expired password with the new one. Note that the RADIUS server can make this change only in the flat file. It cannot make this change in the database version of the users file.

Usage: Change-Password does not appear in a user profile and has no default value.

Class (25)

Description: The Class attribute enables access providers to classify user sessions, such as for the purpose of billing users depending on the service option they choose.

If you include the Class attribute in the RADIUS user profile, the RADIUS server sends it to the MAX in the Access-Accept packet when the session begins. The MAX then includes Class in Accounting-Request packets sent to the RADIUS accounting server under these conditions:

- Whenever a session starts
- Whenever a session stops (as long as the Auth parameter is not set to RADIUS/LOGOUT)

Keep in mind that the accounting entries give the class on a per-user and per-session basis. The Ascend-Number-Sessions attribute reports information on all user sessions—that is, on the number of current sessions of each class.

In addition, suppose the MAX starts CLID authentication by sending an Access-Request packet and receives the Class attribute in an Access-Accept packet. If the MAX requires further authentication, it includes Class in the Access-Request packet.

Usage: Specify an alphanumeric text string containing up to 253 characters. The default value is null.

See Also: “Ascend-Number-Sessions (202)” on page 9-68

Client-Port-DNIS (30)

Description: The Client-Port-DNIS attribute specifies the called-party number, indicating the phone number the user dialed to connect to the MAX. DNIS stands for Dialed Number Information Service. You use this attribute to set up called-number authentication, also known as DNIS authentication.

Usage: Specify the number the remote end dials to reach the MAX, limiting your specification to these characters:

1234567890()[]!z-*#|

You can specify up to 18 characters. The default value is null.

Typically, the phone numbers different callers can use to reach the MAX share a group of digits. For example, a local caller may dial 555-1234, while a long distance caller may dial 1-415-555-1234. In cases such as this, you need only specify the rightmost digits the calls have in common. In this case, you would need to specify only 1234.

Example: This user profile sets up called-number authentication in addition to name and password authentication:

Clara-p50 Password="Ascend", Client-Port-DNIS=1234

User-Service=Framed-User,

Framed-Protocol=MPP,

Framed-Address=200.10.11.12,

Framed-Netmask=255.255.255.248

Filter-Id (11)

Description: This attribute specifies a local data filter or local data firewall profile applied in the current RADIUS user profile. The MAX uses the filter only when it places a call or receives a call using the profile that includes the filter definition. The filters and firewalls specified in the RADIUS user profile are applied for that user the next time the RADIUS user profile is loaded to the MAX.

Usage: You can specify any number of data filters and firewalls. Filter entries apply on a first-match basis, so the order in which you enter the filter entries is significant. If you make changes to a filter in a RADIUS user profile, the changes do not take effect until a call uses that profile.

Example: The following are examples of how a RADIUS user profile can be set up to refer to a filter profile defined on the MAX, and to refer to a firewall defined usingSAM.

Assume the following two filter profiles are already set up on the MAX are:

```
Filter-id=6
Name=DisAllowPing
Out filter 01...Valid=Yes
Out filter 01...Type=IP
Out filter 01...Ip...Forward=No
Out filter 01...Ip...Protoco1=6

Filter-id=9
Name=DisAllowTelnet
Out filter 01...Valid=Yes
Out filter 01...Type=IP
Out filter 01...Ip...Forward=No
Out filter 01...Ip...Protocol=6
Out filter 01...Ip...Src Port Cmp-Eql
Out filter 01...Ip...Src Port #=23
```

The RADIUS user profile is:

```
someuser   Password="ascend"
           User-Service=Framed-User,
           Filter-Id="6",
           Filter-Id="9",
           Ascend-Data-Filter="ip out forward",
           Framed-Protocol=PPP,
           Framed-Address=10.11.1.1,
           Framed-Netmask=255.255.255.0,
           State="p"
```

The first filter is applied, disallowing pings. The second filter disallows Telnet packets. The Ascend-Data-Filter entry allows all IP packets to be forwarded. All pings and Telnet packets will be blocked, but other IP data packets are allowed.

The following is an example of a RADIUS user profile that specifies a firewall set up in SAM:

```
Example: someuser   Password="ascend"
           User-Service=Framed-User,
           Filter-Id="101",
           Framed-Protocol=PPP,
           Framed-Address=10.11.1.1,
           Framed-Netmask=255.255.255.0,
          State="p"
```

See Also: Ascend-Data-Filter, Ascend-Call-Filter

Framed-Address (8)

Description: The Framed-Address attribute specifies the IP address of the caller in a user profile.

RADIUS can authenticate an incoming call by matching its IP address to one you specify in the RADIUS user profile. In addition, if the remote end requires an IP address on an outgoing call, and does not assign one dynamically, you must specify it in the user profile.

Usage: Specify an IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0. An answering user profile with this setting matches all IP addresses.

Dependencies: Every Connection profile and RADIUS user profile that specifies an explicit IP address is a static route.

See Also: “Framed-Netmask (9)” on page 9-94

Framed-Compression (13)

Description: The Framed-Compression attribute turns TCP/IP header compression on or off.

Usage: To turn on TCP/IP header compression, specify Van-Jacobson-TCP-IP. This setting applies only to packets in TCP applications, such as Telnet, and turns on header compression for both sides of the link. By default, this attribute does not turn on header compression.

Dependencies: Turning on header compression is most effective in reducing overhead when the data portion of the packet is small.

See Also: “Ascend-Link-Compression (233)” on page 9-61

Framed-IPX-Network (23)

Description: The Framed-IPX-Network attribute specifies a virtual IPX network required for the Ascend Tunnel Management Protocol (ATMP) home agent to route IPX packets to the mobile node. When specified in a user profile, the Framed-IPX-Network attribute instructs the answering unit to advertise an additional IPX route.

Usage: Specify the IPX network number of the IPX router at the remote end of the connection. The default value is null.

RADIUS requires that Framed-IPX-Network have a decimal value (base 10), but IPX network numbers generally appear as hexadecimal values (base 16). In order to give this attribute a value, you must convert the hexadecimal IPX network number to decimal format for use in the user profile. For example, if the IPX network number is 13870000, you must convert it to the decimal 49990000. This requirement does not apply for the IPX node address, which appears as a 12-digit string enclosed in double-quotes.

See Also: “Ascend-IPX-Node-Addr (182)” on page 9-58

Framed-MTU (12)

Description: The Framed-MTU attribute specifies the maximum number of bytes the MAX can receive in a single packet on a PPP, Frame Relay, EU-UI, or EU-RAW link.

Usage: The default value is 1524. You should accept this default unless the device at the remote end of the link cannot support it. If the administrator of the remote network specifies that you must change this value, specify a number between 1 and 1524 (for a PPP, EU-UI, or EU-RAW link) or between 128 and 1600 (for a Frame Relay link).

Framed-Netmask (9)

Description: The Framed-Netmask attribute specifies a subnet mask for the caller at Framed-Address.

Usage: Specify an IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0. If you accept this default, the MAX assumes a default subnet mask based on the class of the address, as shown in Table 9-16.

Table 9-16.IP address classes and default subnet masks

Class	Address range	Network bits
Class A	0.0.0.0 → 127.255.255.255	8
Class B	128.0.0.0 → 191.255.255.255	16
Class C	192.0.0.0 → 223.255.255.255	24
Class D	224.0.0.0 → 239.255.255.255	N/A
Class E (reserved)	240.0.0.0 → 247.255.255.255	N/A

See Also: "Framed-Address (8)" on page 9-93

Framed-Protocol (7)

Description: The Framed-Protocol attribute specifies the type of framed protocol the link can use. When you set this attribute, the link cannot use any other type of framed protocol.

This attribute can appear in both an Access-Request and Access-Accept packet. However, it does not appear in an Access-Request packet if Auth Send Attr 6, 7=No in the Ethernet> Mod Config>Auth menu.

Usage: Table 9-17 lists the values you can specify for Framed-Protocol.

Table 9-17.Framed-Protocol settings

Setting	Incoming call	Outgoing call
PPP (1)	A user requesting access can dial in using Multilink Protocol Plus (MP+), Multilink Protocol (MP), or Point-to-Point Protocol (PPP) framing. A user requesting access can also dial in unframed, and then change to PPP framing. If the user dials in using any other type of framing, the MAX rejects the call.	Outgoing calls use PPP framing.
SLIP (2)	A user requesting access can dial in unframed and change to SLIP framing. SLIP requires that a user dial in without using a framed protocol before changing to SLIP.	This value does not apply to outgoing calls.
MPP (256)	This value does not apply to incoming calls.	Outgoing calls request MP+ framing.
EURAW (257)	A user requesting access can dial in using EU-RAW framing. EU-RAW is a type of X.75 encapsulation in which IP packets are HDLC encapsulated with a CRC field. If the user dials in using any other type of framing, the MAX rejects the call.	Outgoing calls use EU-RAW framing.
EUUI (258)	A user requesting access can dial in using EU-UI framing. EU-UI is a type of X.75 encapsulation in which IP packets are HDLC encapsulated with a CRC field and a small header. If the user dials in using any other type of framing, the MAX rejects the call.	Outgoing calls use EU-UI framing.
COMB (260)	A user requesting access can dial in using Combinet framing. If the user dials in using any other type of framing, the MAX rejects the call.	Outgoing calls use Combinet framing.
FR (261)	This value does not apply to incoming calls.	Outgoing calls use Frame Relay (RFC 1490) framing.
ARA (262)	A dial-in user can establish an AppleTalk Remote Access (ARA) connection to the Ethernet network.	This value does not apply to outgoing calls.

Table 9-17.Framed-Protocol settings (continued)

Setting	Incoming call	Outgoing call
FR-CIR (263)	This value specifies a Frame Relay circuit.	This value specifies a Frame Relay circuit.

Note: By default, the MAX does not limit the protocols a link can access.

Dependencies: What Framed-Protocol does depends on how you set User-Service:

- If User-Service=Framed-User or is unspecified, a user requesting access can dial in using the framing specified by Framed-Protocol.

  The MAX rejects other types of framing. A user requesting access can also dial in without using a framed protocol, but can then change to the framing specified by the Framed-Protocol attribute.
- If 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 allowed on the outgoing call.

Example: The dial-in user in this example can use only PPP protocols (PPP, MP+, or MP), and cannot use the terminal server:

```
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
```

The dial-in user in this example establishes an ARA connection to the Ethernet network:

```
Ascend Password="Pipeline"
       User-Service=Framed-User,
       Framed-Protocol=ARA,
       Ascend-Idle-Limit=30,
       ...
```

Framed-Route (22)

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

Usage: The Framed-Route attribute has this format:

```
Framed-Route="host_ipaddr[/subnet_mask] gateway_ipaddr metric
[private] [name] [preference]"
```

Table 9-18 describes each Framed-Route argument.

Table 9-18.Framed-Route arguments

Syntax element	Description
host_ipaddr/*subnet_mask*	Indicates the IP address of the destination host or subnet reached by this route. If the address includes a subnet mask, the remote router specified by ***router_ipaddr*** is a router to that subnet, rather than to a whole remote network. To specify the entire remote network, do not specify a subnet mask.
router_ipaddr	Specifies the IP address of the router at the remote end of the connection. The 0.0.0.0 address is a wildcard entry that the MAX replaces with the caller’s IP address.When RADIUS authenticates a caller and sends the MAX an Access-Accept message with a Framed-Route 0.0.0.0 router, the MAX updates its routing tables with the Framed-Route value, but substitutes the caller’s IP address for the router. This setting is especially useful when RADIUS cannot know the IP address of the caller because the IP address comes from an address pool.
metric	Indicates the metric for this route. If the MAX has more than one possible route to a destination network, it chooses the one with the lower metric.
private	Specifies **y** if this route is private, or **n** if it is not private. If you specify that the route is private, the MAX does not disclose the existence of the route when queried by RIP or another routing protocol.
name	Indicates the name outgoing user profile that uses the route.
preference	Specifies the preference the MAX assigns to the route. Routes with lower preferences have priority over identical metrics with higher preferences.

Dependencies: Each static route must appear in a pseudo-user profile. You create a pseudo-user to store information that the MAX can query—in this case, in order to store IP routing information. You can configure pseudo-users for both global and MAX-specific configuration control of IP dialout routes. The MAX loads the unit-specific dialout routes in addition to the global dialout routes.

For a unit-specific IP dialout route, specify the first line of a pseudo-user profile in this format:

```
Route-unit_name-num Password="Ascend", User-Service=Dialout-Framed-
User
```

For a global IP dialout route, specify the first line of a pseudo-user profile in this format:

```
Route-num Password="Ascend", User-Service=Dialout-Framed-User
```

unit_name is the system name of the MAX—that is, the name specified by the Name parameter in the System profile. ***num*** is a number in a sequential series, starting at 1.

In each pseudo-user profile, you can specify one or more routes using the Framed-Route attribute. You should limit each pseudo-user profile to about 25 routes. The MAX fetches information from each profile in order to initialize its routing table. Whenever you power on or reset the MAX, or when you select the Upd Rem Cfg command from the Sys Diag menu, RADIUS adds IP dialout routes to the routing table in this way:

1 RADIUS looks for profiles having the format Route-***unit_name***-1, where ***unit_name*** is the system name.

2 If at least one profile exists, RADIUS loads all existing profiles having the format Route-***unit_name***-***num*** to initialize the IP routing table.

The variable ***num*** is a number in a sequential series, starting with 1.

3 The MAX queries Route-***unit_name***-1, then Route-***unit_name***-2, and so on, until it receives an authentication reject from RADIUS.

4 RADIUS loads the global configuration profiles.

These configurations have the form Route-***num***.

5 The MAX queries Route-1, then Route-2, and so on, until it receives an authentication reject from RADIUS.

The routes remain in effect until the next restart or until overwritten by dynamic updates or routes specified in Connection profiles.

Note: In some cases, you might wish to update the MAX unit's routing tables when connecting to a user whose profile specified User-Service=Framed-User. In this case, you can set the Framed-Route attribute in an incoming user profile to specify the user's IP address and subnet mask in the ***host_ipaddr*** and ***subnet_mask*** arguments, respectively. The route you specify in this manner exists only during the time the call is online. When you also enter a nonzero router address for ***router_ipaddr*** that is different from the caller's address, the static route of a dial-in framed-user persists even after the connection goes offline.

Example: This example shows two RADIUS pseudo-user profiles defining global static IP routes:

```
Route-1   Password="Ascend", 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 "
```

See Also: "Ascend-Route-IP (228)" on page 9-80

Framed-Routing (10)

Description: The Framed-Routing attribute specifies whether the MAX sends Routing Information Protocol (RIP) packets, receives RIP packets, or both.

If you enable RIP to both send and receive RIP updates on the WAN interface, the MAX broadcasts its routing table to the remote network and listens for RIP updates from that network. Gradually, all routers on both networks have consistent routing tables (all of which may become quite large).

Usage: You can specify one of these values:

- None (0) indicates that the MAX does not send or receive RIP updates.

  None is the default. Many sites turn off RIP on the WAN interface in order to avoid storing very large local routing tables. If you turn off RIP, the MAX does not listen to RIP updates across the connection. To route to other networks through that connection, the MAX must rely on static routes specified in a pseudo-user profile. For details, see
- Broadcast (1) indicates that the MAX sends RIP version 1 updates, but does not receive them.
- Listen (2) indicates that the MAX receives RIP version 1 updates, but does not send them.
- Broadcast-Listen (3) indicates that the MAX both sends and receives RIP version 1 updates.
- Broadcast-v2 (4) indicates that the MAX sends RIP version 2 updates, but does not receive them.
- Listen-v2 (5) indicates that the MAX receives RIP version 2 updates, but does not send them.
- Broadcast-Listen-v2 (6) indicates that the MAX both sends and receives RIP version 2 updates.

See Also: "Ascend-Route-IP (228)" on page 9-80

Login-Host (14)

Description: The Login-Host attribute specifies the IP host to which the user automatically connects when you set User-Service=Login-User and specify a value for the Login-Service attribute. Access begins immediately after login.

Usage: Specify an IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0. 0.0.This setting specifies that the Login-User does not automatically connect to a particular host.

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, he or she can only gain access to the hosts listed by the Ascend-Host-Info attribute.

Dependencies: When User-Service=Framed-User, RADIUS ignores the Login-Host attribute.

See Also: "Login-Service (15)" on page 9-101

Login-Service (15)

Description: The Login-Service attribute specifies the type of terminal service connection to an IP host that occurs immediately after authentication.

Usage: Specify one of these values:

- Telnet (0)

  The user immediately establishes a Telnet session with the host specified by the Login-Host attribute.
- Rlogin (1)

  The user immediately establishes an Rlogin session with the host specified by the Login-Host attribute.
- TCP-Clear (2)

  This setting specifies a TCP/IP connection with no Telnet protocol. TCP-Clear establishes a TCP session between the MAX and the host specified by Login-Host over which the user can run an application specified by Login-TCP-Port.

  If you specify this setting, the TCP-Clear must be set to Yes in the Ethernet>Answer> Encaps menu.

When you set the Login-Service attribute, a dial-in terminal server user makes an immediate connection to an IP host on your local network and never sees the terminal server interface.

By default, the MAX does not grant immediate access to an IP host.

Dependencies: Keep this additional information in mind:

- If you specify both Login-Service and Login-Host, 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 unit’s terminal server command-line interface or the terminal server menu interface, depending upon how you configure the MAX.

Example: In this example, an Rlogin session starts automatically for anyone using the Userx user name and xyzzy password. When the session terminates, the connection also terminates.

```
# This profile causes an auto-rlogin to 10.0.200.4 upon login.
Userx  Password="xyzzy"
       User-Service=Login-User,
       Login-Service=Rlogin,
       Login-Host=10.0.200.4
```

Further, when you specify the following settings, a raw TCP session starts automatically for anyone using the User1 user name 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
```

See Also: “Login-Host (14)” on page 9-100
“Login-TCP-Port (16)” on page 9-102

Login-TCP-Port (16)

Description: The Login-TCP-Port attribute specifies the port number to which a TCP session connects when Login-Service=TCP-Clear in a user profile.

Usage: Specify an integer between 1 and 65535. The default value is 23.

See Also: “Login-Service (15)” on page 9-101

NAS-Identifier (4)

Description: The NAS-Identifier attribute indicates the IP address of the MAX. When the MAX sends an Access-Request packet or Ascend-Event-Request packet, it indicates its IP address to the RADIUS server using this attribute.

Usage: In most cases, you never need to specify the NAS-Identifier attribute in a user profile.

However, you might want to specify it if multiple MAX units use a single RADIUS server, and you want to specify the MAX to which a particular user can connect. In this case, the NAS-Identifier value in the Access-Request packet and the NAS-Identifier value in the user profile must match for the RADIUS server to authenticate the connection.

Specify an IP address in dotted decimal notation *n.n.n.n/nn*, where *n* is an integer between 0 and 255, and *nn* is a subnet mask between 8 and 32. The default value is 0.0.0.0/0. The NAS-Identifier value must appear in the first line of the user profile.

Example: Suppose that the user Emma is allowed to dial into the MAX at IP address 200.65.212.46. The first line of the user profile might look like this one:

```
Emma Password="pwd", NAS-Identifier=200.65.212.46
```

NAS-Port (5)

Description: The NAS-Port attribute identifies the network interface and service the session is using. The MAX sends this attribute to the RADIUS server in an Access-Request packet and an Accounting-Request packet.

Usage: You can specify two formats, one restricting the dial-in user to a service, line, and channel, and one restricting the dial-in user to a slot, line, and channel.

1 To restrict a user to a service, line, and channel,

Specify NAS-Port in the first line of the user profile using this format :

```
service line channel
```

- ***service*** can have the value 1 for a digital call, or 2 for an analog call.

  An analog call is one that a modem on the MAX has processed. A value of 1 does not imply that the caller logged in through the MAX unit’s terminal server.
- ***line*** consists of two digits that specify the line number the call is using.
- ***channel*** consists of two digits that represent the channel on the line the call is using.

The incoming authentication request must match the NAS-Port setting. The default value is 0 (zero).

2 To restrict a dial-in user to a shelf, slot, line, and channel, enter a value in the following format:

`FF SSSS LLLLL CCCCC`

`For an ISDN call:`

- **`FF`** specifies the shelf number (always 0 in RADIUS, 1 on the MAX)
- **`SSSS`** specifies the slot number (0–15)
- **`LLLLL`** specifies the line number (0–31)
- **`CCCCC`** specifies the channel number (0–31)

For an analog call, the values are the same, except that the line number can be 0–63, and the channel number is always 1.

Because the value you enter is zero-based, you must add 1 to each component to ascertain the actual slot, line, and channel number. The RADIUS daemon converts the NAS-Port number to decimal on most systems.

Example: To restrict a dial-in user to analog service on line 1, set up a user profile like this one:

```
Dave Password="password", NAS-Port=20100
  User-Name="Dave",
  User-Service=Framed-User,
  Framed-Protocol=PPP,
  Ascend-Assign-IP-Pool=1,
  Ascend-Route-IP=1,
  Ascend-Idle-Limit=300,
  Framed-Routing=None
```

To restrict a dial-in user to channel 10 on line 2 for slot 1, set up a user profile like this one:

```
Robin Password="password", NAS-Port=1098
  User-Service=Framed-User,
  Framed-Protocol=PPP,
  Ascend-Assign-IP-Pool=1,
  Ascend-Route-IP=1,
  Ascend-Idle-Limit=300,
  Framed-Routing=None
```

The value NAS-Port=1098 translates to the following NAS port:

- ***`FF`***=shelf 0
- ***`SSSS`***=slot 1
- ***`LLLLL`***=line 2
- ***`CCCCC`***=channel 10

NAS-Port-Type (61)

Description: The NAS-Port-Type attribute indicates the type of physical port the MAX is using to authenticate the client. The NAS-Port-Type attribute appears in RADIUS Start, Stop, and Checkpoint messages.

Some ISPs offer different levels of service based on connection type. To prevent a client from using a capability to which he or she has not subscribed, set the NAS-Port-Type attribute to an appropriate value.

Usage: You can specify one of these settings:

- Async indicates a call routed to a digital modem.
- Sync indicates a non-ISDN synchronous connection, such as a Switched-56K connection.
- ISDN-Sync indicates a synchronous ISDN connection.
- ISDN-Async-v120 indicates an ISDN connection using V.120 asynchronous rate adaption.
- ISDN-Async-v110 indicates an ISDN connection using V.110 asynchronous rate adaption.
- Virtual indicates a connection to the MAX using a transport protocol instead of a physical port.

See Also: “NAS-Port (5)” on page 9-102

Password (2)

Description: The Password attribute specifies the password of the calling device or dial-in user in a user profile.

Usage: Specify an alphanumeric string containing up to 252 characters. The default value is null. The Password attribute must appear on the first line of the user profile. You can make any of these specifications:

- A static password

  For example, consider this first line in a user profile:

  Emma Password="Pwd"

  The user called Emma must specify the password Pwd in order to gain access to the MAX.

- UNIX

  You can request validation using the /etc/password file on the UNIX host by setting the Password attribute to UNIX, as shown in this first line of a user profile:

  John Password="UNIX"

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

- SAFEWORD

  You can request validation using the Enigma Logic SafeWord dynamic password library by setting the Password attribute to SAFEWORD, as shown in this first line of a user profile:

  Mike Password="SAFEWORD"

- ACE

  You can request validation using the Security Dynamics ACE dynamic password library by setting the Password attribute to ACE, as shown in this first line of a user profile:

  Connor Password="ACE"

- Ascend-CLID

  You can require RADIUS to authenticate incoming calls by checking the calling party's phone number. When you do so, you set the Password attribute to Ascend-CLID, as shown in this first line of a user profile:

  5551212 Password="Ascend-CLID"

- Ascend-DNIS

  You can require RADIUS to authenticate incoming calls by checking the called number. When you do so, you set the Password attribute to Ascend-DNIS, as shown in this first line of a user profile:

  5551212 Password="Ascend-DNIS"

See Also: "Ascend-Ara-PW (181)" on page 9-7

Reply-Message (18)

Description: The Reply-Message attribute carries message text from a RADIUS server to RADIUS clients such as the MAX under these two circumstances:

- In a pseudo-user profile that configures message text and a list of IP hosts, the Reply-Message attribute specifies text that appears to the terminal server operator who is using the menu-driven interface.
- If the RADIUS server determines that the MAX should terminate the session, it sends an Access-Terminate-Session packet containing the Reply-Message attribute.

Usage: Specify a text string containing up to 80 characters. The default value is null. You can specify up to 16 Reply-Message attributes in a pseudo-user profile.

Dependencies: Keep this additional information in mind:

- An Access-Terminate-Session packet is a RADIUS packet identified by the code number 31.

  Only RADIUS daemons you customize to support this packet code can send an Access-Terminate-Session packet. Neither the Ascend RADIUS daemon nor the Livingston RADIUS daemon supports this packet type. This packet can include only one attribute—the Reply-Message attribute—and this attribute can specify up to 80 characters of text.

  When the MAX receives an Access-Terminate-Session packet, it starts a timer, displays any Reply-Message included in the packet, and terminates the session. For example, if a user's bill is past due, the Access-Terminate-Session packet could include the message `Emma, you have not paid your connect charges.`
- If you do not specify a Reply-Message attribute in a user profile that authenticates callers, and the RADIUS server sends an Access-Accept packet, no message appears.
- If the RADIUS server sends an Access-Reject packet and you do not specify a Reply-Message attribute in a customized RADIUS daemon, this message appears:

  ```
  ** Bad Password
  ```

  The MAX then allows the user two additional attempts to enter the correct password. If the user does not supply the correct password in three attempts, the MAX terminates the session.
- If the RADIUS server sends an Access-Terminate-Session packet and you do not specify a Reply-Message attribute in a customized RADIUS daemon, the MAX displays this message to the terminal server user:

  ```
  ** Session Terminated
  ```

The MAX then uses a timer to terminate the login session. The RADIUS server discards all input it received before it terminated the session.

Example: Here is an example of a pseudo-user profile setting up message text for a MAX named Cal:

```
Initial-Banner-Cal Password="Ascend", User-Service=Dialout-Framed-User
     Reply-Message="Up to 16 lines of up to 80 characters each",
     Reply-Message="will be accepted. Long lines will be truncated",
     Reply-Message="Additional lines will be ignored.",
     Reply-Message="",
```

Ascend-Host-Info="1.2.3.4 Berkeley",

Ascend-Host-Info="1.2.3.5 Alameda",

Ascend-Host-Info="1.2.36 San Francisco",

...

See Also: "Ascend-Host-Info (252)" on page 9-54

Tunnel-Client-Endpoint (Attribute 66)

Description: A string assigned by RADIUS that specifies the name for the unit placing the call. This is used by RADIUS accounting for tracking the session.

Dependencies: Keep this additional information in mind:

- DNIS or CLID must be enabled in the Id Auth parameter of Ethernet Answer profile.
- The MAX must have RADIUS user entries that specify DNIS or CLID.

See Also: Client-Port-DNIS (Attribute 30), used for Called Number authentication.

Tunnel-ID (Attribute 68)

Description: String assigned by RADIUS to each session using CLID or DNIS tunneling. This value is used for accounting when accounting is implemented.

Dependencies: Keep this additional information in mind:

- DNIS or CLID must be enabled in the Id Auth parameter of Ethernet Answer profile.
- The MAX must have RADIUS user entries that specify DNIS or CLID.

See Also: Client-Port-DNIS (Attribute 30), used for Called Number authentication.

Tunneling-Protocol (127)

Description: The Tunneling-Protocol attribute indicates if a session used the ATMP tunneling protocol.

Usage: Specify ATMP if the connection uses the ATMP tunneling protocol.

Example: The following is an example of a RADIUS accounting record with the Tunneling-Protocol attribute.

```
Mon Apr 21 02:41:38 1997
        User-Name = "JacobP75"
        NAS-Identifier = 1.1.1.1
        NAS-Port = 10105
        Acct-Status-Type = Stop
        Acct-Delay-Time = 0
        Acct-Session-Id = "111111111"
        Acct-Authentic = RADIUS
        Acct-Session-Time = 0
        Acct-Input-Octets = 215
        Acct-Output-Octets = 208
        Acct-Input-Packets = 10
        Acct-Output-Packets = 10
        Ascend-Disconnect-Cause = 1
        Ascend-Connect-Progress = 60
        Ascend-Data-Rate = 56000
        Ascend-PreSession-Time = 1
        Ascend-Pre-Input-Octets = 215
        Ascend-Pre-Output-Octets = 208
        Ascend-Pre-Input-Packets = 10
        Ascend-Pre-Output-Packets = 10
        Framed-Protocol = PPP
        Framed-Address = 2.2.2.2
        Tunneling-Protocol = ATMP
```

Dependencies: The Tunneling-Protocol attribute is sent in Accounting-Request packets at the end of a session under the following conditions:

- The Accounting -Request packet has Acct-Status-Stop
- The session was authenticated and encapsulated using the ATMP tunneling protocol.

Tunnel-Medium-Type (Attribute 65)

Description: Specifies the transport medium over which the encapsulated traffic is carried (tunneled).

Usage: Tunnel-Medium-Type can have the following values

- IP
- X25 (not yet supported)
- ATM (not yet supported)

Dependencies: Keep this additional information in mind:

- DNIS or CLID must be enabled in the Id Auth parameter of Ethernet Answer profile.
- The MAX must have RADIUS user entries that specify DNIS or CLID.

See Also: Client-Port-DNIS (Attribute 30), used for Called Number authentication.

Tunnel-Server-Endpoint (67)

Description: Specifies the fully-qualified host name or IP address of the network server to contact for building a tunnel. If you set Tunnel-Type to L2TP, Tunnel-Server-Endpoint indicates the IP address of the LNS. If you set Tunnel-Type to PPTP, Tunnel-Sever-Endpoint indicates the IP address of the PNS.

Usage: Specify the primary home agent in the following format:

```
Tunnel-Server-Endpoint="hostname | ip_address"
```

where:

- *hostname* is the fully-host name of the network server.
- *ip_address* is the network server's IP address in dotted decimal notation.
  Specify an IP address if the network server does not have access to a DNS server.

You can specify a host name or IP address, but not both.

Example: To specify the network server maxSF.home.com at IP address 10.10.10.10, specify one of the following lines in the RADIUS user profile:

```
Tunnel-Server-Endpoint=10.10.10.10
```

```
Tunnel-Server-Endpoint=maxSF.home.com
```

Dependencies: For the MAX to correctly create an L2TP tunnel, you must set Tunnel-Type to L2TP and Tunnel-Medium-Type to IP, in addition to specifying the IP address of an accessible LNS.

For the MAX to correctly create an PPTP tunnel, you must set Tunnel-Type to PPTP and Tunnel-Medium-Type to IP, in addition to specifying the IP address of an accessible PPTP Network Server (PNS).

See Also: Tunnel-Type (64), Tunnel-Medium-Type (65)

Tunnel-Type (64)

Description: Specifies the type of tunneling protocol to create.

Usage: You can specify the following values for Tunnel-Type:

- PPTP
- L2TP

Example: Tunnel-Type=L2TP

Dependencies: For the MAX to correctly create an L2TP tunnel, you must set Tunnel-Medium-Type to IP and set Tunnel-Server-Endpoint to the IP address of an accessible LNS, in addition to setting Tunnel-Type to L2TP.

For the MAX to correctly create an PPTP tunnel, you must set Tunnel-Medium-Type to IP and set Tunnel-Server-Endpoint to the IP address of an accessible PNS, in addition to setting Tunnel-Type to PPTP.

See Also: Tunnel-Medium-Type (65), Tunnel-Server-Endpoint (67)

User-Name (1)

Description: The User-Name attribute can specify one of the following in a user profile:

- The name of the calling device or dial-in user.
- The keyword Default.

  If you create a profile with the user name Default and make that profile the *last profile* of the users file, the RADIUS server will use that profile to determine what to do with users who are not in the users file. You can configure only one Default profile in the users file.
- The incoming phone number (for CLID authentication).
- The called number (for called-number authentication).
- The name of a pseudo-user profile.

  You can set up a pseudo-user profile to configure outgoing calls, a pool of dynamic IP addresses, static IP and IPX routes, bridge entries, and the message text and host list for the terminal server interface.

Usage: Specify an alphanumeric string containing up to 252 characters. The default value is null. The user name must be the first word in a user profile. You need not specify the name of the attribute.

Example: For example, consider this first line in a user profile:

```
Emma Password="pwd", Ascend-PW-Expiration="January 30 1997"
```

The user name is Emma. The RADIUS server tests the user’s name and password against the values the user provides when making a request for access. If the RADIUS server does not find a match, it denies the request for access.

Here is a sample user profile for CLID authentication using the incoming phone number as the User-Name:

```
5551212  Password="Ascend-CLID"
         Ascend-Require-Auth=Not-Require-Auth,
         User-Service=Framed-User,
         Framed-Protocol=PPP,
         Framed-Address=255.255.255.254,
         Framed-Netmask=255.255.255.255,
         Ascend-Assign-IP-Pool=1,
         Ascend-Route-IP=Route-IP-Yes,
         Ascend-Idle-Limit=30
```

Finally, this example shows User-Name in a pseudo-user profile for a static route:

```
Route-1 Password="Ascend", User-Service=Dialout-Framed-User
        Framed-Route="10.4.5.0/22 10.9.8.10 1 n inu-out"
```

User-Service (6)

Description: The User-Service attribute specifies the type of services the link can use.

If RADIUS authenticates an incoming call using the User-Name and Password attributes, and the type of call matches the value of the User-Service attribute, the MAX applies the attributes in the user profile to the call. If the type of call does not match the User-Service attribute, the MAX rejects the call.

This attribute can appear in both an Access-Request and Access-Accept packet. However, it does not appear in an Access-Request packet if Auth Send Attr 6, 7=No in the Ethernet> Mod Config>Auth menu.

Usage: You can specify one of these values:

- Login-User (1)

  The operator can use an asynchronous Telnet connection to log into the terminal server. The MAX rejects incoming framed calls. The operator cannot use any framed protocol, but can start Telnet or raw TCP sessions.
- Framed-User (2)

  Incoming calls must use a framed protocol. Otherwise, the MAX rejects them. Asynchronous Telnet sessions are unframed and therefore not allowed when you specify this value.
- Dialout-Framed-User (5)

  The MAX can use this profile for outgoing calls only. The MAX sends this value to the RADIUS server during an authentication request.

By default, the MAX does not limit the services the link can access.

Dependencies: Keep this additional information in mind:

- Login-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 or X.75 encapsulated.
- Asynchronous Telnet sessions are unframed and therefore not allowed when you set User-Service=Framed-User.

Troubleshooting

A

This appendix presents strategies for how to diagnose and resolve problems that may occur when you set up and use the MAX with RADIUS. This appendix contains:

RADIUS authentication problems

General authentication failures

If RADIUS is not properly authenticating dial-in users, follow these steps to pinpoint the source of the problem:

1 To isolate the problem to the RADIUS server, try to authenticate a user with a local Connection profile.

If the Connection profile authenticates the user, you can feel certain that your RADIUS configuration is the source of the problem.

2 In the Ethernet > Mod Config > Auth menu, check the settings for these parameters:

– Auth. You must set this parameter to RADIUS or RADIUS/LOGOUT.

– Auth Host #*n*. This parameter must indicate the correct IP address of the RADIUS server.

– Auth Port. This parameter must indicate the RADIUS daemon's authentication port as specified in the /etc/services file.

– Auth Key. This parameter must indicate the MAX unit's password as specified in the /etc/raddb/clients file. If the accounting process of the daemon is running on the same server as the authentication process (rather than on a separate host), the Acct Key parameter in the Ethernet > Mod Config > Accounting must specify the same password as the Auth Key parameter.

3 Check these settings in the MAX configuration interface:

– The Name parameter in the System profile must indicate the MAX unit's name as specified in the /etc/raddb/clients file. Verify that the IP address of the MAX can be resolved from the name.

– In the Ethernet > Answer menu, you must set Profile Reqd=Yes.

- If you are using PAP, CHAP, or MS-CHAP authentication of incoming PPP, MP, and MP+ calls, you must set Recv Auth to the appropriate value in the Ethernet > Answer > PPP Options menu.
- If you want modem callers to dial into the terminal server, you must set Security=Full in the Ethernet > Mod Config > TServ Options menu.

4 Make sure that you have copied all these files into the /etc/raddb directory:

- dictionary
- users
- clients

5 Verify that you are using the latest version of the Ascend RADIUS daemon.

6 Confirm that there are no syntax errors in the user profile.

7 To isolate the source of the problem, run the RADIUS daemon in debug mode by entering one of these commands:

`radiusd -x` (for the flat ASCII users file)

`radiusd.dbm -x` (for the DBM database)

8 Confirm whether all users are failing authentication.

If all modem users can connect except for users on a particular platform, contact Ascend technical support for assistance.

9 If you are using the HPUX platform, problems may occur when you compile RADIUS with the proprietary compiler.

Try to use a gcc compiler instead.

10 Keep this additional information in mind:

- Authentication using the /etc/passwd file (with the UNIX keyword) is incompatible with CHAP. For a user dialing in with CHAP, you must specify a static password in the user profile.
- A comma must appear at the end of every line in a user profile except the first and last lines.
- The Default profile in the users file must be the last entry in the file.
- You need not restart the RADIUS daemon every time you add an entry to the users file.
- You must restart the RADIUS daemon if you modify the clients file.
- You need only specify an attribute in a user profile when you want to change the value from its default setting.

Checking the logfile

RADIUS writes error messages to /etc/raddb/logfile. The Syslog daemon does not create the RADIUS log file, so you must create the file yourself. Table A-1 provides a partial list of error messages.

Table A-1. Error messages

Message	Description
CALC_DIGEST	The clients file contains an incorrect entry. Or, the name of the MAX is correct, but the RADIUS server is unable to resolve the IP address from the name you specified.
DICT_VAL_FIND	In a user profile, you specified a setting that the dictionary does not support. This error could signal a simple misspelling or a syntax error.
BAD AUTHENTICATOR	You might have specified an incorrect password in the clients file, or in the value of the Auth Key parameter in the Ethernet > Mod Config > Auth menu.
CHAP UNIX FAILURE	You can use the UNIX password only with PAP authentication. In a user profile, the setting Password= “UNIX” causes RADIUS to use the /etc/passwd file for authentication.
WRONG NAS ADDRESS	The entry in the clients file may have the incorrect IP address for the MAX. Or, the RADIUS server may be unable to resolve the IP address from the name of the MAX in the clients file. To resolve this error, specify the correct IP address of the MAX in the clients file.

RADIUS accounting problems

General accounting failures

If RADIUS is not properly providing accounting information, follow these steps to pinpoint the source of the problem:

1 Make sure that the RADIUS daemon is running with the –A option enabled.

– The -A option specifies that the RADIUS daemon creates the accounting process.

If you are using a flat ASCII users file, start the RADIUS daemon with the -A option by entering this command:

```
radiusd -A services | incr
```

When you specify the **services** argument, the daemon creates the accounting process only if a line defining the UDP port to use for accounting appears in the /etc/services file. Otherwise, the daemon does not start.

When you specify the **incr** argument, the daemon creates the accounting process with the UDP port specified as the accounting port in the /etc/services file. If you have not defined the port, the daemon increments the UDP port specified for radiusd and uses that port number. This action is the default when you do not specify the -A argument.

- If you are using a DBM database, start the RADIUS daemon with the -A option by entering this command:

```
radiusd.dbm -A services
```

You must specify the **`services`** argument when you start the daemon in DBM mode.

2 Check to see that the /usr/adm/radacct directory exists.

If it does not exist, you can perform either of these tasks:

- Create the /usr/adm/radacct directory.
- Use the –a option when starting the daemon, and 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 in the directory you specify using the -a option. The *detail* file contains accounting records.

3 In the Ethernet > Mod Config > Auth menu, make sure that Auth=RADIUS.

Accounting is available only with RADIUS authentication. It is not available when Auth=None, TACACS, or RADIUS/LOGOUT.

4 In the Ethernet > Mod Config > Accounting menu, check the settings of these parameters:

- Acct: You must set this parameter to RADIUS.
- Acct Host #*n*. For this parameter, you must specify the IP address of the RADIUS host.
- Acct Port. For this parameter, you must indicate the UDP port number you specified for the accounting process of the daemon in /etc/services. Or, if you used the **`incr`** keyword for the –A option when starting the daemon, you must specify the number of the UDP port for authentication services + 1.
- Acct Key. For this parameter, you must indicate the RADIUS client password exactly as it appears in the RADIUS clients file.
- Sess Timer. The MAX can report the number of sessions by class to a RADIUS accounting server. The Sess Timer parameter specifies the interval in seconds in which the MAX sends session reports. You can specify a number between 0 and 65535. The default value is 0 (zero), which indicates that the MAX does not send reports on session events.

Duplicate or deleted records

If the MAX sends an authentication packet to the RADIUS server and does not receive an acknowledgment from the RADIUS daemon within the time specified by the Auth Timeout parameter in the Ethernet > Mod Config > Auth menu, it resends the packet. Because RADIUS did not see the original packet, it reports the resent packet as a duplicate. This message appears on the console:

```
Dropping duplicate from MAX, id=num
```

This message can also appear if the MAX sends an accounting request to the RADIUS server and does not receive an acknowledgment from the RADIUS daemon within the time specified by the Acct Timeout parameter in the Ethernet > Mod Config > Accounting menu. Delays in the link between the MAX and the RADIUS server can cause these duplications. In addition, these delays can cause accounting records to be lost when the MAX unit's accounting buffer overflows.

These devices can cause delays in the link between the MAX and the RADIUS server:

- An intermediate router or other communication device that stores accounting request packets
- A busy accounting server

Backoff queue error message

The accounting server stores unacknowledged records in the backoff queue. If the unit never receives an acknowledgment to an accounting request, it will eventually run out of memory. In order to keep this situation from occurring, the unit deletes the accounting records and displays this error message:

```
Backoff Q full, discarding user username
```

This error generally occurs for one of two reasons:

- You enabled RADIUS accounting on the MAX, but not on the RADIUS server.
- You are using the Livingston server instead of the Ascend server.

Understanding V.110 module call status information

The MAX supports V.110 module call status information for RADIUS accounting. Table A-2 lists the V.110 call status values for RADIUS attributes for each channel/ITAC in each V.110 interface card.

Table A-2. V.110 call status values

Value	Description
DisconnectReasonType (Ascend-Disconnect-Cause attribute)	DIS_V110_TIMEOUT=160—This value specifies the number of retries for timeouts and resynchronization over MAX_V110_RETRIES.
ProgressType (Ascend-Connect-Progress attribute)	PR_V110_UP=90—A V.110 connection is up. PR_V110_STATE_OPENED—An open has been issued, but the MAX has not yet synched up with the remote end. PR_V110_STATE_CARRIER—The remote end detected a carrier. PR_V110_STATE_RESET—The V.110 connection has reset. PR_V110_STATE_CLOSED—The V.110 connection has closed.

Table A-2. V.110 call status values (continued)

Value	Description
AcctEventType	ACCT_EVNT_V110_BAUD—This value supports the V.110 baud rate, and works exactly like ACCT_EVNT_MODEM_BAUD.

Connect progress codes

The Ascend-Connect-Progress attribute specifies the state of the connection before it is disconnected. The MAX includes Ascend-Connect-Progress in an Accounting-Request packet when both of these conditions are true:

- The session has ended or has failed to authenticate (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Ascend-Connect-Progress can have any one of values specified in Table A-3.

Table A-3. Ascend-Connect-Progress codes

Code	Explanation
0	No progress.
1	Not applicable.
2	The progress of the call is unknown.
10	The call is up.
30	The modem is up.
31	The modem is waiting for DCD.
32	The modem is waiting for result codes.
40	The terminal server session has started up.
41	The MAX is establishing the TCP connection.
42	The MAX is establishing the immediate Telnet connection.
43	The MAX has established a raw TCP session with the host. This code does not imply that the user has logged into the host.
44	The MAX has established an immediate Telnet connection with the host. This code does not imply that the user has logged into the host.
45	The MAX is establishing an Rlogin session.
46	The MAX has established an Rlogin session with the host. This code does not imply that the user has logged into the host.

Table A-3. Ascend-Connect-Progress codes (continued)

Code	Explanation
60	The LAN session is up.
61	LCP negotiations are allowed.
62	CCP negotiations are allowed.
63	IPNCP negotiations are allowed.
64	Bridging NCP negotiations are allowed.
65	LCP is in the Open state.
66	CCP is in the Open state.
67	IPNCP is in the Open state.
68	Bridging NCP is in the Open state.
69	LCP is in the Initial state.
70	LCP is in the Starting state.
71	LCP is in the Closed state.
72	LCP is in the Stopped state.
73	LCP is in the Closing state.
74	LCP is in the Stopping state.
75	LCP is in the Request Sent state.
76	LCP is in the ACK Received state.
77	LCP is in the ACK Sent state.
80	IPXNCP is in the Open state.
90	V.110 is up.
91	V.110 is in the Open state.
92	V.110 is in the Carrier state.
93	V.110 is in the Reset state.
94	V.110 is in the Closed state.

Disconnect progress codes

The Ascend-Disconnect-Cause attribute specifies the reason a connection was taken offline. The MAX includes Ascend-Disconnect-Cause in an Accounting-Request packet when both of these conditions are true:

- The session has ended or has failed to authenticate (Acct-Status-Type=Stop).
- The Auth parameter is not set to RADIUS/LOGOUT.

Ascend-Disconnect-Cause can return any of the values listed in Table A-4.

Table A-4. Ascend-Disconnect-Cause codes

Code	Description
0	No reason.
1	The event was not a disconnect.
2	The reason for the disconnect is unknown. This code can appear when the remote connection goes down.
3	The call has disconnected.
4	CLID authentication has failed.
These codes can appear if a disconnect occurs during the initial modem connection.	
10	The modem never detected DCD.
11	The modem detected DCD, but became inactive.
12	The result codes could not be parsed.
These codes are related to immediate Telnet and raw TCP disconnects during a terminal server session.	
20	The user exited normally from the terminal server.
21	The user exited from the terminal server because the idle timer expired.
22	The user exited normally from a Telnet session.
23	The user could not switch to SLIP or PPP because the remote host had no IP address or because the dynamic pool could not assign one.
24	The user exited normally from a raw TCP session.
25	The login process ended because the user failed to enter a correct password after three attempts.
26	The raw TCP option is not enabled.
27	The login process ended because the user typed Ctrl-C.

Table A-4. Ascend-Disconnect-Cause codes (continued)

Code	Description
28	The terminal server session has ended.
29	The user closed the virtual connection
30	The virtual connection has ended.
31	The user exited normally from an Rlogin session
32	The user selected an invalid Rlogin option.
33	The MAX has insufficient resources for the terminal server session.
These codes concern PPP connections.	
40	PPP LCP negotiation timed out while waiting for a response from a peer.
41	There was a failure to converge on PPP LCP negotiations.
42	PPP PAP authentication failed.
43	PPP CHAP authentication failed.
44	Authentication failed from the remote server.
45	The peer sent a PPP Terminate Request.
46	LCP got a close request from the upper layer while LCP was in an open state.
47	LCP closed because no NCPs were open.
48	LCP closed because it could not determine to which MP bundle it should add the user.
49	LCP closed because the MAX could not add any more channels to an MP session.
These codes are related to immediate Telnet and raw TCP disconnects, and contain more specific information than the Telnet and TCP codes listed earlier in this table.	
50	The Raw TCP or Telnet internal session tables are full.
51	Internal resources are full.
52	The IP address for the Telnet host is invalid.
53	The MAX could not resolve the hostname.
54	The MAX detected a bad or missing port number.

Table A-4. Ascend-Disconnect-Cause codes (continued)

Code	**Description**
The TCP stack can return these disconnect codes during an immediate Telnet or raw TCP session.	
60	The host reset the TCP connection.
61	The host refused the TCP connection.
62	The TCP connection timed out.
63	A foreign host closed the TCP connection.
64	The TCP network was unreachable.
65	The TCP host was unreachable.
66	The TCP network was administratively unreachable.
67	The TCP host was administratively unreachable.
68	The TCP port was unreachable.
These are additional disconnect codes.	
100	The session timed out because there was no activity on a PPP link.
101	The session failed for security reasons.
102	The session ended for callback.
120	One end refused the call because the protocol was disabled or unsupported.
150	RADIUS requested the disconnect.
160	The allowed retries for V.110 synchronization have been exceeded.
170	PPP authentication has timed out.
180	The call disconnected as the result of a local hangup.
185	The call disconnected because the remote end hung up.
190	The call disconnected because the T1 line that carried it was quiesced.
195	The call disconnected because the call duration exceeded the maximum amount of time allowed by the Max Call Mins or Max DS0 Mins parameter on the MAX.

Attribute and Parameter Cross Reference

B

This appendix contains tables that cross reference RADIUS attributes and MAX parameters. This appendix contains:

Parameters and analogous attributes

Table B-1 cross references the Ascend RADIUS dictionary's attributes to parameters in the MAX unit's menu-driven user interface. The table is arranged by parameter in alphabetical order.

Table B-1. Parameters and analogous attributes

Profile	Parameter	Analogous attribute
Answer profile Connection profile (no attributes for COMB encapsulation)	Add Pers	Ascend-Add-Seconds
	Auth Req	Ascend-Require-Auth
	BACP	Ascend-BACP-Enable
	Base Ch Count	Ascend-Base-Channel-Count
	Bill #	Ascend-Billing-Number
	Bridge	Ascend-Bridge
	Callback	Ascend-Callback
	Call-by-Call	Ascend-Call-By-Call
	Called #	Client-Port-DNIS
	Calling #	Caller-Id
	Call Type	Ascend-Call-Type

Table B-1. Parameters and analogous attributes (continued)

Profile	Parameter	Analogous attribute
	CBCP Enable	Ascend-CBCP-Enable
	CBCP Mode	Ascend-CBCP-Mode
	CBCP Trunk Group	Ascend-CBCP-Trunk-Group
	Client Gateway	Ascend-Client-Gateway
	Circuit	Ascend-FR-Circuit-Name
	Data Svc	Ascend-Data-Svc
	DBA Monitor	Ascend-DBA-Monitor
	Dec Ch Cnt	Ascend-Dec-Channel-Count
	Dial #	Ascend-Dial-Number
	DLCI	Ascend-FR-DLCI
	Dyn Alg	Ascend-History-Weigh-Type
	Encaps=TCP-CLEAR	Login-Service=TCP-Clear
	Encaps submenu parameters in the Answer profile Encaps parameter in the Connection profile	Framed-Protocol
	Expect Callback	Ascend-Expect-Callback
	Force 56	Ascend-Force-56
	FR Direct	Ascend-FR-Direct
	FR DLCI	Ascend-FR-Direct-DLCI
	FR Prof	Ascend-FR-Direct-Profile
	Group	Ascend-Group
	Handle IPX	Ascend-Handle-IPX
	Idle	Ascend-Idle-Limit
	Idle Pct	Ascend-MPP-Idle-Percent
	IF Adrs	Ascend-Remote-Addr

Table B-1. Parameters and analogous attributes (continued)

Profile	Parameter	Analogous attribute
	Inc Ch Cnt	Ascend-Inc-Channel-Count
	IP Direct	Ascend-IP-Direct
	IPX Alias#	Ascend-IPX-Alias
	LAN Adrs	Framed-Address Framed-Netmask
	Link Comp	Ascend-Link-Compression
	Login Host	Login-Host
	Login Port	Login-TCP-Port
	Max Call Duration	Ascend-Maximum-Call-Duration
	Max Ch Count	Ascend-Maximum-Channels
	Max Leases	Ascend-DHCP-Maximum-Leases
	Metric	Ascend-Metric
	Min Ch Count	Ascend-Minimum-Channels
	MRU	Framed-MTU
	Multicast Client	Ascend-Multicast-Client
	Multicast Rate Limit	Ascend-Multicast-Rate-Limit
	Net End	Ascend-AppleTalk-Route *net_end*
	Net Start	Ascend-AppleTalk-Route *net_start*
	NetWare t/o	Ascend-Netware-timeout
	Peer	Ascend-IPX-Peer-Mode Ascend-AppleTalk-Peer-Mode (in AppleTalk Options submenu)
	Pool	Ascend-Assign-IP-Pool

Table B-1. Parameters and analogous attributes (continued)

Profile	Parameter	Analogous attribute
	Pool Number	Ascend-DHCP-Pool-Number
	Preempt	Ascend-Preempt-Limit
	PRI # Type	Ascend-PRI-Number-Type
	Recv PW	Password Ascend-Receive-Secret
	Reply Enabled	Ascend-DHCP-Reply
	RIP	Framed-Routing
	Route AppleTalk	Ascend-Route-AppleTalk
	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
	TS Idle Limit	Ascend-TS-Idle-Limit
	TS Idle Mode	Ascend-TS-Idle-Mode
	VJ Comp	Framed-Compression
	Zone Name	Ascend-AppleTalk-Route *zone_name*
Bridging profile	Bridging profile parameters	Ascend-Bridge-Address
Ethernet profile	Acct	Ascend-User-Acct-Type

Table B-1. Parameters and analogous attributes (continued)

Profile	Parameter	Analogous attribute
	Acct Host #1 Acct Host #2 Acct Host #3	Ascend-User-Acct-Host
	Acct-ID Base	Ascend-User-Acct-Base
	Acct Key	Ascend-User-Acct-Key
	Acct Port	Ascend-User-Acct-Port
	Acct Timeout	Ascend-User-Acct-Time
	Banner (terminal server users only)	Reply-Message
	Dialout OK	Ascend-Dialout-Allowed
	Host #1 Addr, Host #1 Text Host #2 Addr, Host #2 Text Host #3 Addr, Host #3 Text Host #4 Addr, Host #4 Text (terminal server users only)	Ascend-Host-Info
	IP Adrs	NAS-Identifier
	Immed Service (terminal server users only)	Login-Service
	Shared Prof	Ascend-Shared-Profile-Enable
Filter profile	Filter profile parameters	Ascend-Call-Filter Ascend-Data-Filter
Frame Relay profile	Call Type	Ascend-Call-Type
	Data Svc	Ascend-Data-Svc
	DCE N392	Ascend-FR-DCE-N392
	DCE N393	Ascend-FR-DCE-N393
	DTE N392	Ascend-FR-DTE-N392
	DTE N393	Ascend-FR-DTE-N393
	FR Type	Ascend-FR-Type

Table B-1. Parameters and analogous attributes (continued)

Profile	Parameter	Analogous attribute
	Link Mgmt	Ascend-FR-Link-Mgt
	Link Up	Ascend-FR-LinkUp
	N391	Ascend-FR-N391
	Nailed Grp	Ascend-FR-Nailed-Grp
	T391	Ascend-FR-T391
	T392	Ascend-FR-T392
IPX Route profile	IPX Route profile parameters	Ascend-IPX-Route
Route profile	Route profile parameters	Framed-Route

Attributes and parameters in numerical order

Table B-2 cross references the Ascend RADIUS dictionary's attributes to parameters in MAX unit's menu-driven user interface. The table is arranged by attribute in numerical order.

Table B-2. Attributes and analogous parameters in numerical order

Attribute number	Attribute name	Attribute values	Analogous parameter
1	User-Name	Text string	Station
2	Password (User-Password)	Text string	Recv PW
3	Challenge-Response	Text string	No analogous parameter
4	NAS-Identifier	IP address	IP Adrs
5	NAS-Port	Integer	No analogous parameter
6	User-Service	Login-User (1) Framed-User (2) Dialout-Framed-User (5) (3, 4, and 6 are not supported)	No analogous parameter

Table B-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
7	Framed-Protocol	PPP (1) SLIP (2) MPP (256) EURAW (257) EUUI (258) COMB (260) FR (261) ARA (262) FR-CIR (263)	No analogous parameter
8	Framed-Address	IP address	LAN Adrs
9	Framed-Netmask	IP address	LAN Adrs
10	Framed-Routing	None (0) Broadcast (1) Listen (2) Broadcast-Listen (3) Broadcast-v2 (4) Listen-v2 (5) Broadcast-Listen-v2 (6)	RIP
11	Filter-Id	0 indicates that no filtering is being used (the default). 1-99 indicates that a filter created using the vt100 interface is being used. 100-199 indicates that a filter created using SAM is being used.	No analogous parameter
12	Framed-MTU	Integer	MRU
13	Framed-Compression	Van-Jacobson-TCP-IP (1) (No other values supported)	VJ Comp
14	Login-Host	IP address	Login Host
15	Login-Service	Telnet (0) Rlogin (1) TCP-Clear (2)	Immed Service Encaps=TCP-CLEAR
16	Login-TCP-Port	Integer	Login Port
17	Change-Password	Text string	No analogous parameter

Table B-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
18	Reply-Message	Text string	Banner (terminal server users only)
21	Ascend-PW-Expiration	Date	No analogous parameter
22	Framed-Route	*host_ipaddr* */subnet_mask* *router_ ipaddr* *metric* *private* *profile_name* *preference*	Dest Gateway Metric Private Name Preference
23	Framed-IPX-Network	Integer	IPX Net#
25	Class	Text string	No analogous parameter
30	Client-Port-DNIS	Text string	Called #
31	Caller-Id	Text string	Calling #
40	Acct-Status-Type	Start (1) Stop (2)	No analogous parameter
41	Acct-Delay-Time	Integer	No analogous parameter
42	Acct-Input-Octets	Integer	No analogous parameter
43	Acct-Output-Octets	Integer	No analogous parameter
44	Acct-Session-Id	Text string	No analogous parameter
45	Acct-Authentic	RADIUS (1) Local (2)	No analogous parameter
46	Acct-Session-Time	Integer	No analogous parameter
47	Acct-Input-packets	Integer	No analogous parameter
48	Acct-Output-packets	Integer	No analogous parameter

Table B-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
61	NAS-Port-Type	Async Sync ISDN-Sync ISDN-Async-v120 ISDN-Async-v110 Virtual	No analogous parameter
64	Tunnel-Type	PPTP L2TP	No analogous parameter
65	Tunnel-Medium-Type	IP X25 (not yet supported) ATM (not yet supported)	No analogous parameter
66	Tunnel-Client-Endpoint	String	No analogous parameter
67	Tunnel-Server-Endpoint	Host name or IP address, but not both	No analogous parameter.
68	Tunnel-ID	String	No analogous parameter.
112	Ascend-CBCP-Enable	CBCP-Enabled (0) CBCP-Not-Enabled (1)	CBCP Enable
113	Ascend-CBCP-Mode	CBCP-No-Callback (1) CBCP-User-Callback (2) CBCP-Profile-Callback (3) CBCP-User-Or-No (7)	CBCP Mode
115	Ascend-CBCP-Trunk-Group	Integer between 4 and 9	CBCP Trunk Group
116	Ascend-AppleTalk-Route	*net_start* *net_end* *zone_name* *profile_name*	Net Start Net End Zone Name string
117	Ascend-AppleTalk-Peer-Mode	Appletalk-Peer-Router (0). Appletalk-Peer-Dialin	Peer (AppleTalk Options submenu)
118	Ascend-Route-AppleTalk	Route-Appletalk-No (0) Route-Appletalk-Yes (1)	Route AppleTalk

Table B-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
120	Ascend-Modem-PortNo	Integer	No analogous parameter.
121	Ascend-Modem-SlotNo	Integer	No analogous parameter
125	Ascend-Maximum-Call-Duration	Integer	Max Call Duration
126	Ascend-Preference	Integer	No analogous parameter
127	Tunneling-Protocol	ATMP	No analogous parameter
128	Ascend-Shared-Profile-Enable	Yes No	Shared Prof
131	Ascend-Dialout-Allowed	Dialout-Not-Allowed (0) Dialout-Allowed (1)	Dialout OK
132	Ascend-Client-Gateway	IP address	Client Gateway
134	Ascend-BACP-Enable	BACP-No (0) BACP-Yes (1)	BACP
138	Ascend-User-Acct-Type	Ascend-User-Acct-None (0) Ascend-User-Acct-User (1) Ascend-User-Acct-User-Default (2)	Acct
139	Ascend-User-Acct-Host	IP address	Acct Host #1 Acct Host #2 Acct Host #3
140	Ascend-User-Acct-Port	Integer	Acct Port
141	Ascend-User-Acct-Key	Text string	Acct Key
142	Ascend-User-Acct-Base	Ascend-User-Acct-Base-10 (0) Ascend-User-Acct-Base-16 (1)	Acct-ID Base
143	Ascend-User-Acct-Time	Integer	Acct Timeout
144	Ascend-Assign-IP-Client	IP address	No analogous parameter
145	Ascend-Assign-IP-Server	IP address	No analogous parameter
146	Ascend-Assign-IP-Global-Pool	Text string	No analogous parameter

Table B-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
147	Ascend-DHCP-Reply	DHCP-Reply-No (0) DHCP-Reply-Yes (1)	Reply Enabled
148	Ascend-DHCP-Pool-Number	Integer	Pool Number
149	Ascend-Expect-Callback	Expect-Callback-No (0) Expect-Callback-Yes (1)	Expect Callback
150	Ascend-Event-Type	Ascend-Coldstart (1) Ascend-Session-Event (2)	No analogous parameter
151	Ascend-Session-Svr-Key	Text string	No analogous parameter
152	Ascend-Multicast-Client	Multicast-No (0) Multicast-Yes (1)	Multicast Client
153	Ascend-Multicast-Rate-Limit	Integer	Multicast Rate Limit
154	Ascend-IF-Netmask	IP address	No analogous parameter
155	Ascend-Remote-Addr	IP address	IF Adrs
156	Ascend-FR-Circuit-Name	Text string	Circuit
157	Ascend-FR-LinkUp	Ascend-LinkUp-Default (0) Ascend-LinkUp-AlwaysUp (1)	Link Up
158	Ascend-FR-Nailed-Grp	Integer	Nailed Grp
159	Ascend-FR-Type	Ascend-FR-DTE (0) Ascend-FR-DCE (1) Ascend-FR-NNI (2)	FR Type
160	Ascend-FR-Link-Mgt	Ascend-FR-No-Link-Mgt (0) Ascend-FR-T1-617D (1) Ascend-FR-Q-933A (2)	Link Mgmt
161	Ascend-FR-N391	Integer	N391
162	Ascend-FR-DCE-N392	Integer	DCE N392
163	Ascend-FR-DTE-N392	Integer	DTE N392
164	Ascend-FR-DCE-N393	Integer	DCE N393
165	Ascend-FR-DTE-N393	Integer	DTE N393
166	Ascend-FR-T391	Integer	T391

Table B-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
167	Ascend-FR-T392	Integer	T392
168	Ascend-Bridge-Address	*MAC_address* *profile_name* *IP_address*	Enet Adrs Net Adrs
169	Ascend-TS-Idle-Limit	Integer	TS Idle Limit
170	Ascend-TS-Idle-Mode	TS-Idle-None (0) TS-Idle-Input (1) TS-Idle-Input-Output (2)	TS Idle Mode
171	Ascend-DBA-Monitor	DBA-Transmit (0) DBA-Transmit-Recv (1) DBA-None (2)	DBA Monitor
172	Ascend-Base-Channel-Count	Integer	Base Ch Count
173	Ascend-Minimum-Channels	Integer	Min Ch Count
174	Ascend-IPX-Route	*profile_name* *network#* **[***node#***]** **[***socket#***]** **[***server_type***]** **[***hop_count***]** **[***tick_count***]** **[***name***]**	Connection # Network Node Socket Server Type Hop Count Tick Count Server Name
175	Ascend-FT1-Caller	FT1-No (0) FT1-Yes (1)	FT1-Caller
176	Ascend-backup	Text string	Backup
177	Ascend-Call-Type	Nailed (1) Nailed/Mpp (2) Perm/Switched (3)	Call Type
178	Ascend-Group	Single integer or comma-separated group of integers	Group
179	Ascend-FR-DLCI	Integer between 16 and 991	DLCI
180	Ascend-FR-Profile-Name	Text string	FR Prof

Table B-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
181	Ascend-Ara-PW	Text string	Password in the Encaps Options submenu of the Connection profile when Encaps=ARA.
182	Ascend-IPX-Node-Addr	12-digit ASCII string	Node
184	Ascend-Home-Agent-Password	Text string	No analogous parameter
185	Ascend-Home-Network-Name	Text string	No analogous parameter
186	Ascend-Home-Agent-UDP-Port	Integer	No analogous parameter
187	Ascend-Multilink-ID	Integer	No analogous parameter
188	Ascend-Num-In-Multilink	Integer	No analogous parameter
189	Ascend-First-Dest	IP address	No analogous parameter
190	Ascend-Pre-Input-Octets	Integer	No analogous parameter
191	Ascend-Pre-Output-Octets	Integer	No analogous parameter
192	Ascend-Pre-Input-packets	Integer	No analogous parameter
193	Ascend-Pre-Output-packets	Integer	No analogous parameter
194	Ascend-Maximum-Time	Integer	Max Call Duration
195	Ascend-Disconnect-Cause	Integer	No analogous parameter
196	Ascend-Connect-Progress	Integer	No analogous parameter
197	Ascend-Data-Rate	Integer	No analogous parameter

Table B-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
198	Ascend-PreSession-Time	Integer	No analogous parameter
199	Ascend-Token-Idle	Integer	No analogous parameter
200	Ascend-Token-Immediate	Tok-Imm-No (0) Tok-Imm-Yes (1)	No analogous parameter
201	Ascend-Require-Auth	Not-Require-Auth (0) Require-Auth (1)	Auth Req
202	Ascend-Number-Sessions	Text string	No analogous parameter
203	Ascend-Authen-Alias	Text string	No analogous parameter
204	Ascend-Token-Expiry	Integer	No analogous parameter
205	Ascend-Menu-Selector	Text string	No analogous parameter
206	Ascend-Menu-Item	Text string	No analogous parameter
208	Ascend-PW-Lifetime	Integer	No analogous parameter
209	Ascend-IP-Direct	IP address	IP Direct
210	Ascend-PPP-VJ-Slot-Comp	VJ-Slot-Comp-No (1)	No analogous parameter
211	Ascend-PPP-VJ-1172	PPP-VJ-1172 (1)	No analogous parameter
212	Ascend-PPP-Async-Map	Integer	No analogous parameter
213	Ascend-Third-Prompt	Text string	3rd Prompt
214	Ascend-Send-Secret	Text string	Send PW
215	Ascend-Receive-Secret	Text string	Recv PW
216	Ascend-IPX-Peer-Mode	IPX-Peer-Router (0) IPX-Peer-Dialin (1)	No analogous parameter

Table B-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
217	Ascend-IP-Pool-Definition	Text string	Pool Start #1, #2 Pool Count #1, #2
218	Ascend-Assign-IP-Pool	Integer	Pool
219	Ascend-FR-Direct	FR-Direct-No (0) FR-Direct-Yes (1)	FR Direct
220	Ascend-FR-Direct-Profile	Text string	FR Prof
221	Ascend-FR-Direct-DLCI	Integer	FR DLCI
222	Ascend-Handle-IPX	Handle-IPX-None (0) Handle-IPX-Client (1) Handle-IPX-Server (2)	Handle IPX
223	Ascend-Netware-timeout	Integer	NetWare t/o
224	Ascend-IPX-Alias	Text string	IPX Alias#
225	Ascend-Metric	Integer	Metric
226	Ascend-PRI-Number-Type	Unknown-Number (0) Intl-Number (1) National-Number (2) Local-Number (4) Abbrev-Number (5)	PRI # Type
227	Ascend-Dial-Number	Text string	Dial #
228	Ascend-Route-IP	Route-IP-No (0) Route-IP-Yes (1)	Route IP
229	Ascend-Route-IPX	Route-IPX-No (0) Route-IPX-Yes (1)	Route IPX
230	Ascend-Bridge	Bridge-No (0) Bridge-Yes (1)	Bridge
231	Ascend-Send-Auth	Send-Auth-None (0) Send-Auth-PAP (1) Send-Auth-CHAP (2)	Send Auth
232	Ascend-Send-Passwd	Text string	Send PW
233	Ascend-Link-Compression	Link-Comp-None (0) Link-Comp-Stac (1)	Link Comp
234	Ascend-Target-Util	Integer	Target Util

Table B-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
235	Ascend-Maximum-Channels	Integer	Max Ch Cnt
236	Ascend-Inc-Channel-Count	Integer	Inc Ch Cnt
237	Ascend-Dec-Channel-Count	Integer	Dec Ch Cnt
238	Ascend-Seconds-Of-History	Integer	Sec Hist
239	Ascend-History-Weigh-Type	History-Constant (0) History-Linear (1) History-Quadratic (2)	Dyn Alg
240	Ascend-Add-Seconds	Integer	Add Pers
241	Ascend-Remove-Seconds	Integer	Sub Pers
242	Ascend-Data-Filter	Filter specification	Filter profile parameters
243	Ascend-Call-Filter	Filter specification	Filter profile parameters
244	Ascend-Idle-Limit	Integer	Idle
245	Ascend-Preempt-Limit	Integer	Preempt
246	Ascend-Callback	Callback-No (0) Callback-Yes (1)	Callback
255	Ascend-Xmit-Rate	Integer	No analogous parameter.

Table B-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
247	Ascend-Data-Svc	Switched-Voice-Bearer (0) Switched-56KR (1) Switched-64K (2) Switched-64KR (3) Switched-56K (4) Nailed-56KR (1) Nailed-64K (2) Switched-384KR (5) Switched-384K (6) Switched-1536K (7) Switched-1536KR (8) Switched-128K (9) Switched-192K (10) Switched-256K (11) Switched-320K (12) Switched-384K-MR (13) Switched-448K (14) Switched-512K (15) Switched-576K (16) Switched-640K (17) Switched-704K (18) Switched-768K (19) Switched-832K (20) Switched-896K (21) Switched-960K (22) Switched-1024K (23) Switched-1088K (24) Switched-1152K (25) Switched-1216K (26) Switched-1280K (27) Switched-1344K (28) Switched-1408K (29) Switched-1472K (30) Switched-1600K (31) Switched-1664K (32) Switched-1728K (33) Switched-1792K (34) Switched-1856K (35) Switched-1920K (36) Switched-inherited (37) Switched-restricted-bearer-x30 (38) Switched-clear-bearer-v110 (39) Switched-restricted-64-x30 (40) Switched-clear-56-v110 (41) Switched-modem (42) Switched-atmodem (43)	Data Svc

Table B-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
248	Ascend-Force-56	Force-56-No (0) Force-56-Yes (1)	Force 56
249	Ascend-Billing-Number	Text string	Bill #
250	Ascend-Call-By-Call	Integer	Call-by-Call
251	Ascend-Transit-Number	Text string	Transit #
252	Ascend-Host-Info	Text string	Host #1 Addr Host #1 Text Host #2 Addr Host #2 Text Host #3 Addr Host #3 Text Host #4 Addr Host #4 Text
253	Ascend-PPP-Address	IP address	No analogous parameter
254	Ascend-MPP-Idle-Percent	Integer	Idle Pct

Attributes and parameters in alphabetical order

Table B-3 cross references the Ascend RADIUS dictionary's attributes to parameters in MAX unit's menu-driven user interface. The table is arranged by attribute in alphabetical order.

Table B-3. Attributes and analogous parameters in alphabetical order

Attribute name	Attribute number	Attribute values	Analogous parameter
Acct-Authentic	45	RADIUS (1) Local (2)	No analogous parameter
Acct-Delay-Time	41	Integer	No analogous parameter
Acct-Input-Octets	42	Integer	No analogous parameter
Acct-Input-packets	47	Integer	No analogous parameter
Acct-Output-Octets	43	Integer	No analogous parameter

Table B-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Acct-Output-packets	48	Integer	No analogous parameter
Acct-Session-Id	44	Text string	No analogous parameter
Acct-Session-Time	46	Integer	No analogous parameter
Acct-Status-Type	40	Start (1) Stop (2)	No analogous parameter
Ascend-Add-Seconds	240	Integer	Add Pers
Ascend-AppleTalk-Peer-Mode	117	Appletalk-Peer-Router (0). Appletalk-Peer-Dialin	Peer (AppleTalk Options submenu)
Ascend-AppleTalk-Route	116	*net_start* *net_end* *zone_name* *profile_name*	Net Start Net End Zone Name string
Ascend-Ara-PW	181	Text string	Password in the Encaps Options submenu of the Connection profile when Encaps=ARA.
Ascend-Assign-IP-Client	144	IP address	No analogous parameter
Ascend-Assign-IP-Global-Pool	146	Text string	No analogous parameter
Ascend-Assign-IP-Pool	218	Integer	Pool
Ascend-Assign-IP-Server	145	IP address	No analogous parameter
Ascend-Authen-Alias	203	Text string	No analogous parameter
Ascend-backup	176	Text string	Backup
Ascend-BACP-Enable	134	BACP-No (0) BACP-Yes (1)	BACP
Ascend-Base-Channel-Count	172	Integer	Base Ch Count

Table B-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-Billing-Number	249	Text string	Bill #
Ascend-Bridge	230	Bridge-No (0) Bridge-Yes (1)	Bridge
Ascend-Bridge-Address	168	*MAC_address* *profile_name* *IP_address*	Enet Adrs Net Adrs
Ascend-Callback	246	Callback-No (0) Callback-Yes (1)	Callback
Ascend-Call-By-Call	250	Integer	Call-by-Call
Ascend-Call-Filter	243	Filter specification	Filter profile parameters
Ascend-Call-Type	177	Nailed (1) Nailed/Mpp (2) Perm/Switched (3)	Call Type
Ascend-CBCP-Enable	112	CBCP-Enabled (0) CBCP-Not-Enabled (1)	CBCP Enable
Ascend-CBCP-Mode	113	CBCP-No-Callback (1) CBCP-User-Callback (2) CBCP-Profile-Callback (3) CBCP-User-Or-No (7)	CBCP Mode
Ascend-CBCP-Trunk-Group	115	Integer between 4 and 9	CBCP Trunk Group
Ascend-Client-Gateway	132	IP address	Client Gateway
Ascend-Connect-Progress	196	Integer	No analogous parameter
Ascend-Data-Filter	242	Filter specification	Filter profile parameters
Ascend-Data-Rate	197	Integer	No analogous parameter

Table B-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-Data-Svc	247	Switched-Voice-Bearer (0) Switched-56KR (1) Switched-64K (2) Switched-64KR (3) Switched-56K (4) Nailed-56KR (1) Nailed-64K (2) Switched-384KR (5) Switched-384K (6) Switched-1536K (7) Switched-1536KR (8) Switched-128K (9) Switched-192K (10) Switched-256K (11) Switched-320K (12) Switched-384K-MR (13) Switched-448K (14) Switched-512K (15) Switched-576K (16) Switched-640K (17) Switched-704K (18) Switched-768K (19) Switched-832K (20) Switched-896K (21) Switched-960K (22) Switched-1024K (23) Switched-1088K (24) Switched-1152K (25) Switched-1216K (26) Switched-1280K (27) Switched-1344K (28) Switched-1408K (29) Switched-1472K (30) Switched-1600K (31) Switched-1664K (32) Switched-1728K (33) Switched-1792K (34) Switched-1856K (35) Switched-1920K (36) Switched-inherited (37) Switched-restricted-bearer-x30 (38) Switched-clear-bearer-v110 (39) Switched-restricted-64-x30 (40) Switched-clear-56-v110 (41) Switched-modem (42) Switched-atmodem (43)	Data Svc

Table B-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-DBA-Monitor	171	DBA-Transmit (0) DBA-Transmit-Recv (1) DBA-None (2)	DBA Monitor
Ascend-Dec-Channel-Count	237	Integer	Dec Ch Cnt
Ascend-DHCP-Maximum-Leases		Integer	Max Leases
Ascend-DHCP-Pool-Number	148	Integer	Pool Number
Ascend-DHCP-Reply	147	DHCP-Reply-No (0) DHCP-Reply-Yes (1)	Reply Enabled
Ascend-Dial-Number	227	Text string	Dial #
Ascend-Dialout-Allowed	131	Dialout-Not-Allowed (0) Dialout-Allowed (1)	Dialout OK
Ascend-Disconnect-Cause	195	Integer	No analogous parameter
Ascend-Event-Type	150	Ascend-Coldstart (1) Ascend-Session-Event (2)	No analogous parameter
Ascend-Expect-Callback	149	Expect-Callback-No (0) Expect-Callback-Yes (1)	Expect Callback
Ascend-First-Dest	189	IP address	No analogous parameter
Ascend-Force-56	248	Force-56-No (0) Force-56-Yes (1)	Force 56
Ascend-FR-Circuit-Name	156	Text string	Circuit
Ascend-FR-DCE-N392	162	Integer	DCE N392
Ascend-FR-DCE-N393	164	Integer	DCE N393
Ascend-FR-DTE-N392	163	Integer	DTE N392
Ascend-FR-DTE-N393	165	Integer	DTE N393
Ascend-FR-Direct	219	FR-Direct-No (0) FR-Direct-Yes (1)	FR Direct
Ascend-FR-Direct-DLCI	221	Integer	FR DLCI
Ascend-FR-Direct-Profile	220	Text string	FR Prof

Table B-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-FR-DLCI	179	Integer between 16 and 991	DLCI
Ascend-FR-Link-Mgt	160	Ascend-FR-No-Link-Mgt (0) Ascend-FR-T1-617D (1) Ascend-FR-Q-933A (2)	Link Mgmt
Ascend-FR-LinkUp	157	Ascend-LinkUp-Default (0) Ascend-LinkUp-AlwaysUp (1)	Link Up
Ascend-FR-N391	161	Integer	N391
Ascend-FR-Nailed-Grp	158	Integer	Nailed Grp
Ascend-FR-Profile-Name	180	Text string	FR Prof
Ascend-FR-T391	166	Integer	T391
Ascend-FR-T392	167	Integer	T392
Ascend-FR-Type	159	Ascend-FR-DTE (0) Ascend-FR-DCE (1) Ascend-FR-NNI (2)	FR Type
Ascend-FT1-Caller	175	FT1-No (0) FT1-Yes (1)	FT1-Caller
Ascend-Group	178	Single integer or comma-separated group of integers	Group
Ascend-Handle-IPX	222	Handle-IPX-None (0) Handle-IPX-Client (1) Handle-IPX-Server (2)	Handle IPX
Ascend-History-Weigh-Type	239	History-Constant (0) History-Linear (1) History-Quadratic (2)	Dyn Alg
Ascend-Home-Agent-Password	184	Text string	No analogous parameter
Ascend-Home-Agent-UDP-Port	186	Integer	No analogous parameter
Ascend-Home-Network-Name	185	Text string	No analogous parameter

Table B-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-Host-Info	252	Text string	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-Idle-Limit	244	Integer	Idle
Ascend-IF-Netmask	154	IP address	No analogous parameter
Ascend-Inc-Channel-Count	236	Integer	Inc Ch Cnt
Ascend-IP-Direct	209	IP address	IP Direct
Ascend-IP-Pool-Definition	217	Text string	Pool Start #1, #2 Pool Count #1, #2
Ascend-IPX-Alias	224	Text string	IPX Alias#
Ascend-IPX-Node-Addr	182	12-digit ASCII string	Node
Ascend-IPX-Peer-Mode	216	IPX-Peer-Router (0) IPX-Peer-Dialin (1)	No analogous parameter
Ascend-IPX-Route	174	*profile_name* *network#* **[***node#***]** **[***socket#***]** **[***server_type***]** **[***hop_count***]** **[***tick_count***]** **[***name***]**	Connection # Network Node Socket Server Type Hop Count Tick Count Server Name
Ascend-Link-Compression	233	Link-Comp-None (0) Link-Comp-Stac (1)	Link Comp
Ascend-Maximum-Call-Duration	125	Integer	Max Call Duration
Ascend-Maximum-Channels	235	Integer	Max Ch Cnt
Ascend-Maximum-Time	194	Integer	Max Call Duration
Ascend-Menu-Item	206	Text string	No analogous parameter

Table B-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-Menu-Selector	205	Text string	No analogous parameter
Ascend-Metric	225	Integer	Metric
Ascend-Minimum-Channels	173	Integer	Min Ch Count
Ascend-Modem-PortNo	120	Integer	No analogous parameter
Ascend-Modem-SlotNo	121	Integer	No analogous parameter
Ascend-MPP-Idle-Percent	254	Integer	Idle Pct
Ascend-Multicast-Client	152	Multicast-No (0) Multicast-Yes (1)	Multicast Client
Ascend-Multicast-Rate-Limit	153	Integer	Multicast Rate Limit
Ascend-Multilink-ID	187	Integer	No analogous parameter
Ascend-Netware-timeout	223	Integer	NetWare t/o
Ascend-Number-Sessions	202	Text string	No analogous parameter
Ascend-Num-In-Multilink	188	Integer	No analogous parameter
Ascend-PPP-Address	253	IP address	No analogous parameter
Ascend-PPP-Async-Map	212	Integer	No analogous parameter
Ascend-PPP-VJ-1172	211	PPP-VJ-1172 (1)	No analogous parameter
Ascend-PPP-VJ-Slot-Comp	210	VJ-Slot-Comp-No (1)	No analogous parameter
Ascend-Preempt-Limit	245	Integer	Preempt
Ascend-Pre-Input-Octets	190	Integer	No analogous parameter
Ascend-Pre-Input-packets	192	Integer	No analogous parameter

Table B-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-Pre-Output-Octets	191	Integer	No analogous parameter
Ascend-Pre-Output-packets	193	Integer	No analogous parameter
Ascend-PreSession-Time	198	Integer	No analogous parameter
Ascend-Primary-Home-Agent		IP address or hostname	No analogous parameter
Ascend-PRI-Number-Type	226	Unknown-Number (0) Intl-Number (1) National-Number (2) Local-Number (4) Abbrev-Number (5)	PRI # Type
Ascend-PW-Expiration	21	Date	No analogous parameter
Ascend-PW-Lifetime	208	Integer	No analogous parameter
Ascend-Receive-Secret	215	Text string	Recv PW
Ascend-Remote-Addr	155	IP address	IF Adrs
Ascend-Remove-Seconds	241	Integer	Sub Pers
Ascend-Require-Auth	201	Not-Require-Auth (0) Require-Auth (1)	Auth Req
Ascend-Route-AppleTalk	118	Route-Appletalk-No (0) Route-Appletalk-Yes (1)	Route AppleTalk
Ascend-Route-IP	228	Route-IP-No (0) Route-IP-Yes (1)	Route IP
Ascend-Route-IPX	229	Route-IPX-No (0) Route-IPX-Yes (1)	Route IPX
Ascend-Secondary-Home-Agent		IP address or hostname	No analogous parameter
Ascend-Seconds-Of-History	238	Integer	Sec Hist
Ascend-Send-Auth	231	Send-Auth-None (0) Send-Auth-PAP (1) Send-Auth-CHAP (2)	Send Auth

Table B-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-Send-Passwd	232	Text string	Send PW
Ascend-Send-Secret	214	Text string	Send PW
Ascend-Session-Svr-Key	151	Text string	No analogous parameter
Ascend-Target-Util	234	Integer	Target Util
Ascend-Third-Prompt	213	Text string	3rd Prompt
Ascend-Token-Expiry	204	Integer	No analogous parameter
Ascend-Token-Idle	199	Integer	No analogous parameter
Ascend-Token-Immediate	200	Tok-Imm-No (0) Tok-Imm-Yes (1)	No analogous parameter
Ascend-Transit-Number	251	Text string	Transit #
Ascend-TS-Idle-Limit	169	Integer	TS Idle Limit
Ascend-TS-Idle-Mode	170	TS-Idle-None (0) TS-Idle-Input (1) TS-Idle-Input-Output (2)	TS Idle Mode
Ascend-User-Acct-Base	142	Ascend-User-Acct-Base-10 (0) Ascend-User-Acct-Base-16 (1)	Acct-ID Base
Ascend-User-Acct-Host	139	IP address	Acct Host #1 Acct Host #2 Acct Host #3
Ascend-User-Acct-Key	141	Text string	Acct Key
Ascend-User-Acct-Port	140	Integer	Acct Port
Ascend-User-Acct-Time	143	Integer	Acct Timeout
Ascend-User-Acct-Type	138	Ascend-User-Acct-None (0) Ascend-User-Acct-User (1) Ascend-User-Acct-User-Default (2)	Acct
Ascend-Xmit-Rate	255	Integer	No analogous parameter
Caller-Id	31	Text string	Calling #

Table B-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Challenge-Response	3	Text string	No analogous parameter
Change-Password	17	Text string	No analogous parameter
Class	25	Text string	No analogous parameter
Client-Port-DNIS	30	Text string	Called #
Filter-ID	11	0 indicates that no filtering is being used (the default). 1-99 indicates that a filter created using the vt100 interface is being used. 100-199 indicates that a filter created using SAM is being used.	No analogous parameter
Framed-Address	8	IP address	LAN Adrs
Framed-Compression	13	Van-Jacobson-TCP-IP (1) (No other values supported)	VJ Comp
Framed-IPX-Network	23	Integer	IPX Net#
Framed-MTU	12	Integer	MRU
Framed-Netmask	9	IP address	LAN Adrs
Framed-Protocol	7	PPP (1) SLIP (2) MPP (256) EURAW (257) EUUI (258) COMB (260) FR (261) ARA (262) FR-CIR (263)	No analogous parameter
Framed-Route	22	*host_ipaddr* */subnet_mask* *router_ ipaddr* *metric* *private* *profile_name* *preference*	Dest Gateway Metric Private Name Preference

Table B-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Framed-Routing	10	None (0) Broadcast (1) Listen (2) Broadcast-Listen (3) Broadcast-v2 (4) Listen-v2 (5) Broadcast-Listen-v2 (6)	RIP
Login-Host	14	IP address	Login Host
Login-Service	15	Telnet (0) Rlogin (1) TCP-Clear (2)	Immed Service Encaps=TCP-CLEAR
Login-TCP-Port	16	Integer	Login Port
NAS-Identifier	4	IP address	IP Adrs
NAS-Port	5	Integer	No analogous parameter
NAS-Port-Type	61	Async Sync ISDN-Sync ISDN-Async-v120 ISDN-Async-v110 Virtual	No analogous parameter
Password (User-Password)	2	Text string	Recv PW
Reply-Message	18	Text string	Banner (terminal server users only)
Tunnel-Client-Endpoint	66	Text string	No analogous parameter
Tunnel-Id	68	Text string	No analogous parameter
Tunnel-Medium-Type	65	IP X25 (not yet supported) ATM (not yet supported)	No analogous parameter
Tunnel-Server-Endpoint	67	Host name or IP address, but not both	No analogous parameter

Table B-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Tunnel-Type	64	PPTP L2TP	No analogous parameter
User-Name	1	Text string	Station
User-Service	6	Login-User (1) Framed-User (2) Dialout-Framed-User (5) (3, 4, and 6 are not supported)	No analogous parameter

Index