MAX TNT RADIUS Guide

Ascend Communications, Inc.
Part Number: 7820-0480-005
For Software Version 7.0.0

Ascend Customer Service

Ascend Customer Service provides a variety of options for obtaining technical assistance, information about Ascend products and services, and software upgrades.

Obtaining technical assistance

You can obtain technical assistance by telephone, email, fax, or modem, or over the Internet.

Enabling Ascend to assist you

If you need to contact Ascend for help with a problem, make sure that you have the following information when you call or that you include it in your correspondence:

- Product name and model.
- Software and hardware options.
- Software version.
- If supplied by your carrier, Service Profile Identifiers (SPIDs) associated with your line.
- 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.

Calling Ascend from within the United States

In the U.S., you can take advantage of Priority Technical Assistance or an Ascend Advantage Pak service contract, or you can call to request assistance.

Priority Technical Assistance

If you need to talk to an engineer right away, call (900) 555-ASND (2763) to reach Ascend's Priority Call queue. The charge of $2.95 per minute does not begin to accrue until you are connected to an engineer. Average wait times are less than three minutes.

Ascend Advantage Pak

Ascend Advantage Pak is a one-year service contract that includes overnight advance replacement of failed products, technical support, software maintenance releases, and software update releases. For more information, call (800) ASCEND-4 (272-3634), or access Ascend's Web site at `www.ascend.com` and select Services and Support, then Advantage Service Family.

Other telephone numbers

For a menu of Ascend's services, call (800) ASCEND-4 (272-3634). Or call (510) 769-6001 for an operator.

Calling Ascend from outside the United States

You can contact Ascend by telephone from outside the United States at one of the following numbers:

Telephone outside the United States	(510) 769-8027
Asia Pacific (except Japan)	(+61) 3 9656 7000
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

Note: For additional support information for the Asia Pacific Region, refer to `http://apac.ascend.com/contacts.html`.

Obtaining assistance through correspondence

Ascend maintains two email addresses for technical support questions. One is for customers in the United States, and the other is for customers in Europe, the Middle East, and Asia. If you prefer to correspond by fax, BBS, or regular mail, please direct your inquiry to Ascend's U.S. offices. Following are the ways in which you can reach Ascend Customer Service:

- Email from within the U.S.—support@ascend.com
- Email from Europe, the Middle East, or Asia—EMEAsupport@ascend.com
- Fax—(510) 814-2312
- Customer Support BBS (by modem)—(510) 814-2302
- Write to Ascend at the following address:

  Attn: Customer Service
  Ascend Communications, Inc.
  One Ascend Plaza
  1701 Harbor Bay Parkway
  Alameda, CA 94502-3002

Finding information and software on the Internet

Visit Ascend's Web site at `http://www.ascend.com` for technical information, product information, and descriptions of available services.

Visit Ascend's FTP site at `ftp.ascend.com` for software upgrades, release notes, and addenda to this manual.

Contents

Chapter 4 Setting Up RADIUS Accounting 4-1

About This Guide

What's new

This guide describes how to install and start up the RADIUS daemon, and provides detailed information about RADIUS attributes, accounting, and call logging. However, it no longer contains information about using RADIUS to set up authentication, authorization, and user connections. For instructions about carrying out these tasks, see the *MAX TNT Network Guide*.

Note: This manual describes the full set of features for the MAX TNT running software version 7.0.0. Some features might not be available with older versions or specialty loads of the software.

What you should know

This guide is intended for the person who will configure and maintain RADIUS and the MAX TNT. To use it effectively, you must have a basic understanding of MAX TNT security and configuration, and be familiar with authentication servers and networking concepts.

While this guide attempts to provide enough conceptual framework to enable an administrator who is not an expert in a particular network technology to configure RADIUS accurately, it does not start from the beginning with any network management topic. Following are the general areas in which it is helpful have some existing knowledge when configuring RADIUS:

- Dial-in LAN connections, such as PPP and MP+
- Connection cost management and accounting
- Modems
- Frame Relay
- NetWare and IPX routing
- IP routing
- DNS
- OSPF routing (if applicable)
- Multicast (if applicable)
- Packet structure and formats (for defining filters)
- Network security

Documentation conventions

Ascend uses standard documentation conventions. The introductory section of each manual includes a section that describes the conventions, which are as follows:

Convention	Meaning
`Monospace text`	Represents text that appears on your computer's screen, or that could appear on your computer's screen.
`Boldface mono-space 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 or menu item. The item that follows the angle bracket is one of the options that appears when you select the item 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.

Manual set

The MAX TNT documentation set consists of the following manuals:

- *The MAX TNT Command-Line Interface*. Shows you how to use the MAX TNT command-line interface effectively.
- *MAX TNT Hardware Installation Guide*. Describes how to install the MAX TNT hardware and use the command-line interface to configure its slot cards for a variety of supported uses. Describes how calls are routed through the system. Includes the MAX TNT technical specifications.
- *MAX TNT Network Guide*. Describes how to configure the MAX TNT for network connectivity.
- *MAX TNT RADIUS Guide* (this manual). Contains installation instructions, descriptions of RADIUS attributes, accounting information, and details about call logging.
- *MAX TNT Reference Guide*. An alphabetic reference to all MAX TNT profiles, parameters, and commands.
- *MAX TNT Glossary*. An alphabetic reference to technical terms and acronyms commonly found in Ascend documentation.
- *MAX TNT Administration Guide*. Describes how to administer the MAX TNT, including how to monitor the system and the cards, troubleshoot the unit, and use SNMP to manage it.

Related publications

Many external references are readily available on the Web or in technical bookstores. You'll find a partial list of such references below.

Related RFCs

RFCs are available on the Web at http://ds.internic.net.

Information about PPP connections

For information about PPP connections and authentication, you might want to download one or more of the following:

- RFC 1662: *PPP in HDLC-like Framing*
- RFC 1661: *The Point-to-Point Protocol (PPP)*
- RFC 1994: *PPP Challenge Handshake Authentication Protocol (CHAP)*
- RFC 1934: *Ascend's Multilink Protocol Plus (MP+)*
- RFC 1969: *The PPP DES Encryption Protocol (DESE)*
- RFC 1989: *PPP Link Quality Monitoring*
- RFC 1990: *The PPP Multilink Protocol (MP)*
- RFC 2125: *The PPP Bandwidth Allocation Control Protocol (BACP)*
- RFC 2153: *PPP Vendor Extensions*
- RFC 1962: *The PPP Compression Control Protocol (CCP)*

- RFC 1974: *PPP Stac LZS Compression Protocol*
- RFC 1877: *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*
- RFC 1618: *PPP over ISDN*
- RFC 1332: *The PPP Internet Protocol Control Protocol (IPCP)*
- RFC 1552: *The PPP Internetwork Packet Exchange Control Protocol (IPXCP)*
- RFC 1378: *The PPP AppleTalk Control Protocol (ATCP)*

Information about IPX routing

For information about IPX routing, see RFC 1634: *Novell IPX Over Various WAN Media (IPXWAN).*

Information about IP routers

RFCs that describe the operation of IP routers include:

- RFC 1812: *Requirements for IP Version 4 Routers*
- RFC 1519: *Classless Inter-Domain Routing (CIDR): An Address Assignment and Aggregation Strategy*
- RFC 2002: *IP Mobility Support*
- RFC 1256: *ICMP Router Discovery Messages*
- RFC 1393: *Traceroute Using an IP Option*
- RFC 1433: *Directed ARP*
- RFC 1582: *Extensions to RIP to Support Demand Circuits*
- RFC 1787: *Routing in a Multi-provider Internet*

Information about OSPF routing

For information about OSPF routing, see:

- RFC 1850: *OSPF Version 2 Management Information Base*
- RFC 1587: *The OSPF NSSA Option*
- RFC 1245: *OSPF protocol analysis*
- RFC 1246: *Experience with the OSPF protocol*
- RFC 1583: *OSPF Version 2*
- RFC 1586: *Guidelines for Running OSPF Over Frame Relay Networks*

Information about multicast

For information about multicast, see:

- RFC 1458: *Requirements for Multicast Protocols*
- RFC 1584: *Multicast Extensions to OSPF*
- RFC 1949: *Scalable Multicast Key Distribution*

Information about firewalls and packet filtering

RFCs that describe firewalls and packet filters include:

- RFC 1858: *Security Considerations for IP Fragment Filtering*
- RFC 1579: *Firewall-Friendly FTP*

Information about general network security

RFCs pertinent to network security include:

- RFC 1704: *On Internet Authentication*
- RFC 1636: *Report of IAB Workshop on Security in the Internet Architecture*
- RFC 1281: *Guidelines for the Secure Operation of the Internet*
- RFC 1244: *Site Security Handbook*

Information about external authentication

For information about RADIUS and TACACS authentication, see:

- RFC 2138: *Remote Authentication Dial In User Service (RADIUS)*
- RFC 1492: *An Access Control Protocol, Sometimes Called TACACS*

ITU-T recommendations

ITU-T recommendations (formerly CCITT) are available commercially. You can order them at http://www.itu.ch/publications/.

Related books

The following books are available in technical bookstores:

- *Routing in the Internet*, by Christian Huitema. Prentice Hall PTR, 1995. Recommended for information about IP, OSPF, CIDR, IP multicast, and mobile IP.
- *SNMP, SNMPV2 and RMON: Practical Network Management*, by William Stallings. Addison-Wesley, 1996. Recommended for network management information.
- *Enterprise Networking: Fractional T1 to Sonet Frame Relay to Bisdn*, by Daniel Minoli. Artech House, 1993. Recommended as a WAN reference.
- *TCP/IP Illustrated*, volumes 1&2, by W. Richard Stevens. Addison-Wesley, 1994.

Getting Acquainted with RADIUS

1

After you familiarize yourself with the basics of RADIUS authentication and accounting, you will find an overview of the files that the RADIUS server uses:

What is RADIUS?

RADIUS is an acronym for Remote Authentication Dial-In User Service. The MAX TNT uses RADIUS as a central location for storing:

- Authentication attributes
- Configuration data for establishing a WAN connection with an incoming call
- Routing information
- Dialout information
- 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. The attributes indicate a user name and password. They also enable you to configure routing, call management, and restrictions on the types of MAX TNT resources a caller can access.

How does RADIUS authentication work?

A RADIUS server is the machine on which the RADIUS daemon is running. A single RADIUS server can administer multiple security systems, maintaining profiles for thousands of users. RADIUS authentication is specified in IETF RFC 2058.

When you use RADIUS authentication, the following events take place:

1. A user dialing in from a modem, ISDN terminal adapter, or router attempts to open a connection to the MAX TNT.
2. The MAX TNT determines that it must use a RADIUS user profile to authenticate the user.
3. The MAX TNT sends the user connection request to the RADIUS server.
4. If you specify Calling-Line ID (CLID) authentication, the RADIUS server checks the calling party's phone number. The RADIUS server can also perform called-number authentication by checking the number the user dialed to reach the MAX TNT.
5. If required, RADIUS obtains the user's name and password with Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), or Microsoft CHAP (MS-CHAP) authentication.
6. If the user specified a UNIX user name and password, RADIUS performs a UNIX login.
7. If you have configured token-card authentication, RADIUS forwards the connection request to an external authentication server, such as a Security Dynamics ACE/Server or Enigma Logic SafeWord server.
8. The RADIUS server sends an authentication response to the MAX TNT. If authentication is unsuccessful, the connection is refused. If authentication is successful, the MAX TNT receives a list of attributes from the user profile in the RADIUS server's database and establishes network access for the caller.
9. The MAX TNT notifies the RADIUS server that the session has begun. The MAX TNT also notifies the RADIUS server when the session ends. If you have accounting enabled, the RADIUS server can generate accounting records.

How does RADIUS accounting work?

RADIUS accounting, specified in IETF RFC 2059, is a way to log information about three types of events:

- Start session. Denotes the beginning of a session with the MAX TNT. Information about this event appears in an accounting Start record.
- Stop session. Denotes the end of a session with the MAX TNT. Information about this event appears in an accounting Stop record.
- Failure-to-start session. Denotes that a login attempt has failed. Information about this event appears in an accounting Failure-to-start record.

When the MAX TNT 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 TNT transmitted and received, the protocol in use, the user name and IP address of the client, and so on.

You can use RADIUS accounting to:

- Gather billing information, including who called, how long the session lasted, and how much traffic occurred during the session.
- Troubleshoot RADIUS and MAX TNT 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.

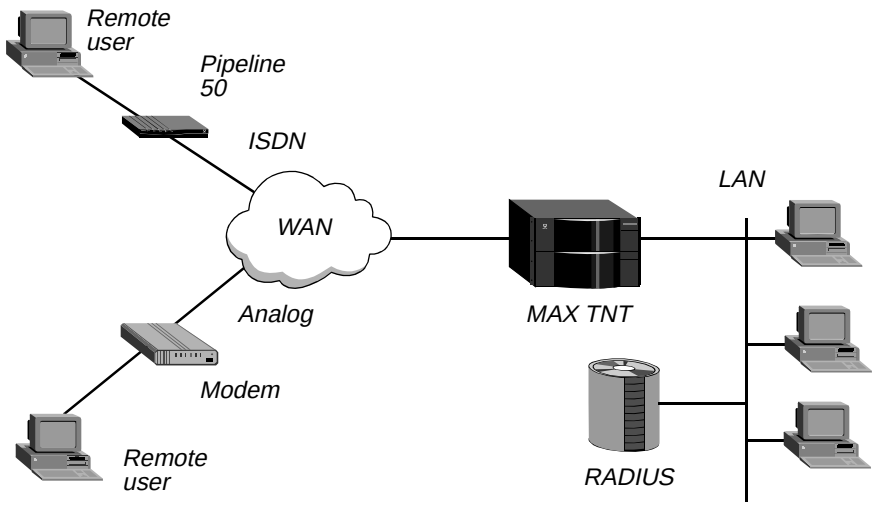

Figure 1-1. RADIUS authentication and accounting

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 TNT 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.

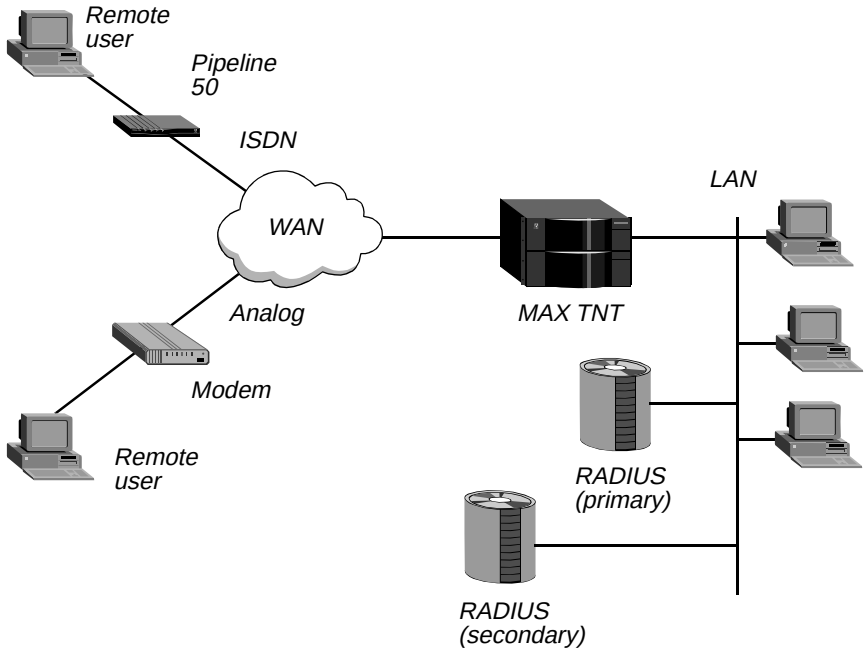

Figure 1-2. RADIUS authentication and accounting with a backup server

RADIUS with an external token-card server

For more secure networks, a service provider or corporate office can use RADIUS as a front end to a token-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, a MAX TNT functioning as a Network Access Server (NAS), a RADIUS server, and an external token-card server.

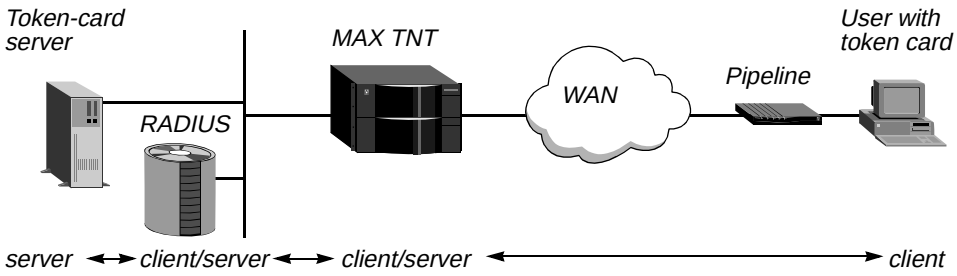

Figure 1-3. RADIUS with an external token-card server

For complete information about configuring RADIUS to work with token-card authentication servers, see the *MAX TNT Network Guide*.

Using RADIUS to sign up new customers

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

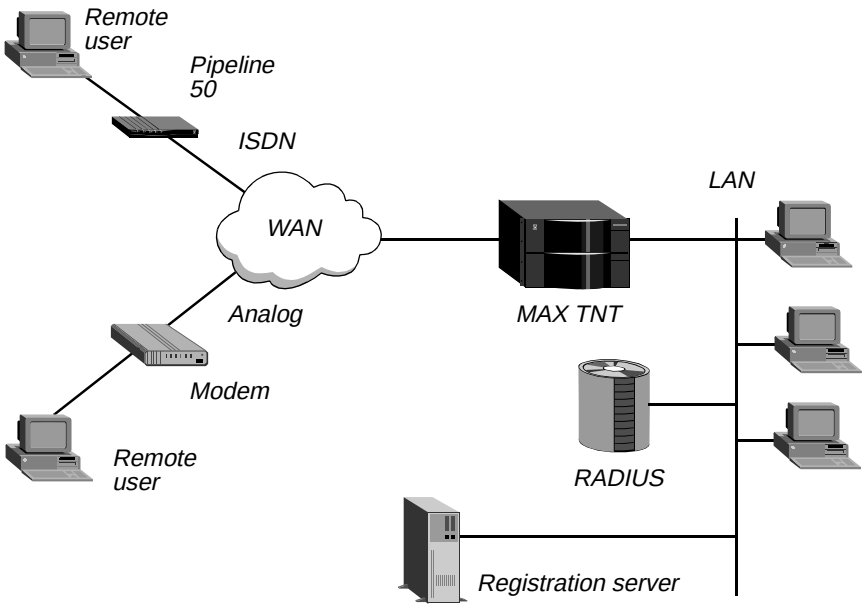

Figure 1-4. Using RADIUS to sign up new customers

A user cannot access any other resource on the system before providing all the registration details and signing 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`	RADIUS daemon for a flat ASCII `users` file. You must use the Ascend RADIUS daemon, version 1.16 (dated 7/25/95) or later if you require RADIUS accounting or any of the Ascend extensions to the RADIUS daemon defined by IETF RFC 2058. For information about running the `radiusd` daemon, see "Running the daemon with a flat ASCII users file" on page 2-19.
`radiusd.dbm`	`/etc/raddb`	RADIUS daemon for a UNIX DBM database. You must use the Ascend RADIUS daemon, version 1.16 (dated 7/25/95) or later if you require RADIUS accounting or any of the Ascend extensions to the RADIUS daemon defined by IETF RFC 2058. For information about running the `radiusd.dbm` daemon, see "Running the daemon with a UNIX DBM database" on page 2-21.
`dictionary`	`/etc/raddb`	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 restart it to make the new attributes available. For further information about the `dictionary` file, see "The dictionary file" on page 1-7.
`clients`	`/etc/raddb`	File that identifies each client that can send requests to the RADIUS server. For overview information about the `clients` file, see "The clients file" on page 1-8. For details about setting up the `clients` file, see "Creating and configuring the clients file" on page 2-3.

Table 1-1. RADIUS files (continued)

File name	Default location	Description
`users`	`/etc/raddb`	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 TNT features to which the user has access. For introductory information about the `users` file, see "The users file" on page 1-8.
`logfile`	`/etc/raddb`	File containing error messages. You must create this file yourself.
`detail`	`/usr/adm/`*`NAS-name`*`/radacct`	File containing accounting records.

The `dictionary` file

Every attribute has a 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. Format of the `dictionary` file

Attribute element	Description
Name	ASCII string denoting the attribute, such as User-Name or Password.
ID	Number from 1 to 255 associated with each attribute. For example, the User-Name attribute is attribute 1 and the Password attribute is attribute 2.
Value type	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 the following:

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

The `clients` file

A client is the MAX TNT 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 TNT, you must enter a line specifying the MAX TNT unit's name and password in the `clients` file. For example:

```
Ascend3    bXSAMpy
```

The `users` file

The `users` file is a text file that can contain both user profiles and pseudo-user profiles.

- A user profile is an entry for a user that RADIUS will authenticate. It consists of attributes describing a user and the services he or she can access.
- A pseudo-user profile is an entry containing information that the MAX TNT 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, and other types of data.

Note: Every attribute name and value is case sensitive. For more complete information about setting up the `users` file, see "Using the RADIUS interface" on page 1-12 and Appendix D, "Sample RADIUS Users File."

Overview of RADIUS packet formats

Each RADIUS packet consists of the fields listed in Table 1-3.

Table 1-3. RADIUS packet fields

Element	Description
Code (8 bits)	Specifies the packet type. For a list of packet types, see Table 1-4 on page 1-9.
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 packet size in bytes.

Table 1-3. RADIUS packet fields (continued)

Element	Description
Authenticator (16 bytes)	Authenticates packets between the NAS and the authentication server. The NAS and the authentication server share a secret that the system uses, along 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 TNT checks all authentication and accounting packets to ensure that they come from known sources. The check makes use of the shared secret, the authenticator field, and MD5 encoding. In addition, all passwords that the MAX TNT 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 the following fields: Attribute ID (8 bits)—These IDs are 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 1-4 lists the packet types that can appear in the code field.

Table 1-4. Code field packet types

Number	Name	Description
1	Access-Request	Access request that the MAX TNT sends to the RADIUS server on behalf of a client attempting to establish a connection.
2	Access-Accept	Packet sent by the RADIUS server to inform the MAX TNT that a client's request for access has been granted.
3	Access-Reject	Packet the RADIUS server sends to inform the MAX TNT that it has not granted a client's request for access. The RADIUS server sends this packet if the user: • Enters an unknown user name • Fails to enter the correct password • Enters an expired password

Table 1-4. Code field packet types (continued)

Number	Name	Description
4	Accounting-Request	Request for accounting information that the MAX TNT sends to the RADIUS accounting server.
5	Accounting-Response	Packet containing accounting information that the RADIUS accounting server sends to the MAX TNT.
7	Access-Password-Request	Password-change request that the MAX TNT sends to the RADIUS server.
8	Access-Password-Ack	Response from the RADIUS server informing the MAX TNT that the new password has been accepted.
9	Access-Password-Reject	Response from the RADIUS server informing the MAX TNT that the new password has been rejected.
11	Access-Challenge	Request for the user to enter a password with a hand-held token card. The authentication server sends this packet through the RADIUS server and the NAS to the user.
26	Vendor-Specific	Encapsulates attributes introduced by vendors.
29	Ascend-Access-Next-Code	Response from the RADIUS server informing the MAX TNT that it should request access again, but with the next password in the sequence.
30	Ascend-Access-New-Pin	Response from the RADIUS server informing the MAX TNT that it should request access again, but with the next PIN in the sequence.

Table 1-4. Code field packet types (continued)

Number	Name	Description
32	Ascend-Password-Expired	Response from the RADIUS server to the MAX TNT 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 TNT 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	Packet containing a notification that the MAX TNT has started up, or a request for the RADIUS server to record the number of open sessions.
34	Ascend-Access-Event-Response	Response from the RADIUS server reporting that the MAX TNT has started up or specifying the number of sessions, and informing the MAX TNT that the server has received and recorded the MAX TNT unit's ID.
40	Disconnect-Request	Message from a client of the MAX TNT asking it to disconnect the session.
41	Disconnect-Request-ACK	Message the MAX TNT sends to the client if it found at least one session to disconnect.
42	Disconnect-Request-NAK	Message the MAX TNT sends to the client if it could not find a session to disconnect.
43	Change-Filter-Request	Request to change the filters for a routing session.
44	Change-Filter-Request-ACK	Message the MAX TNT sends if it found at least one routing session for which filters could be changed.
45	Change-Filter-Request-NAK	Message the MAX TNT sends if it could not find a routing session for which filters could be changed.

Using the RADIUS interface

To set up RADIUS, you must configure attributes in the `users` file. Table 1-5 lists each element of the `users` file.

Table 1-5. Elements of the `users` file

Element	Description
Comment line	Begins with the # character at column one, followed by text that extends to the end of the line.
Pseudo-user profile	Consists of the same elements as the user profile, except that the attributes specify information that the MAX TNT can query, rather than authentication information. For information about the types of pseudo-user profiles you can specify, see "Understanding pseudo-user profiles" on page 1-13. For complete information about setting up pseudo-user profiles, see the *MAX TNT Network Guide*.
User profile	Consists of a first line (also called an *authentication line*), followed by the rest of the profile, including 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 TNT. Columns one and two may contain any characters except the # character, a space, or a tab. Starting at the third column, the first line may 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 must not appear within a profile, but may be present anywhere outside a profile. It must end with a newline.

When setting an attribute in a profile, you specify the name of the attribute, followed by an equal sign (=), followed by the attribute's setting. For attributes with predefined settings, you can spell out the full setting, or specify a numeric equivalent. For instance, you can set the User-Service attribute to Login-User (1) in either of the following ways:

```
User-Service=Login-User
```

```
User-Service=1
```

To see an example of a complete users file, see Appendix D, "Sample RADIUS Users File.".

Understanding pseudo-user profiles

A pseudo-user profile contains information that the MAX TNT 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, and other types of data.

Along with other attributes on the first line, the values you specify for User-Name and Password determine how the MAX TNT uses the profile. Table 1-6 describes how to set up the first line of a pseudo-user profile for various purposes. Each entry of the table contains a reference for information about completing the rest of the profile.

Some profiles use the following arguments:

- *name* is the system name of the Ascend unit (the name specified by the Name parameter in the System profile).
- *num* is a number in a sequential series, starting at 1.

Note: The first line of a pseudo-user profile cannot use newlines. The specifications appear on multiple lines here for printing purposes only.

Table 1-6. First-line configuration of pseudo-user profiles

Element configured	First-line specification
Outgoing calls	For the User-Name attribute, specify the name of the remote device that will receive outgoing calls, appending **`-Out`** to the user name. Then, set **`Password="ascend"`** and **`User-Service= Dialout-Framed-User`**. The User-Service setting ensures that no one can use the profile for authentication of an incoming call. For complete information, see the *MAX TNT Network Guide*.
Nailed/MPP connection	**`permconn-`*`name-num`*` Password="ascend", User-Service= Dialout-Framed-User`** For complete information, see the *MAX TNT Network Guide*.
Nailed-up connection	**`permconn-`*`name-num`*` Password="ascend", User-Service= Dialout-Framed-User`** For complete information, see the *MAX TNT Network Guide*.
Message text and list of hosts	For a configuration specific to a single MAX TNT unit: **`initial-banner-`*`name`*` Password="ascend", User-Service=Dialout-Framed-User`** For a configuration used by several MAX TNT units: **`initial-banner Password="ascend", User-Service= Dialout-Framed-User`** For complete information, see the *MAX TNT Network Guide*.
Frame Relay profile	**`frdlink-`*`name-num`*` Password="ascend", User-Service= Dialout-Framed-User`** For complete information, see the *MAX TNT Network Guide*.

Table 1-6. First-line configuration of pseudo-user profiles (continued)

Element configured	First-line specification
Frame Relay user profile	**permconn-*name*-*num* Password="ascend", User-Service= Dialout-Framed-User** For complete information, see the *MAX TNT Network Guide*.
IP address pools	**pools-*name* Password="ascend", User-Service= Dialout-Framed-User** For complete information, see the *MAX TNT Network Guide*.
Static IP routes	For an IP dialout route specific to a single MAX TNT unit: **route-*name*-*num* Password="ascend", User-Service= Dialout-Framed-User** For an IP dialout route used by several MAX TNT units: **route-*num* Password="ascend", User-Service= Dialout-Framed-User** For complete information, see the *MAX TNT Network Guide*.
Static IPX routes	For an IPX dialout route specific to a single MAX TNT unit: **ipxroute-*name*-*num* Password="ascend", User-Service= Dialout-Framed-User** For an IPX dialout route used by several MAX TNT units: **ipxroute-*num* Password="ascend", User-Service= Dialout-Framed-User** For complete information, see the *MAX TNT Network Guide*.

The following example of part of a `users` file includes 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. Each line of the profile, except the first line and last line, contains a trailing comma.

Installing and Starting RADIUS

2

Before you begin

This section describes:

- System requirements for running the RADIUS daemon.
- Tasks you must carry out at the MAX TNT configuration interface before performing the installation steps in this chapter.

System requirements

To use RADIUS with the MAX TNT, you need a UNIX workstation or PC to run the RADIUS daemon, and a TCP/IP connection between the RADIUS server and the MAX TNT. The supported platforms are:

- HP-UX
- SCO UNIX
- IBM AIX
- SunOS
- Solaris with GCC
- Solaris with CC
- UNIXWARE
- BSDI
- LINUX
- SGI UNIX

Configuring the MAX TNT

Before you install and configure RADIUS, you must carry out the following tasks at the MAX TNT configuration interface:

- Install the hardware.
- Set up call routing.
- Configure Ethernet ports.
- Configure T1 PRI or E1 PRI lines.

For details, see the *MAX TNT Hardware Installation Guide* and the *MAX TNT Network Guide*.

Overview of RADIUS installation tasks

No matter what kind of configuration exists at your site, you are required to carry out the following tasks:

- Install the RADIUS daemon, as described in “Installing the RADIUS daemon” on page 2-2.
- Configure the MAX TNT to use RADIUS, as described in “Configuring the MAX TNT to use the RADIUS server” on page 2-5.
- Start up the RADIUS daemon, as described in “Starting the RADIUS daemon” on page 2-19.

Depending on your configuration, you may also need to carry out the following additional tasks:

- Install RADIPAD for IP pools shared by several MAX TNT units. (For information, see “Installing RADIPAD for global IP pools” on page 2-5.)
- Configure the MAX TNT to accept client disconnect and filter-change requests. (For information, see “Configuring the MAX TNT for RADIUS client requests” on page 2-15.)

Installing the RADIUS daemon

To install the RADIUS daemon, you must perform the following tasks:

- Obtain and compile the RADIUS daemon.
- Install the Ascend RADIUS dictionary.
- Create and configure the `clients` file.
- Create the `users` file.
- Create the log file.
- Specify the MAX TNT unit’s name and IP address.
- Specify the RADIUS daemon’s authentication port.

Obtaining and compiling the RADIUS daemon

The installation instructions on the Ascend FTP server always provide the latest information about installing RADIUS. When you compile the daemon, be aware that 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.

To obtain and compile the RADIUS daemon:

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.
4. Use the appropriate makefile to compile the Ascend RADIUS daemon on your system.

Installing the Ascend RADIUS dictionary

The `dictionary` file is the Ascend RADIUS dictionary. It contains a list of all attributes that the RADIUS server supports.

You must install the dictionary in the same directory as the Ascend RADIUS daemon. By default, the RADIUS daemon resides in the `/etc/raddb` directory. The dictionary 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 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 restart it to make the new attributes available. For further information about the `dictionary` file, see "The dictionary file" on page 1-7.

Creating and configuring the `clients` file

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 TNT is an NAS and a client of the RADIUS server. For the RADIUS daemon to respond to requests from the MAX TNT, you must create a file called `clients` in the `/etc/raddb` directory, and then specify the MAX TNT unit's name and password in the file.

- For the name, enter the value specified by the System profile's Name parameter.
- For the password, enter the value specified by the Auth-Key parameter, which is in the Rad-Auth-Client subprofile of the External-Auth profile.

For example, add a line like the following to the `clients` file:

```
Ascend3    bXSAMpy
```

`Ascend3` is the value specified by the Name parameter. The argument **`bXSAMpy`** is the password specified by the Auth-Key parameter. 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 TNT.

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 Rad-Acct-Client subprofile of the External-Auth profile.

Creating the `users` file

Create a file called `users` in the `/etc/raddb` directory. A user is a caller that connects to the MAX TNT. 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 TNT 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 TNT unit's memory. RADIUS authentication occurs when the caller's name and password match a user profile in the RADIUS `users` file.

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

Creating the log file

Create a file called `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.

Specifying the MAX TNT unit's name and IP address

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

Specifying the RADIUS daemon's authentication port

Use a text editor to open the `/etc/services` file and add a line identifying the port on which the RADIUS daemon receives authentication requests.

For example:

```
RADIUS    1812/udp
```

The port number you specify must match the port number indicated by the Auth-Port parameter in the Rad-Auth-Client subprofile of the External-Auth profile.

Installing RADIPAD for global IP pools

You can use RADIUS to specify pools of IP addresses that a MAX TNT can use to dynamically allocate IP addresses to incoming callers. By default, each MAX TNT handles dynamic IP address allocation individually from a pool of addresses preassigned to each MAX TNT.

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, the central manger for global IP address pools on a network. Although multiple hosts can run the RADIUS daemon, only one host on the network should run RADIPAD.

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

To install RADIPAD:

1. Copy RADIPAD to the same directory in which you installed the RADIUS daemon.
2. In the `/etc/services` file on the host containing RADIPAD, specify the port number the RADIUS daemon uses when running RADIPAD, as in the following example:

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

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
   ```

For information about configuring global IP address pools, follow the instructions in the *MAX TNT Network Guide*.

Configuring the MAX TNT to use the RADIUS server

This section describes how to configure the MAX TNT to communicate with the RADIUS daemon. You use the MAX TNT configuration interface to carry out each step. Some steps are required for all configurations. Others are optional, and depend on the needs of your site. For complete information about each parameter you set, see the *MAX TNT Reference Guide*.

Note: This section describes the basic configuration procedure. It does not cover how to configure RADIUS for accounting purposes. For information about setting up accounting, see Chapter 4, “Setting Up RADIUS Accounting.”.

Performing the required configuration steps

When configuring the MAX TNT to use RADIUS, you must specify:

- Type of authentication in use
- IP address of at least one RADIUS server
- UDP port number for the daemon
- RADIUS client password

You can have up to three RADIUS servers on your network. One is the primary server. Two additional servers can function as backups. If the primary RADIUS server fails, the MAX TNT automatically contacts the secondary RADIUS server to authenticate a user. When it successfully connects to an authentication server, the MAX TNT uses that machine until it fails to serve requests. By default, the MAX TNT does not revert to using 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 TNT use the first host again. For details, see "Using SNMP to specify the primary RADIUS server" on page 2-14.

To specify settings required for RADIUS operation:

1. In the External-Auth profile, set the Auth-Type parameter to RADIUS.
2. Open the Rad-Auth-Client subprofile.
3. For each Auth-Server parameter, specify the IP address of a RADIUS server.

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

   If you specify the same address for all three Auth-Server parameters, the MAX TNT keeps trying to create a connection to the same server.
4. Set the Auth-Port parameter to the destination UDP port number on which the RADIUS daemon receives client requests. Specify the same number you set for the daemon in the `/etc/services` file.
5. Set the Auth-Key parameter to the RADIUS client password you specified in the RADIUS `clients` file. (The password is case sensitive.)

Performing the optional configuration steps

Depending on your needs, you can set parameters to:

- Configure distinct ID sequence spaces for packet IDs.
- Specify how the system behaves when the User-Service (6) attribute is not received.
- Fine-tune the interaction between the MAX TNT and RADIUS.
- Specify the duration of a RADIUS timeout.
- Specify the message resulting from a RADIUS timeout.
- Configure Vendor-Specific Attribute (VSA) support.
- Specify the manner in which the MAX TNT handles the User-Name attribute.
- Specify whether to customize the User-Name string.

The following sections describe the kinds of settings you can make.

Configuring distinct ID sequences for packet IDs

RADIUS uses an ID value to aid in Request-Response matching. By default, the MAX TNT uses a single sequence space for the RADIUS ID number in all RADIUS messages, which limits the number of IDs available for assignment to 256. A combined total of 256 authentication and accounting packets are sent before the ID sequence rolls over. However, by setting Rad-ID-Space=Distinct in the External-Auth profile, you can configure distinct ID sequence spaces for RADIUS accounting and authentication packets.

When you set Rad-ID-Space=Distinct, RADIUS authentication and accounting packets do not share the same ID sequence space. The MAX TNT can send a total of 256 authentication packets before the authentication ID sequence rolls over, and 256 accounting packets before the accounting ID sequence rolls over.

When you configure the MAX TNT to use distinct ID sequence spaces, the RADIUS server must perform additional checks for duplicate detection. The server should check the RADIUS ID value as well as the service type and destination UDP port in each packet. The service type can be determined by sorting all values of the code field into two classes—Auth and Acct—and then comparing the received code value to determine to which class it belongs. The destination UDP port can be the same for both services when a single RADIUS server performs them.

Specifying how the system behaves when User-Service (6) is not received

When NoAttr6-Use-Termsrv=Ye s in the External-Auth profile (the default), the MAX TNT initiates a terminal-server login if the User-Service attribute is not received, regardless of whether the Frame-Protocol (7) attribute is received or not.

If you set NoAttr6-Use-Termsrv=No, the following behavior occurs:

- If User-Service is not received, but Framed-Protocol is received, a framed-protocol login is initiated.
- If neither User-Service nor Framed-Protocol is received, a terminal-server login is initiated.

Fine-tuning the interaction between the MAX TNT and RADIUS

All the steps that follow set parameters in the External-Auth profile's Rad-Auth-Client subprofile. To fine-tune the interaction between the MAX TNT and RADIUS, proceed as follows:

1. Set the Auth-Pool parameter to specify whether the MAX TNT sends the IP address derived from pool #1 to the RADIUS server during an authentication request. (For information about the Auth-Pool parameter, see "Setting up accounting with dynamic IP addressing" on page 4-10.)
2. Set Auth-Rsp-Required=Yes to enforce Calling-Line ID (CLID) authentication for connections that require it. (For detailed information about CLID authentication, see the *MAX TNT Network Guide*
3. Set the Local-Profiles-First parameter to specify whether the MAX TNT first checks for a local Connection profile when attempting to authenticate a connection.
4. Set the Auth-Sess-Interval parameter to specify the interval in seconds at which the MAX TNT sends session reports.

5 Set the Auth-Src-Port parameter to a value representing the MAX TNT unit's UDP source port for sending RADIUS authentication requests. (You can specify the same value for authentication and accounting requests.)

6 If your RADIUS user profiles enable both framed and unframed users to access PPP, set Auth-Send67=No. A framed user dials in using a protocol such as SLIP or MP+. An unframed user makes an asynchronous connection to the terminal server, and can start Telnet, Rlogin, or raw TCP sessions.

7 Set the Auth-ID-Max-Retry-Time parameter to specify a maximum time limit for RADIUS CLID or DNIS authentication retries.

Specifying the duration of a RADIUS timeout

In the Rad-Auth-Client subprofile of the External-Auth profile, set the Auth-Timeout parameter to the number of seconds the MAX TNT waits for a response to a RADIUS authentication request. If you have a high volume of calls, consider a low value for Auth-Timeout. A high timeout value combined with a high call volume can significantly slow the process of authenticating calls. However, if RADIUS is running on a busy shared UNIX host, or if the RADIUS server is on the remote end of a slow link, consider increasing the timeout value above the default of 1 second.

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

Note: If you are not using the Ascend RADIUS daemon, the MAX TNT is limited to 256 session IDs. In this case, you must make sure that the timeout period is short enough that all session IDs are not used up while the MAX TNT is waiting for an authentication response. If you are using the Ascend RADIUS daemon, the MAX TNT is not limited to 256 session IDs. In this case, a lower timeout value will help you eliminate delays in call authentication, but you need not concern yourself with a limitation on session IDs.

Specifying the message resulting from a RADIUS timeout

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. If Windows '95 (MSN) receives the LCP-CLOSE during authentication, it displays an invalid-password message. This message is misleading if the failure resulted from a RADIUS timeout.

When you set Disconnect-On-Auth-Timeout=Yes in the Answer-Defaults profile's PPP-Answer subprofile, the resulting message to the user states that the network failed.

Configuring Vendor-Specific Attribute (VSA) support

RFC 2138, *Remote Authentication Dial In User Service (RADIUS)*, specifies methods of handling vendor extensions and of encrypting and decrypting the User-Password. The RFC-defined methods differ from the way Ascend has implemented these functions in the past. In the past, Ascend extended RADIUS operations by adding Ascend vendor attributes, such as Ascend-Xmit-Rate, and used its own Ascend algorithm for User-Password encryption.

Now, you can configure the MAX TNT with support for the Vendor-Specific Attribute (VSA) and the RFC-defined User-Password encryption algorithm. Ascend maintains backward compatibility by making VSA compatibility mode configurable. However, new Ascend attributes (attributes of Type 91 or smaller) will be available only in VSA compatibility mode. Current Ascend attributes (attributes of Type 92 or higher) are available in both VSA compatibility mode and the default mode, which is compatible with older Ascend implementations.

About the Vendor-Specific attribute

RFC 2138 defines the Vendor-Specific attribute (type 26), which encapsulates attributes introduced by vendors. The purpose of the Vendor-Specific attribute is to enable companies to extend RADIUS operations without leading to possible attribute collisions (two attributes with the same type number but different meanings).

The format of Ascend vendor attributes in a request or response is new. The older Ascend format for all attributes is as follows:

```
 0                   1                   2
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
|     Type      |    Length     | Value ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

The format of the VSA (as defined in RFC 2138) is as follows:

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 Vendor-Id (cont)           | Vendor type   | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Attribute-Specific...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

The Type of the VSA is 26. The Length is 8 or greater. Ascend's Vendor-Id is 529.

The Vendor Type, Vendor Length, and Attribute-Specific Value are the same as the Type, Length, and Value of the unencapsulated Ascend attribute found in the current dictionary. For example, the Type of the Ascend-Xmit-Rate attribute is 255. Because it is an integer, it has a Length of 6. The Value is the transmit rate of the connection. So, the fields of the VSA will specify the following values:

- Type=26
- Length=12
- Vendor-Id=529
- Vendor Type=255
- Vendor Length=6
- Attribute-Specific Value=*transmit-rate*

Note: Some vendors have interpreted RFC 2138 to allow packing more than one vendor attribute in a single VSA. Ascend does not support this use. The MAX TNT sends a single vendor attribute per VSA. If it receives a VSA that contains more than one vendor attribute, it recognizes the first vendor attribute and ignores the rest.

Configuring the MAX TNT for VSA compatibility mode

In VSA compatibility mode, the MAX TNT uses the Vendor-Specific attribute to encapsulate Ascend vendor attributes and uses the RFC-defined User-Password encryption algorithm.

In the Old compatibility mode (the default), the MAX TNT does not send the Vendor-Specific attribute to the RADIUS server and does not recognize it if the server sends it. In this mode, the system uses the Ascend algorithm of encrypting and decrypting the User-Password attribute, which differs from the RFC-defined algorithm in that it does not null fill the password string to a multiple of 16 bytes before encryption, and it does not use the previous segment's hash to calculate the next intermediate value when the password is longer than 16 bytes.

Because administrators can configure RADIUS for four different purposes, with each function operating independently of the others and possibly interacting with different RADIUS servers (or clients), four separate parameters are provided for specifying whether to operate in the older Ascend compatibility mode or in VSA compatibility mode. Proceed as follows:

1 To enable VSA compatibility mode when the MAX TNT is using RADIUS for authentication and authorization purposes, set Auth-RADIUS-Compat=Vendor-Specific in the Rad-Auth-Client subprofile of the External-Auth profile.

2 To enable VSA compatibility mode when the MAX TNT is acting as a RADIUS server that is able to accept some requests for certain limited purposes (such as to change filters or disconnect a user), set RADIUS-Server-Compat=Vendor-Specific in the Rad-Auth-Client subprofile of the External-Auth profile.

3 To enable VSA compatibility mode when the MAX TNT is using RADIUS for accounting purposes, set Acct-RADIUS-Compat=Vendor-Specific in he Rad-Acct-Client subprofile of the External-Auth profile.

4 To enable VSA compatibility mode when the MAX TNT is using RADIUS for call logging to NavisAccess, set Call-Log-RADIUS-Compat in the Call-Logging profile.

Specifying the manner in which the MAX TNT handles the User-Name

The RADIUS server typically returns the User-Name attribute in each Access-Accept packet. When the proxy RADIUS server responds for several RADIUS servers that belong to different organizations, including a User-Name attribute can result in the loss of realm information. To specify the manner in which the MAX TNT handles the User-Name attribute, proceed as follows:

1. Make External-Auth > Rad-Auth-Client the working profile.
2. To specify that the User-Name value provided by the server is used for the status display and for RADIUS accounting purposes, accept the default of Change-Name for the Auth-Keep-User-Name attribute. Then, proceed to step 5.
3. To specify that the MAX TNT does not use the User-Name value returned by the server, set Auth-Keep-User-Name=Keep-Name. If a name has been specified, the system uses it. Otherwise, it uses the User-Name sent to the server for authentication. A user authenticated by CLID or DNIS will appear to have the CLID or DNIS number as his or her user name.
4. When the user name sent to the server is a realm, you can specify that the system behaves as though the setting were Keep-Name. To do so, set Auth-Keep-User-Name to Keep-Realm-Name. (If the user name sent to the server is not a realm, the system behaves as though the setting were Change-Name.)
5. To specify the characters that delimit a realm from the user name, set the Auth-Realm-Delimiters parameter. You can specify up to seven characters in any order. If no characters are listed, the system behaves as though Auth-Keep-User-Name were set to Change-Name. The default is `@/\%`.

Specifying whether to customize the User-Name string

To enable a proxy RADIUS server that does not have the shared secret to distinguish between pseudo-user and real user authentication requests, you can customize the User-Name string presented to the RADIUS server during CLID or DNIS authentication. To do so, specify up to 16 characters for the ID-Auth-Prefix setting in the Rad-Auth-Client subprofile. The specified string is inserted as a prefix to the phone number in CLID or DNIS authentication requests to the RADIUS server. The RADIUS server can then forward different types of requests to different servers.

Example of configuring the MAX TNT to use the RADIUS server

The configuration illustrated in Figure 2-1 uses three RADIUS servers. Clients dialing in across the WAN use both framed and unframed protocols on analog and digital lines. The RADIUS daemon for each server receives client requests on UDP port 512, and the client password is `tntpass`.

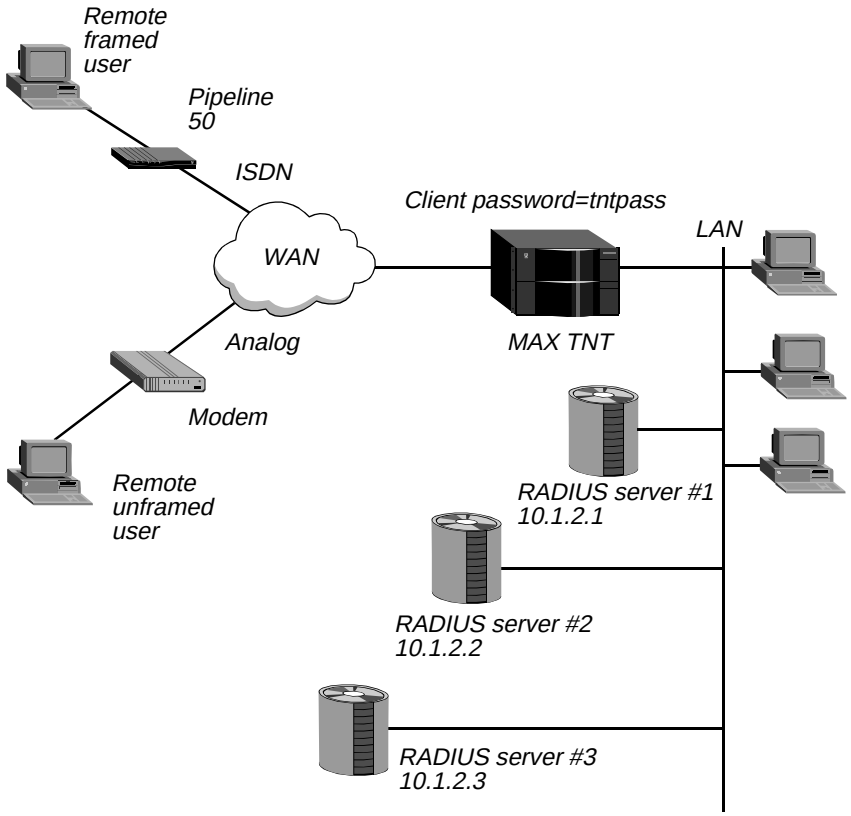

Figure 2-1. Sample network topology for setting up the MAX TNT to use the RADIUS server

In addition to the required parameters, the configuration specifies that the MAX TNT must:

- Use distinct ID sequences to increase the number of concurrent sessions.
- Enforce CLID authentication for all remote users.
- Check for a RADIUS profile before a local Connection profile.
- Send session reports every 60 seconds.
- Use UDP source port 500 for sending authentication requests.
- Allow both framed and unframed users to access PPP.
- Increase the timeout value to 10 seconds.

To set the values for the sample configuration, you would proceed as follows:

```
admin> read external-auth
EXTERNAL-AUTH read

admin> set auth-type=radius

admin> set rad-id-space=distinct

admin> list rad-auth-client
[in EXTERNAL-AUTH:rad-auth-client]
auth-server-1=0.0.0.0
auth-server-2=0.0.0.0
auth-server-3=0.0.0.0
auth-port=0
auth-src-port=0
auth-key=""
auth-pool=no
auth-timeout=0
auth-rsp-required=no
auth-id-fail-return-busy=no
auth-id-timeout-return-busy=no
auth-sess-interval=0
auth-TS-secure=yes
auth-Send67=yes
auth-frm-adr-start=no
auth-boot-host=0.0.0.0
auth-boot-host-2=0.0.0.0
auth-boot-port=0
auth-reset-time=0
auth-id-max-retry-time=0
auth-radius-compat=old-ascend
auth-keep-user-name=change-name
auth-realm-delimiters=/\@%
id-auth-prefix=””

admin> set auth-server-1=10.1.2.1

admin> set auth-server-2=10.1.2.2

admin> set auth-server-3=10.1.2.3

admin> set auth-port=512

admin> set auth-key=tntpass

admin> set auth-rsp-required=yes

admin> set local-profiles-first=lpf-no

admin> set auth-sess-interval=60

admin> set auth-src-port=500

admin> set auth-send67=no

admin> set auth-timeout=10

admin> write external-auth
EXTERNAL-AUTH written
```

Using SNMP to specify the primary RADIUS server

By default, if the MAX TNT switches to a secondary RADIUS authentication server because the primary server goes out of service, the MAX TNT does not use the first host again until the second machine fails. However, you can use an SNMP Set command to specify that the MAX TNT 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 with the Set command, the MAX TNT generates an SNMP trap. The MAX TNT 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).

The following MIB objects support changing the current RADIUS authentication server:

```
radAuthHostIPAddress OBJECT-TYPE
   SYNTAX  IpAddress
   ACESS   read-only
   STATUS  mandatory
   DESCRIPTION "The IP address of the Authentication server.
   The value 0.0.0.0 is returned if entry is invalid."
   ::= { radiusAuthStatsEntry 11 }
radAuthCurrentServerFlag OBJECT-TYPE
   SYNTAX       INTEGER {
                    standby(1),
                    current(2)
                }
   ACCESS       read-write
   STATUS       mandatory
   DESCRIPTION  "Value indicates whether this entry is the
   current authentication server or not. Writing any value
   will cause the current server to be reset to the primary
   server (Host #1)."
   ::= { radiusAuthStatsEntry 12 }
```

Configuring the MAX TNT for RADIUS client requests

As an option, you can configure the MAX TNT to accept RADIUS requests from clients to disconnect a link or change filters for a particular session, user, or IP address. To do so, you need to write your own RADIUS client software that performs disconnects or changes filters. Then, you need to set up the MAX TNT and set several RADIUS attributes.

This section describes how to set up the MAX TNT to handle RADIUS client requests. (For detailed information about specifying disconnects in RADIUS, see the *MAX TNT Network Guide*. For detailed information about specifying filter changes in RADIUS, see the *MAX TNT Network Guide*.)

The process of configuring the MAX TNT for client requests involves both required and optional steps. You perform all the steps by setting parameters in the Rad-Auth-Server subprofile of the External-Auth profile.

Performing the required steps for client requests

You must specify the clients permitted to make requests, and the secret shared between each client and the RADIUS server.

Specifying the clients permitted to make RADIUS requests

To specify the clients permitted to make RADIUS requests, you must use one of the following settings:

- Set one or more Auth-Client parameters to the IP address of a device that can make RADIUS requests.
- Set one or more Auth-Netmask parameters to a range of addresses corresponding to devices permitted to make RADIUS requests.

Specify each IP address or range in dotted decimal notation. The default value is 0.0.0.0. A value of 0.0.0.0 disables the associated parameter. At least one of the parameters must contain an IP address other than 0.0.0.0 for client support to be active.

For example, you can specify values like the following:

- Auth-Client-1=135.50.248.76. This setting specifies the single address of 138.50.248.76.
- Auth-Client-2=255.255.255.255. This setting specifies that the RADIUS server can accept requests from any client.
- Auth-Netmask-1=125.65.5.0/24. This setting specifies any addresses from the 125.65.5 subnet.
- Auth-Netmask-2=125.5.0.0/16. This setting specifies any addresses from the 125.5 subnet.

Specifying the shared secret

Set the Auth-Key parameter to specify the secret shared by each client and the RADIUS server. You can specify a different secret for each client, or specify the same one. RADIUS uses the key to validate the authenticator field in requests and to generate the authenticator for responses. You can enter up to 20 characters.

Performing the optional steps for client requests

When setting up the MAX TNT to accept client requests, you can perform the following optional tasks:

- Specify the UDP port number for client requests.
- Specify session key parameters.

Specifying the UDP port

To indicate the number of the destination UDP port on which the RADIUS server receives client requests, set the Auth-Port parameter. You can enter an integer from 1 to 65535. The default value is 1700. Although the value can match the port setting for RADIUS authentication or accounting, Ascend recommends that you specify a different port.

Specifying session key parameters

If you want the client to send a session key to the RADIUS server, set the Auth-Session-Key parameter to Yes. The session key associates the client request with the user session. When you specify Yes, the client sends a session key specified by the Ascend-Session-Svr-Key attribute. When you specify No, the client does not send a session key. The default value is No.

If you set Auth-Session-Key=Yes, you must set the Auth-Attribute-Type parameter to specify the attributes required for identification of a user session. You can specify one of the following values:

- Rad-Serv-Attr-Any allows the RADIUS server to use any attribute to identify the user session. If the user sends multiple attributes, the RADIUS checks them in the following order:
  - Ascend-Session-Svr-Key (session key)
  - Acct-Session-Id (session ID)
  - User-Name (user name)
  - Framed-Address (IP address)
- Rad-Serv-Attr-Key indicates that the RADIUS server uses only the server key (the value of Ascend-Session-Svr-Key) to identify the session.
- Rad-Serv-Attr-All indicates that a client must send all applicable attributes, and these attributes must 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, a client must send all four attributes to the RADIUS server, and all these attributes must pass validation. However, if a session has only an associated user name, session ID and session key, the client needs to send only those attributes. The IP address is not required.

Example of setting up the MAX TNT to accept client requests

In configuration illustrated in Figure 2-2, the following clients are authorized to make RADIUS requests:

- Client #1 at 135.50.248.76
- Client #2 at 145.55.248.76
- Client #3 at 125.60.5.1

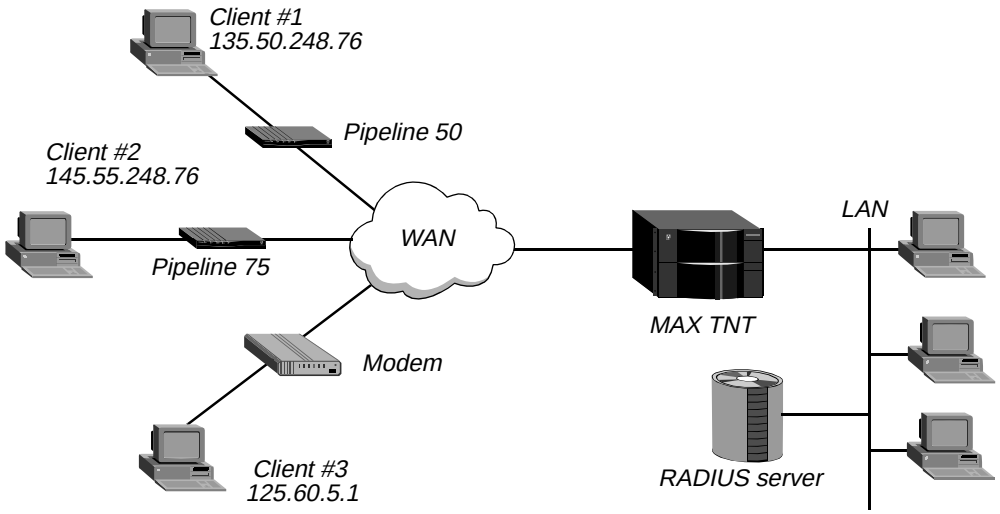

Figure 2-2. Sample network topology for setting up the MAX TNT to accept client requests

The shared secret is `secret001` for client #1, `secret002` for client #2, and `secret003` for client #3. Each client must send the session key specified by the Ascend-Session-Svr-Key attribute. To set the values for the sample configuration, you would proceed as follows:

```
admin> read external-auth
EXTERNAL-AUTH read

admin> list rad-auth-server
[in EXTERNAL-AUTH:rad-auth-server]
auth-port=1700
auth-session-key=no
auth-attribute-type=rad-serv-attr-any
auth-client=[ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0+
auth-netmask=[ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 +
auth-key=[ "" "" "" "" "" "" "" "" "" ]
```

```
admin> list auth-client
[in EXTERNAL-AUTH:rad-auth-server:auth-client]
auth-client[1]=0.0.0.0
auth-client[2]=0.0.0.0
auth-client[3]=0.0.0.0
auth-client[4]=0.0.0.0
auth-client[5]=0.0.0.0
auth-client[6]=0.0.0.0
auth-client[7]=0.0.0.0
auth-client[8]=0.0.0.0
auth-client[9]=0.0.0.0

admin> set 1=135.50.248.76

admin> set 2=145.55.248.76

admin> set 3=125.60.5.1

admin> list ..
[in EXTERNAL-AUTH:rad-auth-server:(changed)]
auth-port=1700
auth-session-key=no
auth-attribute-type=rad-serv-attr-any
auth-client=[ 135.50.248.76 145.55.248.76 125.60.5.1 0.0.0.0 0.0.0.0 +
auth-netmask=[ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 +
auth-key=[ "" "" "" "" "" "" "" "" "" ]

admin> list auth-key
[in EXTERNAL-AUTH:rad-auth-server:auth-key]
auth-key[1]=""
auth-key[2]=""
auth-key[3]=""
auth-key[4]=""
auth-key[5]=""
auth-key[6]=""
auth-key[7]=""
auth-key[8]=""
auth-key[9]=""

admin> set 1=secret001

admin> set 2=secret002

admin> set 3=secret003

admin> list ..
[in EXTERNAL-AUTH:rad-auth-server (changed)]
auth-port=1700
auth-session-key=no
auth-attribute-type=rad-serv-attr-any
auth-client=[ 135.50.248.76 145.55.248.76 125.60.5.1 0.0.0.0 0.0.0.0 +
auth-netmask=[ 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 +
auth-key=[ ********** ********* ********* "" "" "" "" "" "" ]

admin> set auth-session-key=yes

admin> set auth-attribute-type=rad-serv-attr-key

admin> write
EXTERNAL-AUTH written
```

Starting the RADIUS daemon

You can use one of two RADIUS daemons—`radiusd` or `radiusd.dbm`.

- Run `radiusd` with a flat ASCII `users` file.
- Run `radiusd.dbm` if you convert the flat ASCII `users` file to a standard UNIX DBM database.

RADIUS must search a flat ASCII file sequentially, which might increase 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, the new passwords take effect only after you rebuild the database. If resetting expired passwords is an important component of your system, the flat ASCII file might be the better choice.

Running the daemon with a flat ASCII `users` file

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

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

Table 2-1 lists each argument.

Table 2-1. List of radiusd arguments

Argument	Description
`-A` ***`acct`***	Controls the creation of the RADIUS accounting process. You can specify one of the following 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 specified for `radiusd` and uses that port number. This action is the default if you do not specify the `-A` argument.

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

Argument	Description
-a *acctdir*	Specifies the directory containing accounting records. By default, RADIUS stores accounting records in a file named `detail`, which resides in the `/usr/adm/radacct`. You can use the **-a** argument to specify a different directory for the file. The ***acctdir*** directory must already exist. For example, you might enter the following command line: **radiusd -a /home/radacct** The accounting process in the daemon creates a file named `detail`, which contains accounting records, in the `/home/radacct` directory.
-c	Enables Cache-Token authentication in the daemon.
-d *dbdir*	Specifies the directory containing the `clients`, `users`, `dictionary`, and log files. The default directory is `/etc/raddb`. You can use the **-d** argument to specify a different directory for the files. The ***dbdir*** directory must already exist. For example, you might enter the following command line: **radiusd -d /radius/raddb**
-p	Enables each user to change his or her own expired password through a dial-in modem connection.
-s	Specifies that the daemon runs in single-process mode, in which it 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*	Assigns the file name specified by ***usrfile*** to the RADIUS `users` file. The default name is `users`.
-v	Prints the daemon's version number, extension, date, and the arguments selected in the makefile compilation.
-w	Makes the RADIUS daemon generate warnings about syntax errors found in the `users` file when the daemon is running. RADIUS generates a warning only when the daemon examines the user 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	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 **`make dbm`**.

Creating the DBM database

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

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

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 list each argument for the `builddbm` command.

Table 2-2. List of builddbm arguments

Argument	Description
**`-d *dbdir***`	Specifies the directory containing the database files. The default output directory for the database files is `/etc/raddb`. You can use the **`-d`** argument to specify a different directory for the file. The ***`dbdir`*** directory must already exist. For example, you might enter the following command line: **`builddbm -d /radius/raddb`** This command results in two database files—`/radius/raddb/users.dir` and `/radius/raddb/users.pag`.
`-e`	Causes the `builddbm` program to report syntax errors and duplicate entries found 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`	Displays help.
**`-u *usrfile***`	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 specified 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`	Runs `builddbm` in verbose mode.

Starting the RADIUS daemon for a DBM database

To start the RADIUS daemon in DBM mode, enter the following 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 2-19, 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.

Reference to RADIUS Attributes

3

In the following listing of RADIUS attributes found in user and pseudo-user profiles, each entry provides information in the following 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.

Note: All RADIUS attributes and settings are case sensitive. Note that the name of an Ascend unit cannot contain embedded spaces.

Acct-Authentic (45)

Description: Indicates the method the MAX TNT used to authenticate a call, or reports that the MAX TNT accepted the call without authentication.

Usage: Acct-Authentic does not appear in a user profile. It can have either of the following values:

- RADIUS (1) indicates that RADIUS authenticated the incoming call. RADIUS is the default.
- Local (2) indicates that the MAX TNT authenticated the call by means of a local Connection profile, TACACS profile, or TACACS+ profile, or that the MAX TNT accepted the call without authentication.

Dependencies: The MAX TNT sends Acct-Authentic in an Accounting-Request packet under the following conditions:

- At the start of a session (when Acct-Status-Type=Start)
- At the end of an authenticated session (Acct-Status-Type=Stop)

Acct-Delay-Time (41)

Description: Indicates how many seconds the MAX TNT has been trying to send the Accounting packet.

Usage: Acct-Delay-Time does not appear in a user profile. Its default value is 0 (zero).

Dependencies: The MAX TNT sends Acct-Delay-Time in an Accounting-Request packet under the following conditions:

- At the start of a session (when Acct-Status-Type=Start)
- At the end of a session (when Acct-Status-Type=Stop)
- When a session has failed authentication (when Acct-Status-Type=Stop)

Acct-Input-Octets (42)

Description: Indicates how many octets the MAX TNT received during the session. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.

Usage: Acct-Input-Octets does not appear in a user profile. Its default value is 0 (zero).

Dependencies: The MAX TNT sends Acct-Input-Octets in an Accounting-Request packet, at the end of a session (Acct-Status-Type=Stop), when both of the following conditions are true:

- The session has been authenticated.
- The connection was asynchronous.

Acct-Input-Packets (47)

Description: Indicates how many packets the MAX TNT received during the session. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.

Usage: Acct-Input-Packets does not appear in a user profile. Its default value is 0 (zero).

Dependencies: The MAX TNT sends Acct-Input-Packets in an Accounting-Request packet, at the end of a session (Acct-Status-Type=Stop), when both of the following conditions are true:

- The session has been authenticated.
- A framed protocol is in use.

Acct-Output-Octets (43)

Description: Indicates how many octets the MAX TNT has sent during the session. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.

Usage: Acct-Output-Octets does not appear in a user profile. Its default value is 0 (zero).

Dependencies: The MAX TNT sends Acct-Output-Octets in an Accounting-Request packet, at the end of a session (Acct-Status-Type=Stop), when both of the following conditions are true:

- The session has been authenticated.
- The connection was asynchronous.

Acct-Output-Packets (48)

Description: Indicates how many packets the MAX TNT has sent during the session. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.

Usage: Acct-Output-Packets does not appear in a user profile. Its default value is 0 (zero).

Dependencies: The MAX TNT sends Acct-Output-Packets in an Accounting-Request packet, at the end of a session (Acct-Status-Type=Stop), when both of the following conditions are true:

- The session is authenticated.
- A framed protocol is in use.

Acct-Session-Id (44)

Description: Identifies the routing or terminal-server session reported in the Accounting-Request packet. RADIUS correlates the Accounting Start packet and Accounting Stop packet by means of Acct-Session-Id.

Usage: Acct-Session-Id does not appear in a user profile. Its value is a random number with a range from 1 to 2,137,383,647. For every session, RADIUS generates a unique session ID.

Dependencies: The MAX TNT sends Acct-Session-Id in an Accounting-Request packet under the following conditions:

- At the start of a session (when Acct-Status-Type=Start)
- At the end of a session (when Acct-Status-Type=Stop)
- When a session has failed authentication (when Acct-Status-Type=Stop)

In addition, consider the following:

- 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.
- At the MAX TNT configuration interface, you can use the Acct-Id-Base parameter to specify whether the numeric base of the Acct-Session-Id attribute is 10 or 16. For more information, see the *MAX TNT Reference Guide*.

Acct-Session-Time (46)

Description: Indicates how many seconds the session has been logged in.

Usage: Acct-Session-Time does not appear in a user profile. Its default value is 0 (zero).

Dependencies: The MAX TNT sends Acct-Session-Time in an Accounting-Request packet, at the end of a session (Acct-Status-Type=Stop), when the session has been authenticated.

Acct-Status-Type (40)

Description: Indicates whether the Accounting packet the MAX TNT sends to the RADIUS server reports the beginning (Start) or end (Stop) of a routing or terminal-server session.

Usage: Acct-Status-Type does not appear in a user profile.

Dependencies: The MAX TNT includes Acct-Status-Type in an Accounting-Request packet under the following conditions:

- At the start of a session (when Acct-Status-Type=Start)
- At the end of a session (when Acct-Status-Type=Stop)
- When a session has failed authentication (when Acct-Status-Type=Stop)

Ascend-Add-Seconds (240)

Description: 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 TNT begins adding bandwidth to a session. The MAX TNT determines the ALU for a session by applying the algorithm specified by the Ascend-History-Weigh-Type attribute.

When utilization exceeds the threshold for a period greater than the value of the Ascend-Add-Seconds attribute, the MAX TNT 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 an integer from 1 to 300. The default value is 5.

Dependencies: Consider the following:

- Additional channels must be available, and the number of channels the MAX TNT adds cannot exceed the number specified by the Ascend-Maximum-Channels attribute.
- Ascend-Add-Seconds and Ascend-Remove-Seconds have little or no effect on a system with a high Ascend-Seconds-Of-History value. If the value of Ascend-Seconds-Of-History is low, the Ascend-Add-Seconds and Ascend-Remove-Seconds attributes provide an alternative way to ensure that spikes must persist for a certain period of time before the system responds.

See Also: "Ascend-Base-Channel-Count (172)" on page 3-9,
"Ascend-DBA-Monitor (171)" on page 3-27,
"Ascend-Dec-Channel-Count (237)" on page 3-27,
"Ascend-History-Weigh-Type (239)" on page 3-44,
"Ascend-Inc-Channel-Count (236)" on page 3-47,
"Ascend-Maximum-Channels (235)" on page 3-53,
"Ascend-Minimum-Channels (173)" on page 3-57,
"Ascend-Remove-Seconds (241)" on page 3-68,
"Ascend-Seconds-Of-History (238)" on page 3-72, and
"Ascend-Target-Util (234)" on page 3-75.

Ascend-ARA-PW (181)

Description: Specifies the password of the incoming caller over an AppleTalk Remote Access (ARA) connection. The ARA software in the MAX TNT 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 TNT requires both entries.

Example: This example shows how to set 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 3-92.

Ascend-Assign-IP-Client (144)

Description: 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 the attribute. At present, the MAX TNT 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 3-6 and "Ascend-Assign-IP-Server (145)" on page 3-7.

Ascend-Assign-IP-Global-Pool (146)

Description: Specifies the global address pool from which RADIUS should assign each user an address.

A dynamic address comes from the pool of addresses you set up using the Pool-Base-Address and Assign-Count parameters in an IP-Global profile on the MAX TNT, the Ascend-IP-Pool-Definition attribute in a RADIUS profile, or both. An IP address pool you set up in RADIUS overrides an IP address pool you set up in the MAX TNT configuration interface, but only if you designate the two pools by the same number.

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 TNT requires the caller to use the static IP address the attribute specifies.

Example: In the following user profile, the host requests an address from the global address pool configured in the pseudo-user profile called global-pool-Alameda:

```
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-Global-Pool="Global-Pool-Alameda"
```

See Also: “Ascend-IP-Pool-Definition (217)” on page 3-48.

Ascend-Assign-IP-Pool (218)

Description: Specifies the address pool from which RADIUS assigns the user an IP address.

A dynamic address comes from the pool of addresses you set up by assigning values to the Pool-Base-Address and Assign-Count parameters in an IP-Global profile on the MAX TNT, the Ascend-IP-Pool-Definition attribute in a RADIUS profile, or both. An IP address pool you set up in RADIUS overrides an IP address pool you set up in the MAX TNT configuration interface, but only if you designate the two pools by the same number.

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 the following user profile, the host 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 3-48.

Ascend-Assign-IP-Server (145)

Description: 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 the attribute can appear in the profile. The default value is a placeholder only. You must specify a valid IP address for `radipad` to work.

Ascend-ATM-Vci (95)

Description: Specifies the Virtual Channel Identifier for an Asynchronous Transfer Mode (ATM) connection.

Usage: Specify a value from 32 to 1023. The default is 32. The maximum setting is determined by MAX TNT hardware capabilities.

Example: The following sample profile specifies Frame Relay to ATM switching:

```
permconn-yossi-1 Password="ascend", User-Service=Dialout-Framed-User
   Framed-Protocol=ATM-FR-CIR,
   Framed-Address=222.222.222.1,
   Framed-Netmask=255.255.255.0,
   Ascend-FR-Profile-Name="atm-30-sw",
   Ascend-Metric=2,
   Framed-Routing=None,
   Ascend-Idle-Limit=30,
   Ascend-Group="70",
   Acct-Authentic=None,
   Ascend-Send-Auth=Send-Auth-None,
   Ascend-Call-Type=Nailed,
   Ascend-FT1-Caller=FT1-Yes,
   Ascend-Route-IP=Route-IP-No,
   Ascend-ATM-Vpi=1,
   Ascend-ATM-Vci=43,
   Ascend-FR-Circuit-Name="adsl-atm",
   Ascend-Data-Svc=Nailed-64K
```

See Also: “Ascend-ATM-Vpi (94)” on page 3-7 and “Framed-Protocol (7)” on page 3-84.

Ascend-ATM-Vpi (94)

Description: Specifies the Virtual Path Identifier for an Asynchronous Transfer Mode (ATM) connection.

Usage: Specify a value from 0 to 15. The default is 0 (zero).

Example: The following sample profile specifies ATM encapsulation:

```
permconn-yossi-2 Password="ascend", User-Service=Dialout-Framed-User
   Framed-Protocol=ATM-1483,
   Framed-Address=222.222.222.1,
   Framed-Netmask=255.255.255.0,
   Ascend-FR-Profile-Name="atm-30",
   Ascend-Metric=2,
   Framed-Routing=None,
   Ascend-Idle-Limit=30,
   Ascend-Group="70",
   Acct-Authentic=None,
   Ascend-Send-Auth=Send-Auth-None,
   Ascend-Call-Type=Nailed,
   Ascend-FT1-Caller=FT1-Yes,
   Ascend-Route-IP=Route-IP-Yes,
   Ascend-ATM-Vpi=1,
   Ascend-ATM-Vci=42,
   Ascend-Data-Svc=Nailed-64K
```

See Also: “Ascend-ATM-Vci (95)” on page 3-7 and “Framed-Protocol (7)” on page 3-84.

Ascend-Authen-Alias (203)

Description: Sets the MAX TNT unit’s login name during PPP authentication.

When the MAX TNT 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 of up to 16 characters, with no spaces. The default is the value of the Name parameter in the System profile on the MAX TNT.

Example: The following example shows how to use the Ascend-Authen-Alias attribute in an outgoing profile:

```
Homer-Out Password="ascend", User-Service=Dialout-Framed-User
      User-Name="Homer",
      Ascend-Authen-Alias="myMAXTNTcallingU",
      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: Specifies the name of a backup profile for a nailed-up link.

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: Consider the following:

- The Ascend-Backup attribute applies to nailed-up connections only (Ascend-Call-Type=Nailed or Nailed/Mpp).
- Do not create nested backup connections.
- When you use the backup connection, the MAX TNT does not move routes to the backup profile. Therefore, the IP routes that appear in the terminal-server display might be incorrect, although statistical counts reflect the change.
- Do not use the Ascend-Backup attribute to provide alternative lines for getting to a single destination.
- The profile for a backup interface does not inherit features, such as filters or firewalls, from the profile for the primary nailed-up connection.

Ascend-BACP-Enable (133)

Description: 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: Specify one of the following settings:

- BACP-No (0) disables BACP for the link. BACP-No is the default.
- BACP-Yes (1) enables BACP for the link.

Ascend-Base-Channel-Count (172)

Description: Specifies the initial number of channels the MAX TNT sets up when originating calls for a PPP, MP, or MP+ 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.

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 the following values to the same number:

- Base channel count, as specified by Base-Channel-Count (in the Connection profile) or Ascend-Base-Channel-Count (in RADIUS).
- Minimum channel count, as specified by Minimum-Channels (in the Answer-Defaults profile or Connection profile) or Ascend-Minimum-Channels (in RADIUS).
- Maximum channel count, as specified by Maximum-Channels (in the Answer-Defaults profile or Connection profile) or Ascend-Maximum-Channels (in RADIUS).

See Also: "Ascend-Add-Seconds (240)" on page 3-4,
"Ascend-DBA-Monitor (171)" on page 3-27,
"Ascend-Dec-Channel-Count (237)" on page 3-27,
"Ascend-History-Weigh-Type (239)" on page 3-44,
"Ascend-Inc-Channel-Count (236)" on page 3-47,
"Ascend-Maximum-Channels (235)" on page 3-53,
"Ascend-Minimum-Channels (173)" on page 3-57,
"Ascend-Remove-Seconds (241)" on page 3-68,
"Ascend-Seconds-Of-History (238)" on page 3-72, and
"Ascend-Target-Util (234)" on page 3-75.

Ascend-Billing-Number (249)

Description: 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. 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 of up to ten characters, limited to the following:

```
1234567890()[]!z-*# |
```

Dependencies: The MAX TNT uses the Ascend-Billing-Number attribute differently for different types of lines:

- For a T1 line, the MAX TNT 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 applies only to installations in Australia.
- For a T1 PRI line, the MAX TNT uses the value of Ascend-Billing-Number rather than the phone number to identify itself to the answering party. In this situation, the Calling-Line ID (CLID) that the answering side receives is not the true phone number of the caller. This situation presents a security breach if you use CLID-Auth-Mode.

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 3-81.

Ascend-Callback (246)

Description: Enables or disables callback.

Callback occurs when the MAX TNT answers a call and verifies a name and password against a user profile. If Ascend-Callback=Yes, the MAX TNT hangs up and dials back to the caller by using the following 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 you set up a RADIUS user profile for callback and CLID-only authentication, the MAX TNT never answers the call. The caller therefore avoids billing charges.

Usage: Specify one of the following values:

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

See Also: "Ascend-Callback-Delay (108)" on page 3-11.

Ascend-Callback-Delay (108)

Description: Specifies the number of seconds the MAX TNT waits before calling back a remote user.

Usage: Specify an integer from 0 through 60. The unit treats values of 0–3 as 3 seconds. The default is 0 (zero).

Dependencies: If Ascend-Callback=Callback-No, Ascend-Callback-Delay does not apply.

See Also: "Ascend-Callback (246)" on page 3-11.

Ascend-Call-By-Call (250)

Description: Specifies the T1 PRI service that the MAX TNT uses when placing a PPP, MP, or MP+ call.

Usage: Specify a number corresponding to the type of service the MAX TNT uses. The default value is 6. Table 3-1 lists the services available for each service provider.

Table 3-1. Ascend-Call-By-Call settings

Number	AT&T	Sprint	MCI
0	Disable call-by-call service.	Reserved	N/A
1	SDN (including GSDN)	Private	VNET/Vision
2	Megacom 800	Inwatts	800
3	Megacom	Outwatts	PRISM1, PRISM II, WATS
4	N/A	FX	900
5	N/A	Tie Trunk	DAL
6	ACCUNET Switched Digital Services	N/A	N/A
7	Long Distance Service (including AT&T World Connect)	N/A	N/A
8	International 800 (I800)	N/A	N/A
16	AT&T MultiQuest	N/A	N/A

Ascend-Call-Filter (243)

Description: Specifies the characteristics of a call filter in a RADIUS user profile. The MAX TNT uses the filter only when it places a call or receives a call associated with the profile that includes the filter definition.

Usage: Filter entries apply on a first-match basis. Therefore, the order in which you enter them 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.

You can specify an IP filter or a generic filter. The following subsections describe how to configure each of the filter types.

IP call filter entries

Use the following format for an IP call filter entry:

Ascend-Call-Filter="ip *dir action* [dstip *dest_ipaddrsubnet_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 here for printing purposes only.

Table 3-2 describes each element of the syntax. None of the keywords are case sensitive.

Table 3-2. IP call filter syntax elements

Element	Description
ip	Specifies an IP filter.
dir	Specifies filter direction. You can specify **in** (to filter packets coming into the MAX TNT) or **out** (to filter packets going out of the MAX TNT).
action	Specifies the action the MAX TNT should take with a packet that matches the filter. You can specify either **forward** or **drop**.
dstip *dest_ipaddr* *subnet_mask*	The keyword **dstip** enables destination-IP-address filtering. 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 TNT compares only the masked bits. If you set ***dest_ipaddr*** to 0.0.0.0, or if the keyword and its IP address specification are not present, the filter matches all IP packets.
srcip *src_ipaddr* *subnet_mask*	The keyword **srcip** enables source-IP-address filtering. 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 TNT compares only the masked bits. If you set ***src_ipaddr*** to 0.0.0.0, or if the keyword and its specification are not present, the filter matches all IP packets.
proto	Specifies a protocol specified as a name or a number. The filter applies to packets whose protocol field matches this value.The supported names and numbers are `icmp` (1), `tcp` (6), `udp` (17), and `ospf` (89). If you set ***proto*** to 0 (zero), the filter matches any protocol.

Table 3-2. IP call filter syntax elements (continued)

Element	Description
dstport *cmp value*	The keyword **dstport** enables destination-port filtering. 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. The ***cmp*** argument defines 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*	The keyword **srcport** enables source-port filtering. 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. The ***cmp*** argument defines 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).

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 here for printing purposes only.

Table 3-3 describes each element of the syntax. None of the keywords are case sensitive.

Table 3-3. Generic call filter syntax elements

Element	Description
generic	Specifies a generic filter.
dir	Defines filter direction. You can specify **in** (to filter packets coming into the MAX TNT) or **out** (to filter packets going out of the MAX TNT).
action	Defines the action the MAX TNT should take with a packet that matches the filter. You can specify either **forward** or **drop**.
offset	Specifies 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 TNT applies the value of the ***mask*** argument. A mask hides the part of a number that appears behind the binary zeroes in the mask. The unit then compares the unmasked portion of the packet with the value specified by the ***value*** argument.
mask	Specifies which bits to compare in a segment of the packet. The mask must not 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	Specifies 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 TNT ignores the filter.
compare	Defines how the MAX TNT compares a packet's contents to the value specified by ***value***. You can specify == (for Equal) or != (for NotEqual). Equal is the default.
more	If present, specifies whether the MAX TNT 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 TNT ignores the **more** flag.

Example: The following 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"
```

The following 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 3-21.

Ascend-Call-Type (177)

Description: Specifies the type of nailed-up connection in use.

Usage: Table 3-4 lists the settings you can specify for Ascend-Call-Type.

Table 3-4. Ascend-Call-Type settings

Setting	Specifies
Nailed (1)	Link that consists entirely of nailed-up channels. Nailed is the default.
Nailed/Mpp (2)	Link that consists of both nailed-up and switched channels. The MAX TNT establishes the connection whenever any of its nailed-up or switched channels are connected end-to-end. If a Nailed/Mpp link is down and the nailed-up channels are down, the link cannot re-establish itself until the MAX TNT brings up one or more of the nailed-up channels, or dials one or more switched channels. Typically, the MAX TNT dials the switched channels 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 TNT replaces that channel with a switched channel, even if the call is online with more than the minimum number of channels. The MAX TNT always replaces failed nailed-up channels with switched channels, regardless of the Ascend-Minimum-Channels setting.
Perm/ Switched (3)	Permanent switched connection (an outbound call that the MAX TNT attempts to keep up at all times). If the unit or central switch resets, or if one end terminates the link, 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, Ascend recommends that you configure the Connection profile to answer calls but not originate them. If the remote device initiates a call, the MAX TNT 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 Answer-Originate=Ans-Only for that device.

Dependencies: The MAX TNT 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 on the basis of 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.

Ascend-Client-Assign-DNS (137)

Description: Specifies whether or not the MAX TNT sends the Ascend-Client-Primary-DNS and Ascend-Client-Secondary-DNS values during connection negotiation.

Usage: Specify one of the following settings:

- DNS-Assign-No (0) disables client DNS server negotiation for the link. DNS-Assign-No is the default.
- DNS-Assign-Yes (1) enables client DNS server negotiation for the link.

Dependencies: To direct the MAX TNT to send the client DNS server address during connection negotiation, you must include the setting Ascend-Client-Assign-DNS=DNS-Assign-Yes, and specify a valid DNS server by means of the Ascend-Client-Primary-DNS or Ascend-Client-Secondary-DNS attribute.

See Also: "Ascend-Client-Primary-DNS (135)" on page 3-18 and "Ascend-Client-Secondary-DNS (136)" on page 3-18.

Ascend-Client-Gateway (132)

Description: Specifies the default route for IP packets coming from the user on a 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 the default, 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.

Dependencies: The Ascend unit must have a direct route to the address you specify. The direct route can come from 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 that includes a default route, 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 go through the router at 10.0.0.3.

Ascend-Client-Primary-DNS (135)

Description: Specifies a primary DNS server address to send to any client connecting to the MAX TNT.

Usage: Specify the IP address of the primary DNS server. You must specify the address in dotted decimal notation. The default is 0.0.0.0, which specifies that no primary DNS server is available for the connection. If you do not specify Ascend-Client-Primary-DNS or Ascend-Client-Secondary-DNS in any user profile, 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.

Dependencies: You must include the setting Ascend-Client-Assign-DNS=DNS-Assign-Yes to direct the MAX TNT to send the primary DNS server address during connection negotiation.

See Also: "Ascend-Client-Assign-DNS (137)" on page 3-17 and "Ascend-Client-Secondary-DNS (136)" on page 3-18.

Ascend-Client-Secondary-DNS (136)

Description: Specifies a secondary DNS server address to send to any client connecting to the MAX TNT.

Usage: Specify the IP address of the secondary DNS server. You must specify the address in dotted decimal notation. The default is 0.0.0.0, which specifies that no primary DNS server is available for the connection. If you do not specify Ascend-Client-Primary-DNS or Ascend-Client-Secondary-DNS in any user profile, 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.

Dependencies: You must include the setting Ascend-Client-Assign-DNS=DNS-Assign-Yes to direct the MAX TNT to send the secondary DNS server address during connection negotiation.

See Also: "Ascend-Client-Assign-DNS (137)" on page 3-17 and "Ascend-Client-Primary-DNS (135)" on page 3-18.

Ascend-Connect-Progress (196)

Description: Indicates the state of the connection before it disconnects.

Usage: Ascend-Connect-Progress can have any one of values specified in Table 3-5.

Table 3-5. 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.

Table 3-5. Ascend-Connect-Progress codes (continued)

Code	Explanation
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 TNT is establishing the TCP connection.
42	The MAX TNT is establishing the immediate Telnet connection.
43	The MAX TNT has established a raw TCP session with the host. This code does not imply that the user has logged into the host.7
44	The MAX TNT 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 TNT is establishing an Rlogin session.
46	The MAX TNT has established an Rlogin session with the host. This code does not imply that the user has logged into the host.
47	Terminal-server authentication has begun.
50	A modem dial-out session has begun.
60	The LAN session is up.
61	LCP negotiations are allowed.
62	CCP negotiations are allowed.
63	IPNCP 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	BNCP 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.

Table 3-5. Ascend-Connect-Progress codes (continued)

Code	Explanation
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.
81	IPX NCP is in an Open state.
82	BACP is being opened.
83	BACP is in an Open state.
84	CBCP is being opened.
85	CBCP is in an Open state.
90	The Ascend unit has accepted a V.110 call.
91	The V.110 call is in an Open state.
92	The V.110 call is in a carrier state.
93	The V.110 call is in a reset state.
94	The V.110 call is in a closed state.
100	The Ascend unit has determined that the call requires callback.
101	Authentication failed.
102	The remote authentication server timed out.
120	The Frame Relay link is inactive. Negotiations are in progress.
121	The Frame Relay link is active and has end-to-end connectivity.
200	The unit is starting authentication.
201	The unit is opening authentication.
202	The unit is skipping authentication.
203	Authentication is open.

Dependencies: The MAX TNT includes Ascend-Connect-Progress in an Accounting-Request packet when the session has ended or has failed authentication (Acct-Status-Type=Stop).

Ascend-Data-Filter (242)

Description: Specifies the characteristics of a data filter in a RADIUS user profile. The MAX TNT uses the filter only when it places or receives a call associated with the profile that includes the filter definition.

Usage: Filter entries apply on a first-match basis. Therefore, the order in which you enter them 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.

You can specify an IP filter or a generic filter. The following sections describe how to configure each of the filter types.

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 here for printing purposes only.

Table 3-6 describes each element of the syntax. None of the keywords are case sensitive.

Table 3-6. IP data filter syntax elements

Element	Description7
ip	Specifies an IP filter.
dir	Specifies filter direction. You can specify **in** (to filter packets coming into the MAX TNT) or **out** (to filter packets going out of the MAX TNT).
action	Specifies the action the MAX TNT should take with a packet that matches the filter. You can specify either **forward** or **drop**.
dstip *dest_ipaddr \subnet_mask*	The keyword **dstip** enables destination-IP-address filtering. 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 TNT compares only the masked bits. If you set ***dest_ipaddr*** to 0.0.0.0, or if the keyword and its IP address specification are not present, the filter matches all IP packets.

Table 3-6. IP data filter syntax elements (continued)

Element	Description7
srcip ***src_ipaddr \subnet_mask***	The keyword **srcip** enables source-IP-address filtering. 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 TNT compares only the masked bits. If you set ***src_ipaddr*** to 0.0.0.0, or if the keyword and its specification are not present, the filter matches all IP packets.
proto	Specifies a protocol specified 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***	The keyword **dstport** enables destination-port filtering. 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. The ***cmp*** argument defines 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***	The keyword **srcport** enables source-port filtering. 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. The ***cmp*** argument defines 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).

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 here for printing purposes only.

Table 3-7 describes each element of the syntax. None of the keywords are case sensitive.

Table 3-7. Generic data filter syntax elements

Element	Description
generic	Specifies a generic filter.
dir	Defines filter direction. You can specify **in** (to filter packets coming into the MAX TNT) or **out** (to filter packets going out of the MAX TNT).
action	Defines the action the MAX TNT should take with a packet that matches the filter. You can specify either **forward** or **drop**.
offset	Specifies 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 TNT applies the value of the ***mask*** argument. A mask hides the part of a number that appears behind the binary zeroes in the mask. The unit then compares the unmasked portion of the packet with the value specified by the ***value*** argument.
mask	Specifies which bits to compare in a segment of the packet. The mask must not 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	Specifies 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 TNT ignores the filter.
compare	Defines how the MAX TNT compares a packet's contents to the value specified by ***value***. You can specify == (for Equal) or != (for NotEqual). Equal is the default.
more	If present, specifies whether the MAX TNT 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 TNT ignores the **more** flag.

Example: The following 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"
```

The following 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 3-12.

Ascend-Data-Rate (197)

Description: Specifies the rate of data received on the connection in bits per second.

Usage: Ascend-Data-Rate does not appear in a user profile. Its default value is 0 (zero).

Dependencies: The MAX TNT includes Ascend-Data-Rate in an Accounting-Request packet when the session has ended or has failed authentication (Acct-Status-Type=Stop).

Ascend-Data-Svc (247)

Description: Specifies the type of data service the link uses for outgoing calls.

Usage: Set the Ascend-Data-Svc attribute to one of the values listed in Table 3-8. The data service you specify must be available end-to-end.

Table 3-8. Ascend-Data-Svc settings

Setting	Description
Switched-Voice-Bearer (0)	Applies only to calls made over a T1 PRI line. The MAX TNT 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)	Contains restricted data, guaranteeing that the data the MAX TNT 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 that use inband signaling (T1 access lines containing one or more switched channels, and Switched-56 lines) are Switched-56K and Switched-56KR.
Switched-64K (2)	Contains any type of data and connects to the Switched-64 data service.

Table 3-8. Ascend-Data-Svc settings (continued)

Setting	Description
Switched-64KR (3)	Contains restricted data and connects to the Switched-64 data service.
Switched-56K (4)	Contains any type of data and connects to the Switched-56 data service. The only services available to lines that use 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)	Contains restricted data and connects to the Nailed-56 data service.
Nailed-64K (2)	Contains any type of data and connects to the Nailed-64 data service.
Switched-384KR (5)	Contains restricted data, and connects to MultiRate or GloBanD data services at 384 Kbps.
Switched-384K (6)	Contains any type of data and connects to the Switched-384 data service. This AT&T data service does not require MultiRate or GloBanD.
Switched-1536K (7)	Contains any type of data and connects to the Switched-1536 data service at 1536 Kbps. This setting is valid only for a MAX TNT that supports ISDN D-channel signaling, and connects to two or more T1 PRI lines that use Non-Facility Associated Signaling (NFAS).
Switched-1536KR (8)	Contains restricted data, and connects to the Switched-1536 data service at 1536 Kbps. This setting is valid only for a MAX TNT that supports ISDN D-channel signaling, and is connected to two or more T1 PRI lines that use Non-Facility Associated Signaling (NFAS).
Switched-128K (9)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-192K (10)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-256K (11)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-320K (12)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-384K-MR (13)	Available on a T1 PRI line with the MultiRate data service.
Switched-448K (14)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-512K (15)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-576K (16)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-640K (17)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-704K (18)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-768K (19)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-832K (20)	Available on a T1 PRI line with MultiRate or GloBanD data services.

Table 3-8. Ascend-Data-Svc settings (continued)

Setting	Description
Switched-896K (21)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-960K (22)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1024K (23)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1088K (24)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1152K (25)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1216K (26)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1280K (27)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1344K (28)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1408K (29)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1472K (30)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1600K (31)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1664K (32)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1728K (33)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1792K (34)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1856K (35)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-1920K (36)	Available on a T1 PRI line with MultiRate or GloBanD data services.
Switched-restricted-bearer-x30 (38)	Specifies 56-Kbps X.30 switched service from DPNSS and DASS 2 switches.
Switched-restricted-64-x30 (40)	Specifies 64-Kbps X.30 switched service from DPNSS and DASS 2 switches. For most DASS 2 and DPNSS installations, select Switched-restricted-64-x30.
Switched-modem (42)	Places an outgoing call on any available digital modem. If no digital modems are available, the MAX TNT does not place the call. The data rate depends on the quality of the connections between modems and the types of modems used. The Switched-modem setting requires that your MAX TNT have digital modems installed. The setting applies only for PPP and MP+ calls. Currently, the MAX TNT does not support multichannel modem calls.

Dependencies: Consider the following:

- 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 such a case, the MAX TNT cannot connect the call.

Ascend-DBA-Monitor (171)

Description: Specifies how the Ascend calling unit monitors the traffic on an MP+ call. The Ascend unit can use the information to add or subtract bandwidth as necessary.

Usage: Specify one of the following values:

- DBA-Transmit (0) specifies that the MAX TNT adds or subtracts bandwidth on the basis of the amount of data it transmits. DBA-Transmit is the default.
- DBA-Transmit-Recv (1) specifies that the MAX TNT adds or subtracts bandwidth on the basis of the amount of data it transmits *and* receives.
- DBA-None (2) specifies that the MAX TNT does not monitor traffic over the link.

Dependencies: Consider the following:

- The MAX TNT supports Ascend-DBA-Monitor only for 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 3-4,
"Ascend-Base-Channel-Count (172)" on page 3-9,
"Ascend-Dec-Channel-Count (237)" on page 3-27,
"Ascend-History-Weigh-Type (239)" on page 3-44,
"Ascend-Inc-Channel-Count (236)" on page 3-47,
"Ascend-Maximum-Channels (235)" on page 3-53,
"Ascend-Minimum-Channels (173)" on page 3-57,
"Ascend-Remove-Seconds (241)" on page 3-68,
"Ascend-Seconds-Of-History (238)" on page 3-72, and
"Ascend-Target-Util (234)" on page 3-75.

Ascend-Dec-Channel-Count (237)

Description: Specifies the number of channels the MAX TNT removes when bandwidth changes during a call.

Usage: Specify a number from 1 to 32. The default value is 1.

Dependencies: Consider the following:

- 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.
- You cannot clear a call by decrementing channels.

See Also: "Ascend-Add-Seconds (240)" on page 3-4,
"Ascend-Base-Channel-Count (172)" on page 3-9,
"Ascend-DBA-Monitor (171)" on page 3-27,
"Ascend-History-Weigh-Type (239)" on page 3-44,
"Ascend-Inc-Channel-Count (236)" on page 3-47,
"Ascend-Maximum-Channels (235)" on page 3-53,
"Ascend-Minimum-Channels (173)" on page 3-57,
"Ascend-Remove-Seconds (241)" on page 3-68,
"Ascend-Seconds-Of-History (238)" on page 3-72, and
"Ascend-Target-Util (234)" on page 3-75.

Ascend-Dialout-Allowed (131)

Description: Specifies whether the user associated with an outgoing RADIUS user profile can use one of the MAX TNT unit's digital modems to dial out.

Usage: Specify one of the following settings:

- Dialout-Not-Allowed (0) specifies that the RADIUS user profile does not allow modem dialout. Dialout-Not Allowed is the default.
- Dialout-Allowed (1) specifies that the RADIUS user profile allows modem dialout.

Ascend-Dial-Number (227)

Description: Specifies the phone number the MAX TNT dials to reach the router or node at the remote end of the link.

Usage: Specify a telephone number of up to 21 characters, limited to the following:

```
1234567890()[]!z-*#|
```

The MAX TNT sends only the numeric characters to place a call. The default value is null.

Dependencies: If Use-Trunk-Groups=Yes in the System profile, the first digits in the Ascend-Dial-Number attribute have the meanings listed in Table 3-9.

Table 3-9. Ascend-Dial-Number digits

First digit	Significance
4 through 9	The MAX TNT places the call over the corresponding trunk group listed in the Trunk-Group parameter.
3	The MAX TNT places the call to a destination listed in a Call-Route profile. The second and third digits specify the number of the Call-Route profile.
2	The MAX TNT places the call between host ports on the same MAX TNT. If you enter 0 (zero) for the second digit, the call connects to any available serial port and ignores the third digit. If you enter a nonzero value for the second digit, the third digit selects the serial port. If you enter 0 (zero) for the third digit, the call connects to any available serial port in the module selected by the second digit.

Ascend-Disconnect-Cause (195)

Description: Indicates the reason a connection went offline.

Usage: Ascend-Disconnect-Cause can return any of the values listed in Table 3-10..

Table 3-10. Ascend-Disconnect-Cause codes

Code	Description
1	This value is not applied to any call.
2	The disconnect occurred for an unknown reason.
3	The call was disconnected.
4	CLID authentication failed.
5	A RADIUS timeout occurred during authentication.
6	Authentication was successful. The Ascend unit is configured to call back the user.
7	The Pre-T310 Send Disc timer was triggered.
9	No modem is available to accept the call.
10	The modem never detected Data Carrier Detect (DCD).
11	The modem detected DCD, but the modem carrier was lost.
12	The Ascend unit failed to successfully detect modem result codes.
13	The Ascend unit failed to open a modem for an outgoing call.
14	The Ascend unit failed to open a modem for outgoing call while the ModemDiag diagnostic command was enabled.
20	The user exited normally from the terminal server.
21	The terminal server timed out waiting for user input.
22	A forced disconnect occurred when the user exited a Telnet session.
23	No IP address was available when the user entered the PPP or SLIP command.
24	A forced disconnect occurred when the user exited a raw TCP session.
25	The user exceeded the limit for login attempts.
26	The Ascend unit attempted to start a raw TCP session, but raw TCP is disabled.
27	Control-C characters were received during the login.

Table 3-10. Ascend-Disconnect-Cause codes (continued)

Code	Description
28	The terminal-server session cleared ungracefully.
29	The user closed a terminal-server virtual connection normally.
30	The terminal-server virtual connection cleared ungracefully.
31	The user exited from an Rlogin session.
32	The establishment of the Rlogin session failed because of bad options.
33	The Ascend unit lacks the resources to process a terminal-server request.
35	The MP+ session cleared because no null MP packets were received. An Ascend unit sends (and should receive) null MP packets throughout an MP+ session.
40	LCP timed out waiting for a response.
41	LCP negotiations failed, probably because the user is configured to send passwords by means of PAP, and the Ascend unit is configured to accept passwords by means of CHAP (or vice versa).
42	PAP authentication failed.
43	CHAP authentication failed.
44	Authentication failed from a remote server.
45	The Ascend unit received a Terminate Request packet while LCP was in an open state.
46	The Ascend unit received a Close Request from an upper layer, indicating graceful LCP closure.
47	The Ascend unit cleared the call because no PPP Network Core Protocols (NCPs) were successfully negotiated. Typically, there is no agreement on the type of routing or bridging that is supported for the session.
48	An MP session was disconnected. The Ascend unit accepted an added channel, but cannot determine to which call to add the new channel.
49	The Ascend unit disconnected an MP call because no more channels could be added.
50	Telnet or raw TCP session tables are full.
51	The Ascend unit has exhausted Telnet or raw TCP resources.
52	For a Telnet or raw TCP session, the IP address is invalid.

Table 3-10. Ascend-Disconnect-Cause codes (continued)

Code	Description
53	The Ascend unit cannot resolve the host name for a Telnet or raw TCP session.
54	For a Telnet or raw TCP session, the Ascend unit received a bad or missing port number.
60	For a Telnet or raw TCP session, the host was reset.
61	For a Telnet or raw TCP session, the connection was refused.
62	For a Telnet or raw TCP session, the connection timed out.
63	For a Telnet or raw TCP session, the connection was closed by a foreign host.
64	For a Telnet or raw TCP session, the network was unreachable.
65	For a Telnet or raw TCP session, the host was unreachable.
66	For a Telnet or raw TCP session, the network admin was unreachable.
67	For a Telnet or raw TCP session, the host admin was unreachable.
68	For a Telnet or raw TCP session, the port was unreachable.
100	The session timed out.
101	The user name was invalid.
102	Callback is enabled.
105	The safety timer expired before the encaps layer was up.
106	The safety timer expired on a different channel of the multichannel call.
115	The dial-in user is no longer active.
120	A requested protocol is disabled or unsupported.
150	A disconnect was requested by the RADIUS server.
151	The call was disconnected by the local administrator.
152	The call was disconnected by means of SNMP.
160	The unit exceeded the maximum number of V.110 retries.
170	A timeout occurred while the Ascend unit waited for the remote device to be authenticated.
171	The interface was unexpectedly released.
180	The user disconnected the call.

Table 3-10. Ascend-Disconnect-Cause codes (continued)

Code	Description
181	The call was cleared by the system.
185	The signal was lost from remote end, probably because the remote end's modem was turned off.
190	The resource has been quiesced.
195	The maximum duration for the call has been reached.
201	The Ascend unit has low memory.
210	The modem card stopped working because it had calls outstanding.
220	The Ascend unit requires CBCP, but client does not support it.
230	The Ascend unit deleted the Virtual Router (VRouter).
240	The Ascend unit disconnected the call on the basis of LQM measurements.
241	The Ascend unit cleared a backup call.
300	An X.25 terminal error occurred.
350	The master channel host card is down.

Dependencies: The MAX TNT includes Ascend-Disconnect-Cause in an Accounting-Request packet when the session has ended or has failed authentication (Acct-Status-Type=Stop).

Ascend-Dsl-CIR-Recv-Limit (100)

Description: Specifies the maximum data rate (in k-bits per second) to be received across the connection. You can use this setting to limit bandwidth for a connection according to the rate charged for the account.

Usage: Specify a number from 0 to 64000. The default is 0 (zero), which disables the data-rate limit feature. If the value you specify is larger than the actual bandwidth provided by the line, the connection behaves as though the data rate limit were disabled, except that additional computations are performed unnecessarily.

Dependencies: The system activates configurable receive data-rate limits only for connections that use CAP-RADSL, SDSL, and unchannelized DS3 cards. If you specify a value for a connection that does not use these cards, the system ignores the settings.

See Also: "Ascend-Dsl-CIR-Recv-Limit (100)" on page 3-32.

Ascend-Dsl-CIR-Xmit-Limit (101)

Description: Specifies the maximum data rate (in k-bits per second) to be transmitted across the connection. You can use this setting to limit bandwidth for a connection according to the rate charged for the account.

Usage: Specify a number from 0 to 64000. The default is 0 (zero), which disables the data-rate limit feature. If the value you specify is larger than the actual bandwidth provided by the line, the connection behaves as though the data rate limit were disabled, except that additional computations are performed unnecessarily.

Dependencies: The system activates configurable transmit data-rate limits only for connections that use CAP-RADSL, SDSL, and unchannelized DS3 cards. If you specify a value for a connection that does not use these cards, the system ignores the settings.

See Also: " Ascend-Dsl-CIR-Xmit-Limit (101)" on page 3-33.

Ascend-DSL-Downstream-Limit (99)

Description: Specifies the per-session ADSL-CAP or SDSL downstream data rate.

Usage: Specify one of the following rates (in bps):

adslcap-dn-7168000 (0)
adslcap-dn-6272000 (1)
adslcap-dn-5120000 (2)
adslcap-dn-4480000 (3)
adslcap-dn-3200000 (4)
adslcap-dn-2688000 (5)
adslcap-dn-2560000 (6)
adslcap-dn-2240000 (7)
adslcap-dn-1920000 (8)
adslcap-dn-1600000 (9)
adslcap-dn-1280000 (10)
adslcap-dn-960000 (11)
adslcap-dn-640000 (12)

The default is adslcap-dn-2560000 (6).

Dependencies: For SDSL connections, the value of Ascend-DSL-Downstream-Limit must match the value of Ascend-DSL-Upstream-Limit.

See Also: "Ascend-Dsl-Rate-Mode (97)" on page 3-34 and "Ascend-Dsl-Rate-Type (92)" on page 3-34.

Ascend-Dsl-Rate-Mode (97)

Description: Specifies the per-session DSL data-rate mode.

Usage: Specify one of the following settings:

- Rate-Mode-AutoBaud (the default) specifies that a DSL modem should train up to a set data rate. If a DSL modem cannot train to this data rate, it connects to the closest rate to which it can train (the modem's ceiling rate).
- Rate-Mode-Single specifies that a DSL modem should train to a single data rate, even if the DSL modem can possibly train at a higher or lower data rate. If the DSL modem cannot train to the specified single rate, the connection fails. Specify Rate-Mode-Single for an SDSL connection.

See Also: "Ascend-DSL-Downstream-Limit (99)" on page 3-33 and "Ascend-Dsl-Rate-Type (92)" on page 3-34.

Ascend-Dsl-Rate-Type (92)

Description: Specifies the per-session modem type for rate control.

Usage: Specify one of the following settings:

- Rate-Type-Disabled (the default) specifies that modem rate control is not active for this connection. I
- Rate-Type-AdslCap specifies that the per-session modem type is ADSL-CAP.
- Rate-Type-Sdsl specifies that the per-session modem type is SDSL.
- Rate-Type-AdslDmt specifies that the per-session modem type is ADSL-DMT.

See Also: "Ascend-DSL-Downstream-Limit (99)" on page 3-33 and "Ascend-Dsl-Rate-Mode (97)" on page 3-34.

Ascend-DSL-Upstream-Limit (98)

Description: Specifies the symmetrical data rate. This setting applies to connections on the 24-port SDSL data or voice card.

Usage: Specify one of the following settings:

sdsl-144000 (0)
sdsl-272000 (1)
sdsl-400000 (2)
sdsl-528000 (3)
sdsl-784000 (4)
sdsl-1168000 (5)
sdsl-1552000 (6)
sdsl-2320000 (7)

See Also: "Ascend-DSL-Downstream-Limit (99)" on page 3-33.

Ascend-Event-Type (150)

Description: Indicates one of the following:

- A cold-start notification, informing the accounting server that the MAX TNT has started up
- A session event, informing the authentication server that a session has begun

Usage: For a cold-start notification, Ascend-Event-Type=Ascend-Coldstart (1). For a session event, Ascend-Event-Type=Ascend-Session-Event (2).

Dependencies: In a cold-start notification, the MAX TNT sends values for NAS-Identifier, Ascend-Event-Type, and Ascend-Number-Sessions in an Ascend-Access-Event-Request packet (code 33). The RADIUS accounting server must send back an Ascend-Access-Event-Response packet (code 34) with the correct identifier to the MAX TNT.

In a session event, the MAX TNT sends values for Password, NAS-Identifier, Ascend-Access-Event-Type, and Ascend-Number-Sessions in an Ascend-Access-Event-Request packet (code 33). The authentication server must send back an Ascend-Access-Event-Response packet (code 34) with the correct identifier to the MAX TNT.

See Also: "Ascend-Number-Sessions (202)" on page 3-60 and "NAS-Identifier (4)" on page 3-90.

Ascend-Expect-Callback (149)

Description: Specifies whether a user dialing out should expect the remote end to call back.

Usage: Specify one of the following values:

- Expect-Callback-No (0) specifies that the caller does not wait for a callback after placing a call that does not connect. Expect-Callback-No is the default.
- Expect-Callback-Yes (1) specifies 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 3-11.

Ascend-Filter (91)

Description: Specifies a string-format filter, which can include an IP TOS filter specification.

Usage: Filter entries apply on a first-match basis. Therefore, the order in which you enter them 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.

A TOS filter value is specified in the following format:

iptos ***dir*** [**dstip** ***dest_ipaddr\subnet_mask***]
[**srcip** ***src_ipaddr\subnet_mask***][***proto***][**destport** ***cmp value***]
[**srcport** ***cmp value***][**precedence** ***value***][**type-of-service** ***value***]

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

Keyword or argument	Description
iptos	Specifies an IP filter.
dir	Specifies filter direction. You can specify **in** (to filter packets coming into the MAX TNT) or **out** (to filter packets going out of the MAX TNT).
dstip ***dest_ipaddr\subnet_mask***	If the **dstip** keyword is followed by a valid IP address, the TOS filter will set bytes only in packets with that destination address. If a subnet mask portion of the address is present, the MAX TNT compares only the masked bits. If the **dstip** keyword is followed by the zero address (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\subnet_mask***	If the **srcip** keyword is followed by a valid IP address, the TOS filter will set bytes only in packets with that source address. If a subnet mask portion of the address is present, the MAX TNT compares only the masked bits. If the **srcip** keyword is followed by the zero address (0.0.0.0), or if this keyword and its IP address specification are not present, the filter matches all IP packets.
proto	A protocol number. A value of zero matches all protocols. If you specify a non-zero number, the MAX TNT compares it to the Protocol field in packets. For list of protocol numbers, see RFC 1700.
dstport ***cmp value***	If the **dstport** keyword is followed by a comparison symbol and a port, the port is compared to the destination port of a packet. The comparison symbol can be < (less-than), = (equal), > (greater-than), or != (not-equal). The port value can be one of the following names or numbers: `ftp-data` (20), `ftp` (21), `telnet` (23), `smtp` (25), `nameserver` (42), `domain` (53), `tftp` (69), `gopher` (70), `finger` (79), `www` (80), `kerberos` (88), `hostname` (101), `nntp` (119), `ntp` (123), `exec` (512), `login` (513), `cmd` (514), `talk` (517).
srcport ***cmp value***	If the **srcport** keyword is followed by a comparison symbol and a port, the port is compared to the source port of a packet. The comparison symbol can be < (less-than), = (equal), > (greater-than), or != (not-equal). The port value can be one of the following names or numbers: `ftp-data` (20), `ftp` (21), `telnet` (23), `smtp` (25), `nameserver` (42), `domain` (53), `tftp` (69), `gopher` (70), `finger` (79), `www` (80), `kerberos` (88), `hostname` (101), `nntp` (119), `ntp` (123), `exec` (512), `login` (513), `cmd` (514), `talk` (517).

Keyword or argument	Description
precedence *value*	Specifies the priority level of the data stream. The three most significant bits of the TOS byte are priority bits used to set precedence for priority queuing. If a packet matches the filter, those bits are set to the specified value (most significant bit first): 000—Normal priority. 001—Priority level 1. 010—Priority level 2. 011—Priority level 3. 100—Priority level 4. 101—Priority level 5. 110—Priority level 6. 111—Priority level 7 (the highest priority).
type-of-service *value*	Type of Service of the data stream. If a packet matches the filter, the system sets the four bits following the three most significant bits of the TOS byte to the specified value. Those four bits are used to choose a link based on the type of service. Specify one of the following values: Normal (0)—Normal service. Disabled (1)—Disables TOS. Cost (2)—Minimize monetary cost. Reliability (4)—Maximize reliability. Throughput (8)—Maximize throughput. Latency (16)—Minimize delay.

Example: The following RADIUS user profile defines a TOS filter for TCP packets (protocol 6) that are destined for a single host at 10.168.6.24. The packets must be sent on TCP port 23. For incoming packets that match this filter, the priority is set at level 2. This is a relatively low priority, which means that an upstream router that implements priority queuing may drop these packets when it becomes loaded. The commands also set TOS to prefer a low latency connection. This means that the upstream router will choose a a fast connection is one is available, even if it is higher cost, lower bandwidth, or less reliable than another available link.

```
John Password="jlhkjtn", User-Service=Framed-User
    Framed-Protocol=PPP,
    Framed-IP-Address=10.168.6.120
    Framed-IP-Netmask=255.255.255.0
    Ascend-Filter="iptos in dstip 10.168.6.24/32
    dstport=23 precedence 010 type-of-service latency"
```

See Also: “Ascend-IP-TOS (88)” on page 3-49,
“Ascend-IP-TOS-Apply-To (90)” on page 3-50, and
“Ascend-IP-TOS-Precedence (89)” on page 3-50.

Ascend-First-Dest (189)

Description: Records the destination IP address of the first packet the MAX TNT receives on a link after RADIUS authenticates the connection.

Usage: Ascend-First-Dest does not appear in a user profile and has no default value.

Dependencies: Ascend-First-Dest applies only if the session routes IP. The MAX TNT includes Ascend-First-Dest in an Accounting-Request packet when both of the following conditions are true:

- The session has been authenticated.
- The session has ended (Acct-Status-Type=Stop).

Ascend-Force-56 (248)

Description: Specifies whether the MAX TNT uses only the 56-Kbps portion of a channel, even when all 64 Kbps appear to be available:

Usage: Specify one of the following values:

- Force-56-No (0) specifies that the MAX TNT should use the entire 64 Kbps (when available). Force-56-No is the default.
- Force-56-Yes (1) specifies that the MAX TNT should use only the 56-Kbps portion of a channel.

Dependencies: 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.

Ascend-FR-Circuit-Name (156)

Description: Specifies the Permanent Virtual Connection (PVC) for which the user profile is an endpoint.

Usage: Specify a text string of up to 15 characters. The default value is null.

Dependencies: Consider the following:

- You can specify Ascend-FR-Circuit-Name only when Framed-Protocol=FR-CIR.
- The MAX TNT 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 Frame Relay network switches matching pairs of Ascend-FR-Circuit-Name attributes to each other, so make sure that you specify the exact same name for Ascend-FR-Circuit-Name in each profile.

Ascend-FR-DCE-N392 (162)

Description: Specifies the number of errors, during Ascend-FR-DCE-N393-monitored events, that causes the network side to declare the user side's procedures inactive.

Usage: Specify an integer from 1 to 10. The default value is 3.

Dependencies: Consider the following:

- You should 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 3-39 and "Ascend-FR-Type (159)" on page 3-43.

Ascend-FR-DCE-N393 (164)

Description: Specifies the DCE-monitored event count. The MAX TNT considers a link active if the event count does not reach the value of Ascend-FR-DCE-N393.

Usage: Specify a number from 1 to 10. The default value is 4.

Dependencies: The Ascend-FR-DCE-N393 attribute does not apply if Ascend-FR-Type=Ascend-FR-DTE.

See Also: "Ascend-FR-Type (159)" on page 3-43.

Ascend-FR-Direct (219)

Description: Specifies whether the MAX TNT uses a Frame Relay Direct configuration for Frame Relay packets.

Usage: Specify one of the following values:

- FR-Direct-No (0) specifies that the MAX TNT does not use a Frame Relay Direct configuration. FR-Direct-No is the default.
- FR-Direct-Yes (1) specifies that the MAX TNT uses a Frame Relay Direct configuration.

See Also: "Ascend-FR-Direct-DLCI (221)" on page 3-39 and "Ascend-FR-DLCI (179)" on page 3-40.

Ascend-FR-Direct-DLCI (221)

Description: Specifies the Data Link Connection Indicator (DLCI) for the user profile in a Frame Relay Direct configuration.

Usage: Specify an integer from 16 to 991. The default value is 16.

Dependencies: Ascend-FR-Direct-DLCI applies only if Ascend-FR-Direct=FR-Direct-Yes.

See Also: "Ascend-FR-Direct (219)" on page 3-39 and "Ascend-FR-Direct-Profile (220)" on page 3-40.

Ascend-FR-Direct-Profile (220)

Description: Specifies the name of the Frame Relay profile for a Frame Relay Direct configuration.

Usage: Specify the name of a Frame Relay profile. This profile 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 lowercase, alphanumeric characters. The default value is null.

Dependencies: Ascend-FR-Direct-Profile applies only if Ascend-FR-Direct=FR-Direct-Yes.

See Also: "Ascend-FR-Direct (219)" on page 3-39 and "Ascend-FR-Direct-DLCI (221)" on page 3-39.

Ascend-FR-DLCI (179)

Description: Specifies a Data Link Connection Indicator (DLCI) number for a Frame Relay gateway or switch. A DLCI is not an address, but a local label that identifies a logical link between a device and the Frame Relay switch. The switch uses the DLCI to route frames through the network, and the DLCI can change as frames are passed through multiple switches.

Usage: Specify an integer from 16 to 991. The default value is 16.

Dependencies: Ascend-FR-DLCI applies only if Ascend-FR-Direct=FR-Direct-No.

See Also: "Ascend-FR-Direct (219)" on page 3-39 and "Ascend-FR-Profile-Name (180)" on page 3-42.

Ascend-FR-DTE-N392 (163)

Description: Specifies the number of errors, during Ascend-FR-DTE-N393-monitored events, that causes the user side to declare the network side's procedures inactive.

Usage: Specify an integer from 1 to 10. The default value is 3.

Dependencies: Consider the following:

- You should 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 3-40 and "Ascend-FR-Type (159)" on page 3-43.

Ascend-FR-DTE-N393 (165)

Description: Specifies the DTE-monitored event count. The MAX TNT considers a link active if the event count does not reach the value of Ascend-FR-DTE-N393.

Usage: Specify a number from 1 to 10. The default value is 4.

Dependencies: The Ascend-FR-DTE-N393 attribute does not apply if Ascend-FR-Type=Ascend-FR-DCE.

See Also: "Ascend-FR-Type (159)" on page 3-43.

Ascend-FR-Link-Mgt (160)

Description: Specifies the link management protocol the MAX TNT uses to communicate with the Frame Relay switch.

Usage: Specify one of the following values:

- Ascend-FR-No-Link-Mgt (0) specifies no link management, and is the default. The MAX TNT always considers a link active if no link management functions take place.
- Ascend-FR-T1-617D (1) specifies T1.617 Annex D link management.
- Ascend-FR-Q-933A (2) specifies Q.933 Annex A link management.

Ascend-FR-Link-Status-DLCI (106)

Description: Specifies the DLCI to use for link management on the Frame Relay datalink.

Usage: Accept the default of 0 (zero) or specify DLCI 1023.

See Also: "Ascend-FR-Link-Mgt (160)" on page 3-41.

Ascend-FR-N391 (161)

Description: Specifies the number of T391 polling cycles between full Status Enquiry messages.

Usage: Specify an integer from 1 to 255. The default value is 6, which indicates that after six status requests spaced Ascend-FR-T391 seconds apart, the UNI-DTE device requests a full status report.

Dependencies: The Ascend-FR-N391 attribute does not apply if Ascend-FR-Type=Ascend-FR-DCE.

See Also: "Ascend-FR-T391 (166)" on page 3-42 and "Ascend-FR-Type (159)" on page 3-43.

Ascend-FR-Nailed-Grp (158)

Description: Associates a group of nailed-up channels with the Frame Relay profile.

Usage: Specify a number from 1 to 1024. 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: Specifies the name of the Frame Relay profile to use when the MAX TNT is configured as a Frame Relay gateway or Frame Relay switch.

Usage: Specify the name of a Frame Relay profile. This profile connects to the Frame Relay switch handling the Data Link Connection Indicator (DLCI) specified by Ascend-FR-DLCI. You can specify up to 15 lowercase, alphanumeric characters. The default value is null.

Dependencies: Ascend-FR-Profile-Name applies only if Ascend-FR-Direct=FR-Direct-No.

See Also: "Ascend-FR-Direct (219)" on page 3-39 and "Ascend-FR-DLCI (179)" on page 3-40.

Ascend-FR-T391 (166)

Description: Specifies the Link Integrity Verification polling timer.

Usage: Specify a number of seconds from 5 to 30. The value should be less than that of Ascend-FR-T392. The default value is 10, which indicates that after Ascend-FR-N391 status requests spaced ten seconds apart, the UNI-DTE device requests a full status report.

Dependencies: The Ascend-FR-T391 attribute does not apply if Ascend-FR-Type=Ascend-FR-DCE.

See Also: "Ascend-FR-N391 (161)" on page 3-41,
"Ascend-FR-T392 (167)" on page 3-42, and
"Ascend-FR-Type (159)" on page 3-43.

Ascend-FR-T392 (167)

Description: Specifies the interval (in seconds) in which Status Enquiry messages should be received. The network records an error if it does not receive a Status Enquiry within the number of seconds you specify.

Usage: Specify a number of seconds from 5 to 30. The default value is 10.

Dependencies: The Ascend-FR-T392 attribute does not apply if Ascend-FR-Type=Ascend-FR-DTE.

See Also: "Ascend-FR-Type (159)" on page 3-43.

Ascend-FR-Type (159)

Description: Specifies the kind of logical interface between the MAX TNT and the Frame Relay network on the datalink:

- The UNI (User to Network Interface) is the interface between an end-user and a network endpoint (a router or a switch) on the Frame Relay network.
- A DCE (Data Circuit-Terminating Equipment) is a device that connects the DTE (Data Terminal Equipment) to a communications channel, such as a telephone line.
- A DTE refers to a device that an operator uses, such as a computer or a terminal.
- NNI (Network-to-Network Interface) operation allows the MAX TNT to act as a Frame Relay switch communicating with another Frame Relay switch.

Usage: Specify one of the following values:

- Ascend-FR-DTE (0) specifies a UNI-DTE connection (the default). The MAX TNT operates as the user side, communicating with the network-side DCE switch.
- Ascend-FR-DCE (1) specifies a UNI-DCE connection. The MAX TNT operates as the network side, communicating with the user side (UNI-DTE) of a Frame Relay terminating unit.
- Ascend-FR-NNI (2) specifies an NNI connection. The MAX TNT performs both DTE and DCE link management.

See Also: "Ascend-FR-Link-Mgt (160)" on page 3-41.

Ascend-FT1-Caller (175)

Description: Specifies whether the MAX TNT initiates an FT1-B&O call, or waits for the remote end to initiate these types of calls.

Usage: Specify one of the following values:

- FT1-No (0) specifies that the MAX TNT waits for the remote end to initiate the call. FT1-No is the default.
- FT1-Yes (1) specifies that the MAX TNT initiates the call. If you choose this setting, the MAX TNT dials to bring online any switched circuits that are part of the call.

Dependencies: 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 TNT. But if the remote end has FT1-Caller=Yes or Ascend-FT1-Caller=FT1-Yes, set Ascend-FT1-Caller=FT1-No in the user profile for the local MAX TNT.

Ascend-Group (178)

Description: Points to the nailed-up channels used by the profile's WAN 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 from 1 to 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 from 1 to 60, separated by commas, with no spaces. The default value is 1.

Dependencies: Consider the following:

- Ascend-Group does not apply if the link consists entirely of switched channels.
- If you add channels for the Ascend-Group attribute, the MAX TNT adds the channels to any online connection that uses the group.
- Do not duplicate group numbers in active profiles.
- Although you can assign multiple groups to a user profile, do not mix the Serial WAN circuit with nailed-up T1/E1 channels.

Example: If you set the Ascend-Group attribute to `"1,3,5,7"` and Ascend-Call-Type=Nailed/Mpp, the MAX TNT assigns four nailed-up groups to the profile.

Ascend-History-Weigh-Type (239)

Description: Specifies which Dynamic Bandwidth Allocation (DBA) algorithm to use for calculating average line utilization (ALU) of transmitted data.

Usage: Specify one of the following settings:

- History-Constant (0) gives equal weight to all samples taken during the historical time period specified by the Ascend-Seconds-Of History attribute. When you select this option, older historical samples have as much impact on the decision to change bandwidth allocation as more recent samples.
- History-Linear (1) gives more weight to recent samples of bandwidth usage than to older samples taken during the historical period specified by Ascend-Seconds-Of-History. The weighting grows at a linear rate.
- History-Quadratic (2) gives more weight to recent samples of bandwidth usage than to older samples taken during the historical period specified by the Ascend-Seconds-Of-History attribute. The weighting grows at a quadratic rate. History-Quadratic is the default.

See Also: "Ascend-Add-Seconds (240)" on page 3-4,
"Ascend-Base-Channel-Count (172)" on page 3-9,
"Ascend-DBA-Monitor (171)" on page 3-27,
"Ascend-Dec-Channel-Count (237)" on page 3-27,
"Ascend-Inc-Channel-Count (236)" on page 3-47,
"Ascend-Maximum-Channels (235)" on page 3-53,
"Ascend-Minimum-Channels (173)" on page 3-57,
"Ascend-Remove-Seconds (241)" on page 3-68,
"Ascend-Seconds-Of-History (238)" on page 3-72, and
"Ascend-Target-Util (234)" on page 3-75.

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

Description: Indicates the IP address of the Home Agent used for the Mobile Client.

Usage: The Ascend-Home-Agent-IP-Addr attribute appears in an accounting Stop record under the following conditions:

- The session has ended.
- The Accounting-Request packet includes Acct-Status-Type=Stop.
- The session was authenticated and encapsulated by means of Ascend Tunnel Management Protocol (ATMP).

See Also: "Understanding accounting records" on page 4-13.

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

Description: Specifies the UDP port number to which the Foreign Agent directs Ascend Tunnel Management Protocol (ATMP) messages.

Usage: Specify a UDP port number from 0 to 65535. The default value is 5150.

Dependencies: If you specify a value for the *udp_port* argument of Ascend-Server-Endpoint 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-Secondary-Home-Agent (130)" on page 3-70 and "Tunnel-Server-Endpoint (67)" on page 3-96.

Ascend-Home-Network-Name (185)

Description: Specifies the name of the Connection profile that defines the link on which the Home Agent sends all packets it receives from the Mobile Client during Ascend Tunnel Management Protocol (ATMP) operation.

Usage: Specify the name of the Home Agent's Connection profile. The default value is null.

Dependencies: You must specify a value for the Ascend-Home-Network-Name attribute only if the Home Agent is a gateway.

Note: The standard attribute Tunnel-Private-Group-ID (81) is equivalent to Ascend-Home-Network Name.

Ascend-Host-Info (252)

Description: 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 the following format:

Ascend-Host-Info="*IP_address text*"

where ***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 each entry 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 specify the following settings in the Menu-Mode-Options subprofile of the Terminal-Server profile:

- Start-With-Menus=Yes or Toggle-Screen=Yes
- Remote-Configuration=Yes

Example: To set up a host list for a MAX TNT named Cal, you would configure a pseudo-user profile as follows:

```
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. ",
     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 3-93.

Ascend-Idle-Limit (244)

Description: Specifies the number of seconds the MAX TNT waits before clearing a call when a session is inactive.

Usage: Specify a number from 0 to 65535. If you specify 0 (zero), the MAX TNT always clears a call when a session is inactive. The default value is 120 seconds. If you accept the default, and the Answer-Defaults profile specifies a value for the analogous Idle-Timer parameter, the MAX TNT ignores the Idle-Timer value and uses the Ascend-Idle-Limit default.

Dependencies: Ascend-Idle-Limit will be deprecated in favor of the RFC-defined attribute Idle-Timeout (28) over time. Currently, if a user profile specifies both an RFC-defined attribute and an Ascend vendor attribute that performs a similar function, the last one sent by the server is used. However, using both attributes is not reliable and is not recommended.

See Also: "Ascend-MPP-Idle-Percent (254)" on page 3-58
"Ascend-Preempt-Limit (245)" on page 3-62, and
"Idle-Timeout (28)" on page 3-88.

Ascend-IF-Netmask (153)

Description: Specifies the subnet mask in use for the local numbered interface.

Usage: Specify a subnet mask consisting of four numbers from 0 to 255, separated by periods. The default value is 0.0.0.0.

See Also: "Ascend-PPP-Address (253)" on page 3-60 and "Ascend-Remote-Addr (154)" on page 3-67.

Ascend-Inc-Channel-Count (236)

Description: Specifies the number of channels the MAX TNT adds when bandwidth changes during a call.

Usage: Specify a number from 1 to 32. The default value is 1.

Dependencies: Consider the following:

- 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.
- MP+ calls cannot exceed 32 channels.
- The sum of Ascend-Base-Channel-Count and Ascend-Inc-Channel-Count must not exceed the maximum number of channels available.

See Also: "Ascend-Add-Seconds (240)" on page 3-4,
"Ascend-Base-Channel-Count (172)" on page 3-9,
"Ascend-DBA-Monitor (171)" on page 3-27,
"Ascend-Dec-Channel-Count (237)" on page 3-27,
"Ascend-History-Weigh-Type (239)" on page 3-44,
"Ascend-Maximum-Channels (235)" on page 3-53,
"Ascend-Minimum-Channels (173)" on page 3-57,
"Ascend-Remove-Seconds (241)" on page 3-68,
"Ascend-Seconds-Of-History (238)" on page 3-72, and
"Ascend-Target-Util (234)" on page 3-75.

Ascend-IP-Direct (209)

Description: Specifies the IP address to which the MAX TNT redirects packets from the user. When you include this attribute in a user profile, the MAX TNT bypasses all internal routing tables, and simply sends all packets it receives on the connection's WAN interface to the specified IP address.

Ascend-IP-Direct only affects packets *from* the user. It does not affect packets that go *to* the user. The MAX TNT uses its internal routing scheme to route packets to the user.

Usage: Specify an IP address in dotted decimal notation. The default value is 0.0.0.0. If you accept the default, the MAX TNT does not redirect IP traffic.

Dependencies: Consider the following:

- You can specify the Ascend-IP-Direct attribute only if IP routing is in use and Framed-Protocol is not set to 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 TNT forwards all RIP packets it receives to the IP address you specify. To turn off RIP, set Framed-Routing=None.

Example: To specify that the MAX TNT redirects incoming packets to the host at IP address 10.2.3.11, you could configure a user profile as follows:

```
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-IP-Direct=10.2.3.11,
     Ascend-Metric=2,
     Framed-Routing=None,
     ...
```

See Also: "Framed-Routing (10)" on page 3-87.

Ascend-IP-Pool-Definition (217)

Description: Specifies the first address in an IP address pool, as well as the number of addresses in the pool.

Usage: The Ascend-IP-Pool-Definition attribute has the following format:

Ascend-IP-Pool-Definition="*num first_ipaddr max_entries* [*vrouter_name*]"

Table 3-11 describes each Ascend-IP-Pool-Definition argument.

Table 3-11. Ascend-IP-Pool-Definition arguments

Argument	Specifies
num	Number of the pool. The default value is 1. Specify pool numbers starting with 1, unless you have defined pools with the Pool-Base-Address and Assign-Count parameters in the MAX TNT interface, and do not wish to override those settings. In that case, for the ***num*** argument, start with one plus the highest number you used for an IP address pool on the MAX TNT. For example, if you set up address pools 1 through 5 on the MAX TNT, specify pool numbers starting with 6 in RADIUS.
first_ipaddr	First IP address in the address pool. The address you specify should not accept a subnet mask, because it always becomes a host route. The default value is 0.0.0.0. **Note:** In Windows, the default subnet mask for PPP interfaces is 255.255.255.0. Therefore, if NetBIOS over IP is enabled, connected Windows users will broadcast to .255, causing a performance problem for anyone connected at that address.

Table 3-11. Ascend-IP-Pool-Definition arguments (continued)

Argument	Specifies
max_entries	Maximum number of IP addresses in the pool. The MAX TNT assigns addresses sequentially, from ***first_ipaddr*** on, up to the limit of addresses specified by ***max_entries***. The default value is 0 (zero). You can specify up to 500 addresses.
vrouter_name	Name of the Virtual Router (VRouter) to which the IP address pool belongs.

Example: In the following example, an administrator configures a pseudo-user profile to create two address pools. 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-TNT 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 3-6.

Ascend-IP-TOS (88)

Description: Specifies the Type-of-Service (TOS) of the data stream.

Usage: The value you specify sets the four bits following the three most significant bits of the TOS byte. which are used to choose a link based on the type of service. Specify one of the following values:

- Ascend-IP-TOS IP-TOS-Normal (0) specifies normal service.
- Ascend-IP-TOS IP-TOS-Disabled (1) disables TOS.
- Ascend-IP-TOS IP-TOS-Cost (2) minimizes monetary cost.
- Ascend-IP-TOS IP-TOS-Reliability (4) maximizes reliability.
- Ascend-IP-TOS IP-TOS-Throughput (8) maximizes throughput.
- Ascend-IP-TOS IP-TOS-Latency (16) minimizes delay.

See Also: "Ascend-IP-TOS-Apply-To (90)" on page 3-50 and "Ascend-IP-TOS-Precedence (89)" on page 3-50.

Ascend-IP-TOS-Apply-To (90)

Description: Specifies the direction in which Type-of-Service (TOS) is enabled.

Usage: Specify one of the following values:

- IP-TOS-Apply-To-Incoming (1024) specifies that bits are set in packets received on the interface. This setting is the default.
- IP-TOS-Apply-To-Outgoing (2048) specifies that bits are set in outbound packets only.
- IP-TOS-Apply-To-Both (3072) specifies that both incoming and outgoing packets are tagged.

See Also: "Ascend-IP-TOS (88)" on page 3-49 and "Ascend-IP-TOS-Precedence (89)" on page 3-50.

Ascend-IP-TOS-Precedence (89)

Description: Specifies the priority level of the data stream.

Usage: The three most significant bits of the TOS byte are priority bits used to set precedence for priority queuing. When TOS is enabled, those bits can be set to one of the following values (most significant bit first):

- IP-TOS-Precedence-Pri-Normal (0) specifies normal priority.
- IP-TOS-Precedence-Pri-One (32) specifies priority level 1.
- IP-TOS-Precedence-Pri-Two (64) specifies priority level 2.
- IP-TOS-Precedence-Pri-Three (96) specifies priority level 3.
- IP-TOS-Precedence-Pri-Four (128) specifies priority level 4.
- IP-TOS-Precedence-Pri-Five (160) specifies priority level 5.
- IP-TOS-Precedence-Pri-Six (192) specifies priority level 6.
- IP-TOS-Precedence-Pri-Seven (224) specifies priority level 7 (the highest priority).

See Also: "Ascend-IP-TOS (88)" on page 3-49 and "Ascend-IP-TOS-Apply-To (90)" on page 3-50

Ascend-IPX-Alias (224)

Description: 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 the Ascend-IPX-Alias attribute have a decimal value (base 10), but IPX network numbers generally have hexadecimal values (base 16). In order to give the Ascend-IPX-Alias 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 3-51,
"Ascend-IPX-Route (174)" on page 3-51, and
"Ascend-Route-IPX (229)" on page 3-69.

Ascend-IPX-Peer-Mode (216)

Description: Specifies whether the caller associated with the user profile is an Ethernet client with its own IPX network address, or a dial-in PPP client.

Dial-in clients do not belong to an IPX network, so you must assign them an IPX network number. When you do so, a dial-in client can establish a routing connection with the MAX TNT. You must use the IPX-Dialin-Pool parameter in the MAX TNT configuration interface to define a virtual IPX network. The MAX TNT advertises the route to the virtual network, and assigns it as the network address for dial-in clients.

Usage: Specify one of the following values:

- IPX-Peer-Router (0) specifies that the caller is on the Ethernet network and has its own IPX address. IPX-Peer-Router is the default.
- IPX-Peer-Dialin (1) specifies 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 TNT to assign the caller an IPX address derived from the value of IPX-Dialin-Pool.

Dependencies: If the client does not supply its own unique node number, the MAX TNT assigns a unique node number to the client as well. The MAX TNT 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 3-51 and “Ascend-Route-IPX (229)” on page 3-69.

Ascend-IPX-Route (174)

Description: Enables you to configure a static IPX route in a pseudo-user profile.

Usage: To configure a static IPX route, use the following format:

Ascend-IPX-Route="*profile_name network#* [*node#*] [*socket#*] [*server_type*] [*hop_count*] [*tick_count*] [*server_name*]"

Table 3-12 describes each Ascend-IPX-Route argument.

Table 3-12. Ascend-IPX-Route arguments

Argument	Specifies
profile_name	RADIUS user profile the MAX TNT uses to reach the network. The default value is null.
network#	Unique internal network number for the NetWare server. The default value is 00000000.
node#	Node number for the NetWare server. The default value is 0000000000001 (the typical node number for a NetWare file server.)

Table 3-12. Ascend-IPX-Route arguments (continued)

Argument	Specifies
socket#	Socket number for 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 might 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	SAP service type of the NetWare server. NetWare file servers have SAP service type 0004. The default value is 0000.
hop_count	Distance to the destination network, in hops. The default value is 1.
tick_count	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	Name of an IPX server. The default value is null.

Example: To define an IPX route, you would configure a pseudo-user profile as follows:

```
ipxroute-CA-1 Password="ascend", User-Service=Dialout-Framed-User
        Ascend-IPX-Route="def 6 7 8 9 10"
```

See Also: "Ascend-IPX-Alias (224)" on page 3-50, "Ascend-IPX-Peer-Mode (216)" on page 3-51, and "Ascend-Route-IPX (229)" on page 3-69.

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 the following 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 the 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 the Ascend-Link-Compression attribute to turn on data compression.

By default, NetWare relies on the Data Link layer (also called Layer 2) to validate and guarantee data integrity. When you configure Stac compression, the system performs an eight-bit checksum, which is inadequate for NetWare data. Therefore, for NetWare connections, carry out one of the following tasks:

- Specify Link-Comp-Stac-Draft-9 or Link-Comp-MS-Stac, which use a more robust error-checking method.
- Disable link compression by setting Ascend-Link-Compression=Link-Comp-None. When you do so, the MAX TNT guarantees data integrity by means of PPP.
- Accept the default Link-Comp-Stac setting, and enable IPX checksums on your NetWare servers and clients. Both the server and the client must support IPX checksums. If you enable checksums on your servers, but not on your clients, all logins will fail.

See Also: "Framed-Compression (13)" on page 3-83.

Ascend-Maximum-Call-Duration (125)

Description: Specifies the maximum number of minutes that the MAX TNT allows individual channels in a call to stay connected, regardless of the data traffic over the connection. When the time expires in single-channel calls, the MAX TNT disconnects the call. When the time expires for a channel in a multichannel call, the MAX TNT disconnects only the single channel, leaving the call connected.

Usage: Specify an integer from 0 to 1440. The MAX TNT 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), which specifies that the MAX TNT does not set a limit on the duration of the call.

Dependencies: For single-channel calls, the functionality of Ascend-Maximum-Time matches the functionality of Ascend-Maximum-Call-Duration.

See Also: "Ascend-Maximum-Time (194)" on page 3-54.

Ascend-Maximum-Channels (235)

Description: Specifies the maximum number of channels allowed on an MP+ call.

Usage: Specify an integer from 1 to the maximum number of channels your system supports. The default value is 1, which prevents a client from establishing a multichannel call.

Dependencies: The Ascend-Maximum-Channels attribute applies only to MP+ calls. For optimum MP+ performance, both sides of a connection must set the following values to the same number:

- Base channel count, as specified by Base-Channel-Count (in the Connection profile) or Ascend-Base-Channel-Count (in RADIUS).
- Minimum channel count, as specified by Minimum-Channels (in the Answer-Defaults profile or Connection profile) or Ascend-Minimum-Channels (in RADIUS).
- Maximum channel count, as specified by Maximum-Channels (in the Answer-Defaults profile or Connection profile) or Ascend-Maximum-Channels (in RADIUS).

See Also: "Ascend-Add-Seconds (240)" on page 3-4,
"Ascend-Base-Channel-Count (172)" on page 3-9,
"Ascend-DBA-Monitor (171)" on page 3-27,
"Ascend-Dec-Channel-Count (237)" on page 3-27,
"Ascend-History-Weigh-Type (239)" on page 3-44,
"Ascend-Inc-Channel-Count (236)" on page 3-47,
"Ascend-Minimum-Channels (173)" on page 3-57,
"Ascend-Remove-Seconds (241)" on page 3-68,
"Ascend-Seconds-Of-History (238)" on page 3-72, and
"Ascend-Target-Util (234)" on page 3-75.

Ascend-Maximum-Time (194)

Description: Specifies the maximum number of seconds that the MAX TNT allows the call to stay connected, regardless of the data traffic over the connection. When the time expires, the MAX TNT disconnects the call.

Usage: Specify an integer from 0 to 4,294,967,295. The default value is 0 (zero) , which specifies that the MAX TNT does not enforce a time limit.

Dependencies: Consider the following:

- Ascend-Maximum-Time will be deprecated in favor of the RFC-defined attribute Session-Timeout (27). Currently, if a user profile specifies both an RFC-defined attribute and an Ascend vendor attribute that performs a similar function, the last one sent by the server is used. However, using both attributes is not reliable and is not recommended.
- For single-channel calls, the functionality of Ascend-Maximum-Time matches the functionality of Ascend-Maximum-Call-Duration.

See Also: "Ascend-Maximum-Call-Duration (125)" on page 3-53 and "Session-Timeout (27)" on page 3-94.

Ascend-Menu-Item (206)

Description: Defines a single terminal-server menu item for a user profile. You can specify up to 20 Ascend-Menu-Item attributes per profile. The screen displays the menu items in the order in which they appear in the RADIUS profile.

Using the Ascend-Menu-Item attribute, you can configure a profile to give a 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 the following format:

`Ascend-Menu Item=`*`command;text;match`

Table 3-13 lists each argument. If any entry consists of an option containing more than the maximum number of characters allowed, the RADIUS server discards the entry.

Table 3-13. Ascend-Menu-Item arguments

Argument	Description
command	Specifies the string sent to the terminal server when the user selects the menu item. The string must be in a format that the Ascend terminal server understands. It can contain up to 80 characters.
text	Specifies the text that appears on the user's screen, up to 31 characters.
match	Specifies the pattern, of up to 10 characters, that the user must type to select the item. The MAX TNT considers blanks part of the matching pattern.
; (semi-colon)	The first semicolon (;) you enter acts as the delimiter between ***command*** and ***text***. If you enter a second semicolon, it acts as the delimiter between ***text*** and ***match***.

By default, the MAX TNT uses the standard terminal-server menu.

Example: Suppose you set the following 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 the following text:

```
1. Display IP Stats     3. Telnet to Ken's machine
2. Ping server          4. Display ARP Table.
               Option:
```

See Also: "Ascend-Menu-Selector (205)" on page 3-56.

Ascend-Menu-Selector (205)

Description: 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 the following 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 automatically determines the value of *num* by counting 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.

Usage: Specify a text string of up to 31 characters. The terminal server displays the string when prompting the user for a menu selection.

Example: Suppose you set the following 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 the following 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 3-54.

Ascend-Metric (225)

Description: Specifies the virtual hop count of an IP route.

If there are two routes available to a single destination network, you can make sure that the MAX TNT uses any available nailed-up channel before it uses 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 TNT will bring the link online. The MAX TNT uses the lowest metric.

Usage: Specify a number from 1 to 15. The default value is 7.

Dependencies: 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 TNT does not bring the user's link online. However, if the link is already online, the MAX TNT does not use the nailed-up line.

See Also: "Ascend-Route-IP (228)" on page 3-69 and "Framed-Route (22)" on page 3-86.

Ascend-Minimum-Channels (173)

Description: Specifies the minimum number of channels an MP+ call maintains.

Usage: Specify a number from 1 to 32. The default value is 1.

Dependencies: The Ascend-Minimum-Channels attribute applies only to MP+ calls. For optimum MP+ performance, both sides of a connection must set the following values to the same number:

- Base channel count, as specified by Base-Channel-Count (in the Connection profile) or Ascend-Base-Channel-Count (in RADIUS).
- Minimum channel count, as specified by Minimum-Channels (in the Answer-Defaults profile or Connection profile) or Ascend-Minimum-Channels (in RADIUS).
- Maximum channel count, as specified by Maximum-Channels (in the Answer-Defaults profile or Connection profile) or Ascend-Maximum-Channels (in RADIUS).

See Also: "Ascend-Add-Seconds (240)" on page 3-4,
"Ascend-Base-Channel-Count (172)" on page 3-9,
"Ascend-DBA-Monitor (171)" on page 3-27,
"Ascend-Dec-Channel-Count (237)" on page 3-27,
"Ascend-History-Weigh-Type (239)" on page 3-44,
"Ascend-Inc-Channel-Count (236)" on page 3-47,
"Ascend-Maximum-Channels (235)" on page 3-53,
"Ascend-Remove-Seconds (241)" on page 3-68,
"Ascend-Seconds-Of-History (238)" on page 3-72, and
"Ascend-Target-Util (234)" on page 3-75.

Ascend-Modem-PortNo (120)

Description: Indicates the number of the port on the specified slot that terminates the call.

Usage: The Ascend-Modem-PortNo attribute appears in Start records, Stop records, and Checkpoint records.

See Also: "Ascend-Modem-ShelfNo (122)" on page 3-57 and "Ascend-Modem-SlotNo (121)" on page 3-58.

Ascend-Modem-ShelfNo (122)

Description: Indicates the number of the shelf that terminates the call.

Usage: The Ascend-Modem-ShelfNo attribute appears in Start records, Stop records, and Checkpoint records.

See Also: "Ascend-Modem-PortNo (120)" on page 3-57 and "Ascend-Modem-SlotNo (121)" on page 3-58.

Ascend-Modem-SlotNo (121)

Description: Indicates the number of the slot on the specified shelf that terminates the call.

Usage: The Ascend-Modem-SlotNo attribute appears in Start records, Stop records, and Checkpoint records.

See Also: "Ascend-Modem-PortNo (120)" on page 3-57 and "Ascend-Modem-ShelfNo (122)" on page 3-57.

Ascend-MPP-Idle-Percent (254)

Description: Specifies a percentage of bandwidth utilization below which the MAX TNT clears a single-channel MP+ call.

Usage: Specify a number from 0 to 99. The default value is 0 (zero), which causes the MAX TNT to ignore bandwidth utilization when determining whether to clear a call.

Dependencies: Consider the following:

- MP+ must be in use on the link.
- If either end of a connection sets the Ascend-MPP-Idle-Percent attribute to 0 (zero), the MAX TNT ignores bandwidth utilization when determining when to clear a call.
- Bandwidth utilization *on both sides of the connection* must fall below the percentage specified by Ascend-MPP-Idle-Percent before the MAX TNT 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 TNT 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, Ascend recommends that you use the Ascend-Idle-Limit attribute instead.

See Also: "Ascend-Idle-Limit (244)" on page 3-46 and "Ascend-Preempt-Limit (245)" on page 3-62.

Ascend-Multicast-Client (155)

Description: Specifies whether the user is a multicast client of the MAX TNT.

Usage: Specify one of the following values:

- Multicast-No (0) specifies that the user is not a multicast client of the MAX TNT. Multicast-No is the default.
- Multicast-Yes (1) specifies that the user is a multicast client of the MAX TNT.

See Also: "Ascend-Multicast-Rate-Limit (152)" on page 3-59.

Ascend-Multicast-GLeave-Delay (111)

Description: Specifies the number of seconds the MAX TNT waits before forwarding an IGMP version 2 `leave group` message from a multicast client.

Usage: Specify a number of seconds from 0 to 120. The default is 0 (zero). If you specify a value other than the default, and the MAX TNT receives a `leave group` message, the unit sends an IGMP query to the WAN interface or client from which it received the `leave group` message. If the MAX TNT does not receive a response from an active multicast client from the same group, it sends a `leave group` message when the time you specify expires.

If you accept the default, the MAX TNT forwards a `leave group` message immediately. If users might establish multiple multicast sessions for identical groups, set Ascend-Multicast-GLeave-Delay to a value of 10 to 20 seconds.

Dependencies: Ascend-Multicast-GLeave-Delay applies only if you set Multicast-Forwarding=Yes in the IP-Global profile, and Multicast-Allowed=Yes in the IP-Interface profile.

See Also: "Ascend-Multicast-Client (155)" on page 3-58.

Ascend-Multicast-Rate-Limit (152)

Description: Specifies how many seconds the MAX TNT 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 TNT accepts packets from clients.

Usage: Specify an integer. If you set the attribute to 0 (zero), the MAX TNT does not apply rate limiting. The default value is 100.

See Also: "Ascend-Multicast-Client (155)" on page 3-58.

Ascend-Multilink-ID (187)

Description: Specifies the ID number of the Multilink bundle when the session closes. A Multilink bundle is a multichannel MP or MP+ call.

Usage: Ascend-Multilink-ID does not appear in a user profile and has no default value.

Dependencies: The MAX TNT sends Ascend-Multilink-ID in an Accounting-Request packet when both of the following conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).

See Also: "Ascend-Num-In-Multilink (188)" on page 3-60.

Ascend-Number-Sessions (202)

Description: Indicates 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.

Dependencies: The MAX TNT sends the Ascend-Number-Sessions attribute in an Ascend-Access-Event-Request (33) packet. Only RADIUS daemons you customize to recognize this packet respond to requests from the MAX TNT. Other daemons ignore it.

When modifying the daemon, make sure that it recognizes an Ascend-Access-Event-Request packet in the following 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 TNT 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 TNT sends back to the RADIUS accounting server has three Ascend-Number-Session attributes, one for each of the class/session pairs.

See Also: "Ascend-Event-Type (150)" on page 3-35 and "Class (25)" on page 3-82.

Ascend-Num-In-Multilink (188)

Description: Indicates the number of sessions remaining in a Multilink bundle when the session closes. A Multilink bundle is a multichannel MP or MP+ call.

Usage: Ascend-Num-In-Multilink does not appear in a user profile and has no default value.

Dependencies: The MAX TNT sends Ascend-Num-In-Multilink in an Accounting-Request packet when both of the following conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).

See Also: "Ascend-Multilink-ID (187)" on page 3-59.

Ascend-PPP-Address (253)

Description: Specifies the IP address of the local numbered interface.

Usage: Specify an IP address in dotted decimal notation. The default value is 0.0.0.0.

See Also: "Ascend-IF-Netmask (153)" on page 3-46 and "Ascend-Remote-Addr (154)" on page 3-67.

Ascend-PPP-Async-Map (212)

Description: Specifies the async control character map for the PPP, MP, or MP+ session. The MAX TNT passes the control characters through the link as data. Only applications running over the link use the characters.

Usage: Specify a four-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 the following:

```
Emma Password="m2dan", User-Service=Login-User
     Ascend-PPP-Async-Map=19,
     ...
```

The number 19 translates to 13 hexadecimal or 10011 binary. Therefore, NUL (00), SOH (01), and EOT (04) are mapped.

Ascend-PPP-VJ-1172 (211)

Description: Specifies whether the MAX TNT uses the 0037h value for the VJ compression type. The MAX TNT uses the value only during IPNCP negotiation.

RFC 1172 section 5.2 contains an erroneous statement that the VJ compression type value is 0037h. It should be 002dh. However, many older implementations use the 0037h value when negotiating VJ compression. If you do not specify a value for Ascend-PPP-VJ-1172, the VJ compression type is 002dh.

Usage: Enter your specification in the following format:

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

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

Description: Instructs the MAX TNT to not use slot compression when sending VJ-compressed packets.

When you turn on VJ compression, the MAX TNT 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 TNT associates it with the last-used slot ID. This scenario uses slot ID compression, because the slot ID does not appear in any packet but the first in a stream.

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 3-83.

Ascend-Preempt-Limit (245)

Description: Specifies the number of idle seconds the MAX TNT waits before using one of the channels of an idle link for a new call.

Usage: Specify a number from 0 to 65535. The MAX TNT 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 3-46 and "Ascend-MPP-Idle-Percent (254)" on page 3-58.

Ascend-Pre-Input-Octets (190)

Description: Reports the number of octets received before authentication. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.

Usage: Ascend-Pre-Input-Octets does not appear in a user profile. Its default value is 0 (zero).

Dependencies: The MAX TNT includes Ascend-Pre-Input-Octets in an Accounting-Request packet when all of the following conditions are true:

- The session was authenticated.
- The connection was asynchronous.
- The session has ended (Acct-Status-Type=Stop).

Ascend-Pre-Input-Packets (192)

Description: Reports the number of packets received before authentication. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.

Usage: Ascend-Pre-Input-Packets does not appear in a user profile. Its default value is 0 (zero).

Dependencies: The MAX TNT includes Ascend-Pre-Input-Packets in an Accounting-Request packet when both of the following conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).

Ascend-Pre-Output-Octets (191)

Description: Reports the number of octets transmitted before authentication. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.

Usage: Ascend-Pre-Output-Octets does not appear in a user profile. Its default value is 0 (zero).

Dependencies: The MAX TNT includes Ascend-Pre-Output-Octets in an Accounting-Request packet when all of the following conditions are true:

- The session was authenticated.
- The connection was asynchronous.
- The session has ended (Acct-Status-Type=Stop).

Ascend-Pre-Output-Packets (193)

Description: Reports the number of packets transmitted before authentication. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.

Usage: Ascend-Pre-Output-Packets does not appear in a user profile. Its default value is 0 (zero).

Dependencies: The MAX TNT includes Ascend-Pre-Output-Packets in an Accounting-Request packet when both of the following conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).

Ascend-PreSession-Time (198)

Description: Reports the length of time in seconds from when a call connected to when it completes authentication.

Usage: Ascend-PreSession-Time does not appear in a user profile. Its default value is 0 (zero).

Dependencies: The MAX TNT includes Ascend-PreSession-Time in an Accounting-Request packet when the session has ended or has failed authentication (Acct-Status-Type=Stop).

Ascend-PRI-Number-Type (226)

Description: Specifies the type of phone number the MAX TNT dials.

Usage: Specify one of the settings listed in Table 3-14.

Table 3-14. Ascend-PRI-Number-Type settings

Setting	Specifies
Unknown-Number (0)	Any type of number.
Intl-Number (1)	A number outside the U.S.
National-Number (2)	A number inside the U.S. The default value is National-Number.
Local-Number (4)	A number within your Centrex group.
Abbrev-Number (5)	An abbreviated phone number.

Ascend-Private-Route (104)

Description: Specifies a destination address and next-hop router address for a private route.

A RADIUS user profile can specify a list of private routes associated with the connection. The private routes affect only packets received from the connection. (The routes are not added to the global routing table.) If a destination is not found in the list of private routes and there is no default private route, the global routing table is consulted for a decision on routing the packets. Otherwise, only the private routing table is consulted.

Usage: In a user profile, specify the attribute in the following format:

Ascend-Private-Route="*dest_addr/netmask next_hop/netmask*"

where ***dest_addr/netmask*** is the destination address of the route, and ***next_hop/netmask*** is the address of the next-hop router.

Example: Following is a sample user profile that creates three private routes associated with the caller:

```
pipe50 Password="ascend", User-Service=Framed-User
   Framed-Protocol=PPP,
   Framed-Address=10.1.1.1,
   Framed-Netmask=255.0.0.0,
   Ascend-Private-Route="170.1.0.0/16 10.10.10.1"
   Ascend-Private-Route="200.1.1.1/32 10.10.10.2"
   Ascend-Private-Route="20.1.0.0/16 10.10.10.3"
   Ascend-Private-Route="0.0.0.0/0 10.10.10.4"
```

With this profile, the private routing table for the connection contains the following routes, including a default route:

```
Dest/Mask        Gateway
170.1.0.0/16     10.10.10.1
200.1.1.1/32     10.10.10.2
20.1.0.0/16      10.10.10.3
0.0.0.0/0        10.10.10.4
```

Dependencies: The user profile can also specify the Ascend-Client-Gateway attribute, but the specification will *not* modify the private default route if one has been specified via the Ascend-Private-Route attribute.

See Also: "Ascend-Client-Gateway (132)" on page 3-17.

Ascend-PW-Expiration (21)

Description: Specifies an expiration date for a user's password. When the MAX TNT 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 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, 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.

Usage: Specify a month, day, and year in the following format:

month day year

Separate each part of the date specification with one or more spaces, tabs, or commas. The default value is 00/00/00.

Table 3-15 lists each argument.

Table 3-15. Ascend-PW-Expiration arguments

Argument	Specifies
month	The first three letters of the month in which you want the password to expire, or the entire name of the month. Begin the specification with a capital letter.
day	One or more digits indicating a valid day of the month. The settings 2, 02, 002, and 0021 are all valid, but 32 is not.
year	A four-digit year.

Dependencies: Consider the following:

- 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.
- If the password has not expired, the value of Ascend-PW-Expiration overrides the value of Ascend-PW-Lifetime.

Example: You might enter a specification like the following:

```
Emma Password="m2dan", Ascend-PW-Expiration="January 1, 1997"
...
```

See Also: "Ascend-PW-Lifetime (208)" on page 3-66.

Ascend-PW-Lifetime (208)

Description: Specifies the number of days that a password is valid.

Usage: Specify an integer. You can set the Ascend-PW-Lifetime attribute on any line other than the first.

Dependencies: Consider the following:

- 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.
- If the password has not expired, the value of Ascend-PW-Expiration overrides the value of Ascend-PW-Lifetime.
- 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), which indicates that passwords do not expire.

Example: You might make the following specification:

```
Emma Password="m2dan", Ascend-PW-Expiration="Jan 1, 1997"
     Ascend-PW-Lifetime=30
```

See Also: "Ascend-PW-Expiration (21)" on page 3-65.

Ascend-PW-Warntime (207)

Description: Specifies the number of days before password expiration that the RADIUS server sends a message informing the user that the password will expire. The message appears when the user establishes a connection, and is carried to the MAX TNT in the Reply-Message attribute.

Usage: Specify an integer. The default is 0 (zero), which indicates that no warning message is sent.

Example: Suppose you set Ascend-PW-Warntime=5. Starting five days before the expiration of the password, the RADIUS server sends a message telling the user the number of days until the password expires.

Dependencies: Note that the user might never see a warning message, even though the RADIUS server returns the message to the MAX TNT. This situation can occur if the user is using PPP for authentication (rather than the terminal server), or using a script to exchange information with the terminal server.

See Also: "Ascend-PW-Expiration (21)" on page 3-65 and "Ascend-PW-Lifetime (208)" on page 3-66.

Ascend-Receive-Secret (215)

Description: Specifies a value that must match the password the calling unit sends to your MAX TNT.

Usage: Specify up to 20 characters. The default value is null.

Dependencies: You can set the Ascend-Receive-Secret attribute for Cache-Token or PAP-Token-CHAP authentication only.

Example: The following example shows the settings you would specify for a user called Emma to access an Enigma Logic server. Because the profile includes Ascend-Receive-Secret, the MAX TNT can authenticate additional channels through CHAP without having to use the SAFEWORD server for authentication.

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

Ascend-Redirect-Number (93)

Description: Indicates the redirected number extracted from the Redirect Number Information Element (IE) in an ISDN frame. If the IE is present, this number is sent to the RADIUS server for each Start and Stop accounting request. If the IE is not present in the frame, the attribute is not sent to the RADIUS server

Usage: You can use the Redirect Number Information Element in an ISDN frame to bill dial-in clients according to the original called number. This Information Element is generated by a Public Switched Telephone Network (PSTN) switch when the phone number dialed by a customer has been redirected to an another number.

Ascend-Remote-Addr (154)

Description: Specifies the IP address of the numbered interface at the remote end of a link.

Usage: Specify the IP address of the numbered interface in dotted decimal notation. 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-IF-Netmask (153)" on page 3-46,
"Ascend-PPP-Address (253)" on page 3-60, and
"Ascend-Route-IP (228)" on page 3-69.

Ascend-Remove-Seconds (241)

Description: Specifies the number of seconds that average line utilization (ALU) for transmitted data must fall below the Ascend-Target-Util threshold before the MAX TNT begins removing bandwidth from a session. The MAX TNT determines the ALU for a session by means of the Ascend-History-Weigh-Type algorithm.

When utilization falls below the threshold for a period of time greater than the value of the Ascend-Remove-Seconds attribute, the MAX TNT 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 from 1 to 300. The default value is 10.

Dependencies: Consider the following:

- 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 3-4,
"Ascend-Base-Channel-Count (172)" on page 3-9,
"Ascend-DBA-Monitor (171)" on page 3-27,
"Ascend-Dec-Channel-Count (237)" on page 3-27,
"Ascend-History-Weigh-Type (239)" on page 3-44,
"Ascend-Inc-Channel-Count (236)" on page 3-47,
"Ascend-Maximum-Channels (235)" on page 3-53,
"Ascend-Minimum-Channels (173)" on page 3-57,
"Ascend-Seconds-Of-History (238)" on page 3-72, and
"Ascend-Target-Util (234)" on page 3-75.

Ascend-Require-Auth (201)

Description: Specifies whether the MAX TNT requires additional authentication after Calling-Line ID (CLID) or called-number authentication.

Usage: Specify one of the following values:

- Not-Require-Auth (0) specifies that the MAX TNT does not require additional authentication. Not-Require-Auth is the default.
- Require-Auth (1) specifies that the MAX TNT requires additional authentication.

Dependencies: 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 another user profile.

Example: The following example shows a two-tiered approach to using the Ascend-Require-Auth attribute. The first user profile specifies CLID authentication, and indicates that additional authentication will follow. Because Recv-Auth-Mode=CHAP-PPP-Auth in the PPP-Answer subprofile of the Answer-Defaults 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 allowed for the user profile.

Usage: Specify one of the following values:

- Route-AppleTalk-No (0) disables AppleTalk routing for the profile. This setting is the default.
- Route-AppleTalk-Yes (1) enables AppleTalk routing for the profile.

See Also: "Ascend-ARA-PW (181)" on page 3-5.

Ascend-Route-IP (228)

Description: Specifies whether IP routing is allowed for the user profile.

Usage: Specify one of the following values:

- Route-IP-No (0) disables IP routing for the profile.
- Route-IP-Yes (1) enables IP routing for the profile. Route-IP-Yes is the default.

See Also: "Framed-Route (22)" on page 3-86.

Ascend-Route-IPX (229)

Description: Specifies whether IPX routing is allowed for the user profile.

Usage: Specify one of the following values:

- Route-IPX-No (0) disables IPX routing. Route-IPX-No is the default.
- Route-IPX-Yes (1) enables IPX routing.

Dependencies: For PPP and MP+ calls, both ends of the connection must have matching settings to route IPX.

See Also: "Ascend-IPX-Alias (224)" on page 3-50,
"Ascend-IPX-Peer-Mode (216)" on page 3-51, and
"Ascend-IPX-Route (174)" on page 3-51.

Ascend-Route-Preference (126)

Description: Specifies the preference for a route defined by the Framed-Address attribute in a 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. Ascend recommends that you accept the default.

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
Infinite	225

See Also: “Framed-Address (8)” on page 3-83.

Ascend-Secondary-Home-Agent (130)

Description: Specifies the secondary Home Agent the Foreign Agent tries to reach when the primary Home Agent (Tunnel-Server-Endpoint) times out, or the Foreign Agent receives an error code in an ATMP Register Reply or Challenge Request message. The attribute also specifies the UDP port the Foreign Agent uses for the link.

Usage: Specify the secondary Home Agent using the following format:

`Ascend-Secondary-Home-Agent="`*`hostname`*` | `*`ip_address`*` [:`*`udp_port`*`]"`

Table 3-16 lists each element of the syntax.

Table 3-16. Ascend-Secondary-Home-Agent syntax

Syntax element	Specifies
hostname	Home Agent's symbolic hostname.
ip_address	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 host name or an IP address, but not both. The Home Agent IP address should be the system address, not the IP address of the interface on which the Home Agent receives tunneled data.
udp_port	UDP port on which the Foreign Agent communicates with the Home Agent. The default value is 5150.
: (colon)	Separator between the hostname (or IP address) and the UDP port.

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.

Example: To specify max2.home.com at IP address 10.0.0.2 as the secondary Home Agent, and to indicate that the Foreign Agent should use UDP port 6002, enter one of the following 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 the following lines in the RADIUS user profile:

```
Tunnel-Server-Endpoint="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.

See Also: "Ascend-Home-Agent-UDP-Port (186)" on page 3-45,
"Ascend-Home-Network-Name (185)" on page 3-45,
"Tunnel-Server-Endpoint (67)" on page 3-96, and
"Tunnel-Server-Endpoint (67)" on page 3-96.

Ascend-Seconds-Of-History (238)

Description: Specifies the number of seconds the MAX TNT uses as a sample for calculating average line utilization (ALU) of transmitted data. The MAX TNT arrives at this average by using the algorithm specified by the Ascend-History-Weigh-Type attribute.

Usage: Specify a number from 1 to 300. The default value is 15 seconds. The number of seconds you specify depends on your device's traffic patterns. For example, if you want to average spikes with normal traffic flow, you might want the MAX TNT to use a longer time period. If, on the other hand, traffic patterns consist of many spikes that are short in duration, you might want to specify a shorter period of time. Doing so assigns less weight to the short spikes.

Dependencies: Consider the following:

- Ascend-Seconds-Of-History applies only to MP+ calls.
- If you specify a small value for the Ascend-Seconds-Of-History attribute, and increase the values of the Ascend-Add-Seconds and Ascend-Remove-Seconds attributes, the system becomes less responsive to quick spikes.
- The easiest way to determine the values for all the attributes is to observe usage patterns.

See Also: "Ascend-Add-Seconds (240)" on page 3-4,
"Ascend-Base-Channel-Count (172)" on page 3-9,
"Ascend-DBA-Monitor (171)" on page 3-27,
"Ascend-Dec-Channel-Count (237)" on page 3-27,
"Ascend-History-Weigh-Type (239)" on page 3-44,
"Ascend-Inc-Channel-Count (236)" on page 3-47,
"Ascend-Maximum-Channels (235)" on page 3-53,
"Ascend-Minimum-Channels (173)" on page 3-57,
"Ascend-Remove-Seconds (241)" on page 3-68, and
"Ascend-Target-Util (234)" on page 3-75.

Ascend-Send-Auth (231)

Description: Specifies the authentication protocol that the MAX TNT requests when initiating a PPP or MP+ connection. The answering side of the connection determines which authentication protocol, if any, the connection uses.

Usage: Specify one of the following values:

- Send-Auth-None (0) specifies that the MAX TNT does not request an authentication protocol for outgoing calls. Send-Auth-None is the default.
- Send-Auth-PAP (1) specifies that the MAX TNT requests Password Authentication Protocol (PAP). The MAX TNT requests PAP authentication, but uses CHAP authentication if the called unit requires CHAP. To send your password unencrypted, choose this setting.
- Send-Auth-CHAP (2) specifies that the MAX TNT requests Challenge Handshake Authentication Protocol (CHAP). The remote device must support CHAP. To send an encrypted password, choose this setting.

Dependencies: Consider the following:

- Ascend-Send-Auth applies 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 with Ascend-Send-Secret or Ascend-Send-Passwd.
- You must set Ascend-Send-Auth=Send-Auth-None for a CBCP application.

See Also: "Ascend-Send-Passwd (232)" on page 3-73 and "Ascend-Send-Secret (214)" on page 3-73.

Ascend-Send-Passwd (232)

Description: Specifies the password that the RADIUS server sends to the remote end of a connection on an outgoing call. It is not encrypted when passed between the RADIUS server and the MAX TNT.

Usage: Specify a text string of 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 TNT does not support Ascend-Send-Secret.

See Also: "Ascend-Send-Auth (231)" on page 3-72 and "Ascend-Send-Secret (214)" on page 3-73.

Ascend-Send-Secret (214)

Description: 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 TNT.

Usage: Specify a text string of 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 TNT does not support Ascend-Send-Secret.

See Also: "Ascend-Send-Auth (231)" on page 3-72 and "Ascend-Send-Passwd (232)" on page 3-73.

Ascend-Session-Svr-Key (151)

Description: Enables the MAX TNT to match a user session with a client request to perform certain operations, such as disconnecting a session or changing a session's filters.

Usage: Specify up to 16 characters. The default value is null.

Dependencies: Consider the following:

- 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.
- The Ascend-Session-Svr-Key attribute appears in a RADIUS Accounting-Start packet when a session starts.
- The client sends the Ascend-Session-Svr-Key attribute only if Auth-Session-Key=Yes in the Rad-Auth-Server subprofile of the External-Auth profile.

Ascend-Shared-Profile-Enable (128)

Description: Specifies whether multiple incoming callers can share a single RADIUS user profile.

Usage: Specify one of the following settings:

- Shared-Profile-No (0) specifies that multiple incoming callers cannot share the RADIUS user profile. Shared-Profile-No is the default.
- Shared-Profile-Yes (1) specifies that multiple incoming callers can share the RADIUS user profile.

Dependencies: For the Ascend-Shared-Profile-Enable attribute to apply, you must set Shared-Prof=No in the IP-Global profile to disable shared profiles for the MAX TNT.

Ascend-Source-Auth (103)

Description: Specifies a source IP address and associated billing code.

RADIUS can look up a billing code on the basis of the source IP address of a packet. When the MAX TNT places a call on behalf of a packet with the specified source address, it also sends the associated billing code to the network switch. This feature is referred to as Source Auth.

Because looking up an IP address resembles a route lookup, this feature uses some of the same mechanisms as static routes. For example, Source Auth entries are retrieved from RADIUS when the router is initialized and the Source Auth information is cached for later use. The Source Auth entries can be refreshed by using the new Refresh –s command

Usage: In a user profile or pseudo-user profile, make your specification in the following format:

`Ascend-Source-Auth="`*`address/mask – authcode`*`"`

where ***`address/mask`*** is the source address and subnet mask, and ***`authcode`*** is the billing code conveyed to the switch when a call is placed on behalf of a packet from the given source address.

As with static routes, you can indicate the subnet mask with any desired level of specificity, and the most specific entry prevails in case of conflict. The maximum length of an ***authcode*** is the same as the maximum for Ascend-Billing-Number: 24 digits. The hyphen (–) delimiter is reserved for future capabilities.

Example: **`Ascend-Source-Auth="10.150.0.0/16 - 5105551212"`**

Ascend-Source-IP-Check (96)

Description: Enables or disables anti-spoofing for this session.

Usage: Specify one of the following settings:

- Source-IP-Check-No (0) disables anti-spoofing. This setting is the default.
- Source-IP-Check-Yes (1) specifies that the system checks all packets received on this interface to ensure that the source IP address in the packets matches the far-end remote address or the address agreed upon in IPCP negotiation. If the addresses do not match, the system discards the packet.

Example: In the following RADIUS user profile, anti-spoofing is enabled:

```
ed-mc1-p75 Password="localpw", User-Service=Framed-User
    Framed-Protocol=PPP,
    Framed-Address=10.7.8.200,
    Framed-Netmask=255.255.255.0,
    Ascend-Source-IP-Check=Source-IP-Check-Yes
```

Ascend-Target-Util (234)

Description: Specifies the percentage of bandwidth use at which the MAX TNT adds or subtracts bandwidth.

Usage: Specify a number from 0 to 100. The default value is 70. With a value of 70%, the device adds bandwidth when it exceeds a 70 percent utilization rate, and subtracts bandwidth when it falls below that number.

Dependencies: When choosing a target utilization rate, consider the following:

- Monitor how the application behaves when using different bandwidths. For example, an application might be able to use 88% of a 64-Kbps link, but only 70% of a 256-Kbps link.
- Monitor the application at different loads.
- Ascend-Target-Util applies only if the link is using MP+ encapsulation.

See Also: “Ascend-Add-Seconds (240)” on page 3-4,
“Ascend-Base-Channel-Count (172)” on page 3-9,
“Ascend-DBA-Monitor (171)” on page 3-27,
“Ascend-Dec-Channel-Count (237)” on page 3-27,
“Ascend-History-Weigh-Type (239)” on page 3-44,
“Ascend-Inc-Channel-Count (236)” on page 3-47,
“Ascend-Maximum-Channels (235)” on page 3-53,
“Ascend-Minimum-Channels (173)” on page 3-57,
“Ascend-Remove-Seconds (241)” on page 3-68, and
“Ascend-Seconds-Of-History (238)” on page 3-72.

Ascend-Third-Prompt (213)

Description: Indicates the value entered at the prompt specified by the Third-Login-Prompt parameter.

Usage: The Ascend-Third-Prompt attribute can contain up to 80 characters. It does not appear in a user profile. If the user enters more than 80 characters at the third prompt, the MAX TNT truncates the input to 80. If the user does not enter any characters, the MAX TNT sets the attribute to null.

Ascend-Token-Expiry (204)

Description: Specifies the lifetime (in minutes) of a cached token.

Usage: On the first line of the user profile, specify an integer representing the number of minutes in the lifetime of the cached token. The default value is 0 (zero). If you accept the default, the MAX TNT rejects subsequent Cache-Token requests from the same user.

Example: The following two-line example shows how to set 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 password.

```
Connor  Password="ACE", Ascend-Token-Expiry=90
        Ascend-Receive-Secret="shared-secret",
        ...
```

See Also: “Ascend-Token-Idle (199)” on page 3-76 and “Ascend-Token-Immediate (200)” on page 3-77.

Ascend-Token-Idle (199)

Description: 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 0 (zero). If you accept the 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 shows how to set 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 3-76 and “Ascend-Token-Immediate (200)” on page 3-77.

Ascend-Token-Immediate (200)

Description: Specifies how RADIUS treats the password it receives when the user profile specifies a token-card server. Use this attribute in an ACE or SAFEWORD user profile that contains the setting User-Service=Login-User.

Usage: Specify one of the following values:

- Tok-Imm-No (0) specifies that the MAX TNT ignores the password it receives from the user. Choose this value for a security server that requires a user to enter a token-card challenge before the server derives a password. Tok-Imm-No is the default.
- Tok-Imm-Yes (1) specifies that the MAX TNT sends the password to the token-card server for authentication.

Dependencies: The Ascend-Token-Immediate attribute does not work with CHAP authentication.

Example: To specify that the MAX TNT must send the password it receives from the login user to the ACE server, you would configure the user profile as follows:

```
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 3-76 and "Ascend-Token-Idle (199)" on page 3-76.

Ascend-Transit-Number (251)

Description: 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 a 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 TNT uses any available IEC for long-distance calls.

Ascend-TS-Idle-Limit (169)

Description: Specifies the number of seconds that a terminal-server connection must be idle before the MAX TNT disconnects the session.

Usage: Specify a value from 0 to 65535.The default value is 120. A setting of 0 (zero) specifies 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 3-78.

Ascend-TS-Idle-Mode (170)

Description: Specifies whether the MAX TNT uses a terminal-server idle timer and, if so, whether both the user and host must be idle before the MAX TNT disconnects the session.

Usage: Specify one of the following settings:

- TS-Idle-None (0) specifies that the MAX TNT does not disconnect the session no matter how long the line is idle. This setting disables the idle timer.
- TS-Idle-Input (1) specifies that the MAX TNT 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) specifies that the MAX TNT 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: To specify that the user must be idle for 90 seconds before the MAX TNT disconnects the session, you could configure a user profile as follows:

```
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 3-77.

Ascend-User-Acct-Base (142)

Description: Specifies whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16.

Usage: Specify one of the following settings:

- Ascend-User-Acct-Base-10 specifies that the numeric base is 10. The default value is 10.
- Ascend-User-Acct-Base-16 specifies that the numeric base is 16.

Dependencies: Changing the value of Ascend-User-Acct-Base while sessions are active results in inconsistent reporting between the Start and Stop records.

Example: When you set Ascend-User-Acct-Base=Ascend-User-Acct-Base-10, the MAX TNT presents a typical session ID to the accounting server in the following way:

```
"1234567890"
```

When you set Ascend-User-Acct-Base=Ascend-User-Acct-Base-16, the MAX TNT presents the same session ID in the following way:

```
"499602D2"
```

See Also: “Ascend-User-Acct-Host (139)” on page 3-79,
“Ascend-User-Acct-Key (141)” on page 3-79,
“Ascend-User-Acct-Port (140)” on page 3-79,
“Ascend-User-Acct-Time (143)” on page 3-80, and
“Ascend-User-Acct-Type (138)” on page 3-80.

Ascend-User-Acct-Host (139)

Description: Specifies the IP address of the RADIUS accounting server for the connection.

Usage: Specify an IP address in dotted decimal notation. The default value is 0.0.0.0.

See Also: "Setting up accounting on a per-user basis" on page 4-7,
"Ascend-User-Acct-Base (142)" on page 3-78,
"Ascend-User-Acct-Key (141)" on page 3-79,
"Ascend-User-Acct-Port (140)" on page 3-79,
"Ascend-User-Acct-Time (143)" on page 3-80, and
"Ascend-User-Acct-Type (138)" on page 3-80.

Ascend-User-Acct-Key (141)

Description: Specifies the RADIUS client password as it appears in the `clients` file.

Usage: Specify a text string. The default value is null.

See Also: "Setting up accounting on a per-user basis" on page 4-7,
"Ascend-User-Acct-Base (142)" on page 3-78,
"Ascend-User-Acct-Host (139)" on page 3-79,
"Ascend-User-Acct-Port (140)" on page 3-79,
"Ascend-User-Acct-Time (143)" on page 3-80, and
"Ascend-User-Acct-Type (138)" on page 3-80.

Ascend-User-Acct-Port (140)

Description: 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` argument when starting the daemon, specify the number of the UDP port for authentication services plus 1. You can specify a number from 1 to 32767.

See Also: "Setting up accounting on a per-user basis" on page 4-7,
"Ascend-User-Acct-Base (142)" on page 3-78,
"Ascend-User-Acct-Host (139)" on page 3-79,
"Ascend-User-Acct-Key (141)" on page 3-79,
"Ascend-User-Acct-Time (143)" on page 3-80, and
"Ascend-User-Acct-Type (138)" on page 3-80.

Ascend-User-Acct-Time (143)

Description: Specifies the number of seconds the MAX TNT waits for a response to a RADIUS accounting request for the connection.

Usage: Specify an integer from 1 to 10. The default value is 0 (zero).

See Also: "Setting up accounting on a per-user basis" on page 4-7, "Ascend-User-Acct-Base (142)" on page 3-78, "Ascend-User-Acct-Host (139)" on page 3-79, "Ascend-User-Acct-Key (141)" on page 3-79, "Ascend-User-Acct-Port (140)" on page 3-79, and "Ascend-User-Acct-Type (138)" on page 3-80.

Ascend-User-Acct-Type (138)

Description: Specifies the RADIUS accounting server(s) to use for the connection.

Usage: Specify one of the following settings:

- Ascend-User-Acct-None (0) specifies the MAX TNT sends accounting information to the RADIUS server specified by the Acct-Server parameter. This server is known as the *default server.* Ascend-User-Acct-None is the default.
- Ascend-User-Acct-User (1) specifies that the MAX TNT 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) specifies that the MAX TNT 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: "Setting up accounting on a per-user basis" on page 4-7, "Ascend-User-Acct-Base (142)" on page 3-78, "Ascend-User-Acct-Host (139)" on page 3-79, "Ascend-User-Acct-Key (141)" on page 3-79, "Ascend-User-Acct-Port (140)" on page 3-79, and "Ascend-User-Acct-Time (143)" on page 3-80.

Ascend-VRouter-Name (102)

Description: Specifies the name of a defined Virtual Router (VRouter). Specifying the VRouter name in a RADIUS user profile groups the WAN interfaces with the VRouter.

Usage: Specify the name of a VRouter. The default is null, which specifies that the global VRouter is in use.

Example: The following user profiles specifies a VRouter called Corpa:

```
bob Password="bob", User-Service=Framed-User
   Framed-Protocol=PPP,
   Ascend-VRouter-Name="Corpa"
```

See Also: "Ascend-IP-Pool-Definition (217)" on page 3-48 and "Framed-Route (22)" on page 3-86.

Ascend-Xmit-Rate (255)

Description: Specifies the rate of data transmitted on the connection in bits per second. For ISDN calls, Ascend-Xmit-Rate indicates the transmit data rate. For analog calls, it indicates the modem baud rate at the time of the initial connection.

Usage: Ascend-Xmit-Rate does not appear in a user profile. Its default value is 0 (zero).

Dependencies: The MAX TNT includes Ascend-Xmit-Rate in an Accounting-Request packet when the session has ended or has failed authentication (Acct-Status-Type=Stop).

Caller-Id (31)

Description: 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 TNT.

Usage: Specify a telephone number of up to 37 characters, limited to the following:

`1234567890()[]!z-*#|`

The default value is null.

Example: To set up CLID authentication with a name, password, and caller ID, you could configure a user profile as follows:

```
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-Route-IP=Route-IP-Yes,
      Ascend-Idle-Limit=30
```

Challenge-Response (3)

Description: Specifies the value that a Challenge Handshake Authentication Protocol (CHAP) user provides in response to the password challenge.

Usage: The MAX TNT sends the Challenge-Response value in an Access-Request packet. The default value is null.

Change-Password (17)

Description: Enables the MAX TNT 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 TNT sends an Access-Password-Request packet containing 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 the change only in the flat file. It cannot make the 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: Enables you to classify user sessions for purposes such as billing users on the basis of the service option they choose.

Keep in mind that accounting entries specify the class on a per-user and per-session basis. The Ascend-Number-Sessions attribute reports information about all user sessions (that is, on the number of current sessions of each class).

Usage: Specify an alphanumeric text string of up to 253 characters. The default value is null.

Dependencies: If you include the Class attribute in the RADIUS user profile, the RADIUS server sends it to the MAX TNT in the Access-Accept packet when the session begins. The MAX TNT then includes Class in Accounting-Request packets it sends to the RADIUS accounting server under the following conditions:

- Whenever a session starts
- Whenever a session stops

In addition, suppose the MAX TNT starts CLID authentication by sending an Access-Request packet, and receives the Class attribute in an Access-Accept packet. If the MAX TNT requires further authentication, it includes Class in the Access-Request packet

See Also: "Classifying user sessions in RADIUS" on page 4-11 and "Ascend-Number-Sessions (202)" on page 3-60.

Client-Port-DNIS (30)

Description: Specifies the called-party number, indicating the phone number the user dialed to connect to the MAX TNT. You use this attribute to set up called-number authentication or to route an incoming call to a particular device.

Usage: Specify the number the remote end dials to reach the MAX TNT, limiting your specification to the following 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 TNT share a group of digits. For example, a local caller might dial 555-1234, while a long distance caller would dial 1-415-555-1234. In such cases, you need only specify the rightmost digits the calls have in common. In this example, you would specify only 1234.

Example: To set up called-number authentication in addition to name and password authentication, you could configure the user profile as follows:

```
Clara-p50 Password="ascend", Client-Port-DNIS=1234
     User-Service=Framed-User,
     Framed-Protocol=PPP,
     Framed-Address=200.10.11.12,
     Framed-Netmask=255.255.255.248
```

Filter-ID (11)

Description: Specifies the name of a local Filter profile that defines a data filter. The next time the MAX TNT accesses the RADIUS user profile in which the Filter-ID attribute appears, the specified data filter is applied to the connection.

Usage: Specify a text string. The default is null. As is always the case with filters, the order in which they are applied within the user profile is significant. If the MAX TNT supports multiple Filter profiles with similar names, it uses the first Filter profile to match the characters specified in the user profile.

Dependencies: Filter-ID does not apply to call filters or Secure Access Firewalls.

See Also: "Ascend-Data-Filter (242)" on page 3-21.

Framed-Address (8)

Description: Specifies the IP address of a caller. RADIUS can authenticate an incoming caller by matching the user's IP address to the one specified in the user profile.

Usage: Specify an IP address in dotted decimal notation. The default value is 0.0.0.0. An answering user profile with the default 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 3-84.

Framed-Compression (13)

Description: 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, the Framed-Compression attribute does not turn on header compression.

Dependencies: Turning on header compression is most effective in reducing overhead when the data portion of the packet is small.

Framed-MTU (12)

Description: Specifies the maximum number of bytes the MAX TNT can receive in a single packet on a PPP, MP, MP+, or Frame Relay link.

Usage: The default value is 1524. You should accept the default unless the device at the remote end of the link cannot support it. If the administrator of the remote network determines that you must change the value, specify a number from 1 to 1524 (for a PPP, MP, or MP+ link) or from 128 to 1600 (for a Frame Relay link).

Framed-Netmask (9)

Description: Specifies a subnet mask for the caller at Framed-Address.

Usage: Specify an IP address in dotted decimal notation. The default value is 0.0.0.0, which specifies that the MAX TNT assumes a default subnet mask on the basis of the class of the address (as shown in Table 3-17).

Table 3-17. 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 3-83.

Framed-Protocol (7)

Description: In an Access-Request or Access-Accept packet, specifies the type of framed protocol the link can use. In an Accounting packet, specifies the type of framed protocol in use.

Note: When you set this attribute, the link cannot use any other type of framed protocol.

Usage: Table 3-18 lists the values for Framed-Protocol. By default, the MAX TNT does not limit the protocols a link can access.

Table 3-18. Framed-Protocol settings

Setting	Incoming call	Outgoing call
PPP (1)	A user requesting access can dial in with 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, MP, or MP+ framing. If the user dials in with any other type of framing, the MAX TNT rejects the call.	Outgoing calls use PPP framing.
SLIP (2)	A user requesting access can dial in unframed and change to SLIP framing.	Does not apply to outgoing calls.
ARA (255)	Specifies an AppleTalk Remote Access (ARA) connection.	Does not apply to outgoing calls.

Table 3-18. Framed-Protocol settings (continued)

Setting	Incoming call	Outgoing call
MPP (256)	Does not apply to incoming calls.	Outgoing calls request MP+ framing.
FR (261)	Does not apply to incoming calls.	Outgoing calls use Frame Relay (RFC 1490) framing.
MP (262)	Does not apply to incoming calls.	Outgoing calls request MP framing.
FR-CIR (263)	Specifies a Frame Relay circuit.	Specifies a Frame Relay circuit.
ATM-1483 (264)	Specifies ATM AAL5 encapsulation (defined in RFC 1483).	Specifies ATM AAL5 encapsulation (defined in RFC 1483).
ATM-FR-CIR (265)	Enables Frame Relay to ATM switching by converting Frame Relay encapsulation (defined in RFC 1490) to ATM AAL5 encapsulation (defined in RFC 1483). The conversion is described in the Frame Relay Forum FRF-5 implementation agreement.	Enables Frame Relay to ATM switching.

Dependencies: Framed-Protocol can appear in both Access-Request and Access-Accept packets. However, it does not appear in an Access-Request packet if Auth-Send67=No in the External-Auth profile's Rad-Auth-Client subprofile.

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 with the framing specified by Framed-Protocol. The MAX TNT rejects other types of framing. A user requesting access can also dial in without a framed protocol, and then change to the framing specified by Framed-Protocol.
- 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.

When Framed-Protocol=ATM-1483 or ATM-FR-CIR, you must specify a value for Ascend-ATM-Vpi and Ascend-ATM-Vci.

Example: To specify that a dial-in user can only use PPP protocols (PPP, MP+, or MP), and cannot use the terminal server, you could configure a user profile as follows:

```
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
       ...
```

See Also: "Ascend-ATM-Vci (95)" on page 3-7, "Ascend-ATM-Vpi (94)" on page 3-7, and "User-Service (6)" on page 3-98.

Framed-Route (22)

Description: Enables you to add static IP routes to the MAX TNT unit's routing table.

Usage: The Framed-Route attribute has the following format:

Framed-Route="*host_ipaddr*[*/subnet_mask*] *gateway_ipaddr metric* [*private*] [*profile_name*][*vrouter_name*]"

Table 3-19 describes each Framed-Route argument.

Table 3-19. Framed-Route arguments

Syntax element	Specifies
host_ipaddr [***/subnet_mask***]	IP address of the destination host or subnet reached by the route. The default value is 0.0.0.0/0., which represents the default route (the destination to which the MAX TNT forwards packets when no route to the packet's destination exists). 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	IP address of the router the MAX TNT uses to reach the target destination. The default value is 0.0.0.0. The 0.0.0.0 address is a wildcard entry the MAX TNT replaces with the caller's IP address.When RADIUS authenticates a caller and sends the MAX TNT an Access-Accept message with a value of 0.0.0.0 for ***router_ipaddr***, the MAX TNT 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 the MAX TNT assigns an IP address from an address pool and RADIUS cannot know the IP address of the caller.

Table 3-19. Framed-Route arguments (continued)

Syntax element	Specifies
metric	Metric for the route. If the MAX TNT has more than one possible route to a destination network, it chooses the one with the lower metric. The default value is 8.
private	Value **y** if the route is private, or **n** if it is not private. If you specify that the route is private, the MAX TNT does not disclose the existence of the route when queried by RIP or another routing protocol. The default value is **n**.
profile_name	Name of the outgoing user profile that uses the route. The default value is null.
vrouter_name	The Virtual Router (Vrouter) whose routing table will contain the static IP route.

Example: The following example shows how to set up two RADIUS pseudo-user profiles to define 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 3-69.

Framed-Routing (10)

Description: Specifies whether the MAX TNT sends Routing Information Protocol (RIP) packets, receives RIP packets, or both.

If you enable RIP to both send and receive updates on the WAN interface, the MAX TNT 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 can become quite large).

Usage: Specify one of the following values:

- None (0) specifies that the MAX TNT does not send or receive RIP updates. None is the default.
- Broadcast (1) specifies that the MAX TNT sends RIP version 1 updates, but does not receive them.
- Listen (2) specifies that the MAX TNT receives RIP version 1 updates, but does not send them.
- Broadcast-Listen (3) specifies that the MAX TNT both sends and receives RIP version 1 updates.

- Broadcast-v2 (4) specifies that the MAX TNT sends RIP version 2 updates, but does not receive them.
- Listen-v2 (5) specifies that the MAX TNT receives RIP version 2 updates, but does not send them.
- Broadcast-Listen-v2 (6) specifies that the MAX TNT both sends and receives RIP version 2 updates.

Dependencies: If you set Framed-Routing=None, the MAX TNT must rely on static routes you specify with Framed-Route.

See Also: "Ascend-Route-IP (228)" on page 3-69.

Idle-Timeout (28)

Description: Specifies the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt.

Usage: Specify a number from 0 to 65535. If you specify 0 (zero), the MAX TNT always clears a call when a session is inactive. The default value is 120 seconds. If you accept the default, and the Answer-Defaults profile specifies a value for the analogous Idle-Timer parameter, the MAX TNT ignores the Idle-Timer value and uses the Idle-Timeout default.

Dependencies: Consider the following:

- If the time set by the Idle-Timeout 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 Idle-Timeout attribute has expired.
- Because the Ascend-MPP-Idle-Percent attribute is dependent on traffic levels on both sides of the connection, Ascend recommends that you use the Idle-Timeout attribute instead.
- The Idle-Timeout attribute does not apply to nailed-up link.
- Idle-Timeout is identical to the Ascend vendor attribute Ascend-Idle-Limit, whose use will be deprecated over time. Currently, if a user profile specifies both an RFC-defined attribute and an Ascend vendor attribute that performs a similar function, the last one sent by the server is used. However, using both attributes is not reliable and is not recommended.

See Also: "Ascend-MPP-Idle-Percent (254)" on page 3-58 and "Ascend-Preempt-Limit (245)" on page 3-62.

Login-Host (14)

Description: Specifies the IP host to which the user automatically connects when you:

- Set User-Service=Login-User.
- Specify a value for Login-Service.

Access begins immediately after login.

Usage: Specify an IP address in dotted decimal notation. The default value is 0.0. 0.0, which specifies that the Login-User does not automatically connect to a particular host.

Dependencies: Consider the following:

- 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.)
- Closing the remote terminal-server session also automatically closes the session with Login-Host.
- When User-Service=Framed-User, RADIUS ignores the Login-Host attribute.
- You can configure up to four login host and port destinations for a TCP-Clear connection. While the TCP-Clear session is being established, if the TCP connection to the first specified host/port combination fails, the system attempts to connect to the next specified host, and so forth. If all connection attempts fail, the session terminates and the MAX TNT returns a TCP connection error to the dial-in client.
- TCP-Clear connections are managed on a per-router basis.

See Also: "Login-Service (15)" on page 3-89 and "User-Service (6)" on page 3-98.

Login-Service (15)

Description: Specifies the type of terminal-server connection a dial-in user makes to the IP host on your local network. The user makes the connection immediately after authentication, and never sees the terminal-server interface.

Usage: Specify one of the following values:

- Telnet (0) specifies that the user immediately establishes a Telnet session with the host specified by Login-Host.
- Rlogin (1) specifies that the user immediately establishes an Rlogin session with the host specified by Login-Host.
- TCP-Clear (2) specifies that the user immediately establishes a TCP session between the MAX TNT and the host specified by Login-Host. The TCP/IP connection cannot use the Telnet protocol. The user can run an application specified by Login-TCP-Port.

By default, the MAX TNT does not grant immediate access to an IP host.

Dependencies: Consider the following:

- If you specify both Login-Service and Login-Host, the MAX TNT automatically connects the Login-User to the host specified by Login-Host.
- If you do not specify Login-Service or Login-Host, the user sees either the MAX TNT unit's terminal-server command-line interface or the terminal-server menu interface, depending upon how you configure the MAX TNT.

Example: When you specify the following settings, a raw TCP session starts automatically for anyone who enters the Greg user name and the test1 password:

```
# The following profile causes an auto-TCP to 4.2.3.1 port 9
upon login.
Greg   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 3-89 and "Login-TCP-Port (16)" on page 3-90.

Login-TCP-Port (16)

Description: Specifies the port number to which a TCP session connects when Login-Service=TCP-Clear.

Usage: Specify an integer from 1 to 65535. The default value is 23.

Dependencies: You can configure up to four login host and port destinations for a TCP-Clear connection. While the TCP-Clear session is being established, if the TCP connection to the first specified host/port combination fails, the system attempts to connect to the next specified host, and so forth. If all connection attempts fail, the session terminates and the MAX TNT returns a TCP connection error to the dial-in client.

See Also: "Login-Host (14)" on page 3-89,
"Login-Service (15)" on page 3-89, and
"Login-TCP-Port (16)" on page 3-90.

NAS-Identifier (4)

Description: Indicates the IP address of the MAX TNT.

Usage: NAS-Identifier does not appear in a user profile. Its default value is 0.0.0.0.

NAS-Port (5)

Description: Indicates the network port on which the MAX TNT receives a call. The MAX TNT sends NAS-Port to the RADIUS server in an Accounting-Request packet. If you specify NAS-Port on the first line of a user profile, the MAX TNT sends the value you specify to the RADIUS server in an Access-Request packet.

Usage: The format of the NAS-Port value depends on the setting of the New-NAS-Port-ID-Format parameter in the System profile.

When New-NAS-Port-ID-Format=Yes

When New-NAS-Port-ID-Format=Yes, the NAS-Port value has the following format:

shelf slot line channel

where *shelf* specifies the shelf number (0–3), *slot* specifies the slot number (0–15), *line* specifies the line number (0–31), and *channel* specifies the channel number (0–31) for an ISDN call. For an analog call, the values are the same, except that line number can be 0–63, and the channel number is always 1. The default value for the RADIUS daemon appears in the `/etc/services` file.

The values are all bit encoded. For an ISDN call, the bit-encoded number has the following format:

- The shelf number is composed of two bits.
- The slot number is composed of four bits.
- The line and channel numbers are each composed of five bits.

For an analog call, the bit-encoded number has the following format:

- The shelf number is composed of two bits.
- The slot number is composed of four bits.
- The line number is composed of six bits.
- The channel number is composed of four bits.

When using this attribute for accounting purposes, you must add 1 to each component to ascertain the actual shelf, slot, line, and channel number.

When New-NAS-Port-ID-Format=No

When New-NAS-Port-ID-Format=Yes, the NAS-Port value has the following format:

tllcc

where *t* indicates `1` for a digital call or `2` for an analog call, *ll* indicates the line number, and *cc* indicates the channel number.

Example: To restrict an ISDN user to channel 2 on line 2 for slot 2 and shelf 1, you could set up a user profile as follows:

```
Robin Password="password", NAS-Port=1057, User-Service=Framed-User
      Framed-Protocol=PPP,
      Ascend-Assign-IP-Pool=1,
      Ascend-Route-IP=1,
      Ascend-Idle-Limit=300,
      Framed-Routing=None
```

The NAS-Port value of 1057 translates to the bit-encoded number 0000010000100001. This number indicates the following NAS port:

shelf=00 (shelf 1)

slot=0001 (slot 2)

line=00001 (line 2)

channel=00001 (channel 2)

NAS-Port-Type (61)

Description: Specifies the type of service in use for the session.

Some ISPs offer different levels of service on the basis of 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: Specify one of the following settings:

- NAS_Port_Type_Sync specifies a synchronous ISDN connection.
- NAS_Port_Type_Async specifies a call that the MAX TNT routes to a digital modem. NAS_Port_Type_Async is the default.

See Also: “NAS-Port (5)” on page 3-91.

Password (2)

Description: Specifies the password of the calling device or dial-in user.

Usage: Specify an alphanumeric string of up to 252 characters. The default value is null. The Password attribute must appear on the first line of the user profile.

Reply-Message (18)

Description: Carries message text from the RADIUS server to a RADIUS client (such as the MAX TNT). 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 at the menu-driven interface. In addition, if the RADIUS server determines that the MAX TNT should terminate the session, it sends an Access-Terminate-Session packet containing the Reply-Message attribute.

Usage: Specify a text string of up to 80 characters. The default value is null. You can specify up to 16 Reply-Message attributes in a pseudo-user profile.

Dependencies: Consider the following:

- 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.
- 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, the following message appears:

  ```
  ** Bad Password
  ```

- 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 TNT displays the following message to the terminal-server user:

  ```
  ** Session Terminated
  ```

Example: To set up message text for a MAX TNT named Cal, you could configure a pseudo-user profile as follows:

```
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. ",
    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 3-45.

Session-Timeout (27)

Description: Specifies the maximum number of seconds of service to be provided to the user before termination of the session or prompt.

Usage: Specify a number from 0 to 4,294,967,295. The default value is 0 (zero), which specifies that the MAX TNT does not enforce a time limit.

Dependencies: Session-Timeout is identical to the Ascend vendor attribute Ascend-Maximum-Time, whose use will be deprecated over time. Currently, if a user profile specifies both an RFC-defined attribute and an Ascend vendor attribute that performs a similar function, the last one sent by the server is used. However, using both attributes is not reliable and is not recommended.

See Also: "Ascend-MPP-Idle-Percent (254)" on page 3-58 and "Ascend-Preempt-Limit (245)" on page 3-62.

Tunnel-Client-Endpoint (66)

Description: Specifies a string assigned by RADIUS that specifies the name for the unit placing the call. This value is used by RADIUS accounting for tracking the session.

Dependencies: Consider the following:

- DNIS or CLID authentication must be enabled.
- The MAX TNT must have RADIUS user entries that specify DNIS or CLID.

See Also: "Client-Port-DNIS (30)" on page 3-82.

Tunnel-ID (68)

Description: Specifies a string assigned by RADIUS to each session using CLID or DNIS tunneling. This value is used for accounting when accounting.

Dependencies: Consider the following:

- DNIS or CLID must be enabled
- The MAX TNT must have RADIUS user entries that specify DNIS or CLID.

See Also: "Client-Port-DNIS (30)" on page 3-82.

Tunneling-Protocol (127)

Description: Specifies whether a session used the ATMP tunneling protocol.

Usage: The value is ATMP if the connection used 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 (65)

Description: Specifies the media to be used for the tunnel.

Usage: Only IP (1) is supported at this time.

Dependencies: Consider the following:

- DNIS or CLID must be enabled.
- The MAX TNT must have RADIUS user entries that specify DNIS or CLID.

See Also: “Tunnel-Server-Endpoint (67)” on page 3-96 and “Tunnel-Type (64)” on page 3-97.

Tunnel-Password (69)

Description: Specifies the password that the Foreign Agent sends to the Home Agent during Ascend Tunnel Management Protocol (ATMP) operation. The password must match the value of the Home Agent's ATMP-Home-Agent-Password parameter in the ATMP subprofile of the IP-Interface profile. All Mobile Clients accessing a single Home Agent must specify the same password.

Usage: Specify a text string of up to 20 characters. The default value is null.

Tunnel-Server-Endpoint (67)

Description: Specifies the IP address or hostname of the Ascend Tunnel Management Protocol (ATMP) primary Home Agent, L2TP Network Server (LNS) endpoint, PPTP Network Server (PNS) endpoint., or the destination that will decapsulate IP packets under IP-in-IP encapsulation.

Usage: Make your specification in the following format:

`Tunnel-Server-Endpoint="`*`hostname`*` | `*`ip_address`*` [:`*`udp_port`*`]"`

Table 3-20 lists each element of the syntax.

Table 3-20. Tunnel-Server-Endpoint syntax

Syntax element	Specifies
`hostname`	Symbolic hostname.
`ip_address`	IP address in dotted decimal notation. Specify an IP address if a DNS server is not set up. You can specify a host name or an IP address, but not both. The IP address should be the system address, not the IP address of the interface on which the unit receives tunneled data.
`udp_port`	UDP port on which the Foreign Agent communicates with the Home Agent. The default value is 5150.
`:` (colon)	Separator between the hostname (or IP address) and the UDP port.

Dependencies: Consider the following:

- If you specify the Ascend-Home-Agent-UDP-Port attribute on the line immediately following the Tunnel-Server-Endpoint attribute, you need not specify a value for *`udp_port`*.
- If you specify a value for the *`udp_port`* argument of Tunnel-Server-Endpoint, or if you accept the default of 5150, you need not specify the Ascend-Home-Agent-UDP-Port attribute.
- Use Tunnel-Server-Endpoint instead of the Ascend-Home-Agent-IP-Addr attribute.
- To specify a secondary Home Agent for use if the primary Home Agent is unavailable, enter a value for the Ascend-Secondary-Home-Agent attribute.

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, enter one of the following lines in a RADIUS user profile:

```
Tunnel-Server-Endpoint="max1.home.com:6001"
```

```
Tunnel-Server-Endpoint="10.0.0.1:6001"
```

See Also: "Ascend-Home-Agent-UDP-Port (186)" on page 3-45, "Ascend-Home-Network-Name (185)" on page 3-45, "Ascend-Secondary-Home-Agent (130)" on page 3-70, "Tunnel-Medium-Type (65)" on page 3-95, "Tunnel-Server-Endpoint (67)" on page 3-96, and "Tunnel-Type (64)" on page 3-97.

Tunnel-Type (64)

Description: Specifies the tunneling protocol to use.

Usage: Specify one of the following values:

- PPTP (1) specifies Point-to-Point Tunneling Protocol.
- L2TP (3) specifies Layer 2 Tunneling Protocol.
- ATMP (4) specifies Ascend Tunnel Management Protocol.
- IP-in-IP (7) specifies that IP packets are encapsulated in IP.

Example: The following the following user profile specifies CLID authentication for an L2TP tunnel to an L2TP Network Server (LNS) at 200.10.10.1:

```
5551000 Password="Ascend-CLID", User-Service=Dialout-Framed-User
   Tunnel-Type=L2TP,
   Tunnel-Medium-Type=IP
   Tunnel-Server-Endpoint=200.10.10.1
```

See Also: "Tunnel-Medium-Type (65)" on page 3-95 and "Tunnel-Server-Endpoint (67)" on page 3-96.

User-Name (1)

Description: Specifies one of the following:

- The name of the calling device or dial-in user
- The keyword Default
- The incoming phone number (for CLID authentication)
- The called-party number (for called-number authentication)
- The name of a pseudo-user profile

Usage: Specify an alphanumeric string of 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: Suppose you enter the following first line of a user profile for a user named Emma:

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

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.

To use CLID authentication with the incoming phone number as the User-Name, you could configure a user profile as follows:

```
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-Route-IP=Route-IP-Yes,
         Ascend-Idle-Limit=30
```

Finally, the following example shows how you would enter 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: Specifies the type of services the link can use.

Usage: Specify one of the following values:

- Login-User (1) specifies that the caller can use an asynchronous connection to log into the terminal server. The caller can start Telnet, Rlogin, or raw TCP sessions. The MAX TNT rejects incoming framed calls.
- Framed-User (2) specifies that incoming calls must use a framed protocol. If they do not, the MAX TNT rejects them.
- Dialout-Framed-User (5) specifies that the MAX TNT can use the profile only for outgoing calls.

By default, the MAX TNT does not limit the services the link can access.

Dependencies: Consider the following:

- When you specify the Login-User setting, the caller must have an asynchronous means of reaching the MAX TNT. The MAX TNT must have digital modems, or the call must be V.120 encapsulated.
- The User-Service attribute can appear in both an Access-Request and an Access-Accept packet. However, it does not appear in an Access-Request packet if Auth-Send67=No in the External-Auth profile's Rad-Auth-Client subprofile.

Vendor-Specific (26)

Description: Encapsulates attributes introduced by vendors. The purpose of the Vendor-Specific attribute is to enable companies to extend RADIUS operations without leading to possible attribute collisions (two attributes with the same type number but different meanings).

Usage: In Vendor-Specific Attribute (VSA) compatibility mode, the MAX TNT uses the Vendor-Specific attribute to encapsulate Ascend vendor attributes and uses the RFC-defined User-Password encryption algorithm. In the Old compatibility mode (the default), the MAX TNT does not send the Vendor-Specific attribute to the RADIUS server and does not recognize it if the server sends it. In this mode, the system uses the Ascend algorithm of encrypting and decrypting the User-Password attribute, which differs from the RFC-defined algorithm in that it does not null fill the password string to a multiple of 16 bytes before encryption, and it does not use the previous segment's hash to calculate the next intermediate value when the password is longer than 16 bytes.

See Also: For complete information about configuring the MAX TNT to use the Vendor-Specific attribute, see "Configuring Vendor-Specific Attribute (VSA) support" on page 2-9.

Setting Up RADIUS Accounting

4

Before you begin

Before you set up RADIUS accounting, you must install the most recent Ascend RADIUS daemon. Follow the instructions in “Installing the RADIUS daemon” on page 2-2.

Overview of accounting configuration tasks

When you set up the RADIUS server for accounting, you must specify certain system-wide settings, as explained in “Performing required accounting configuration tasks” on page 4-2. Other system-wide settings are optional, as described in “Performing optional accounting configuration tasks” on page 4-3. In addition, depending on your accounting needs, you can carry out the following tasks:

- Configure accounting in each RADIUS user profile. (For instructions, see “Setting up accounting on a per-user basis” on page 4-7.)
- Configure accounting with dynamic IP addressing. (For instructions, see “Setting up accounting with dynamic IP addressing” on page 4-10.)
- Gather information about user sessions. (For instructions, see “Classifying user sessions in RADIUS” on page 4-11.)
- Use the SNMP Set command to specify the primary accounting server. (For instructions, see “Using SNMP to specify the primary accounting server” on page 4-12.)

Finally, to start up the RADIUS accounting server, follow the instructions in “Starting the RADIUS daemon with accounting enabled” on page 4-13.

Setting up system-wide RADIUS accounting values

This section explains how to configure RADIUS accounting on a system-wide basis. Some steps are required. Others are optional.

Performing required accounting configuration tasks

When you set up RADIUS accounting, you must specify:

- System-wide accounting parameters
- Accounting port in `/etc/services`
- Accounting directory

Specifying system-wide accounting parameters on the MAX TNT

To set accounting parameters that affect all users on a system-wide basis, perform the following steps at the MAX TNT configuration interface:

1. In the External-Auth profile, set Acct-Type =RADIUS.
2. Open the Rad-Acct-Client subprofile.
3. For each Acct-Server parameter, specify the IP address of a RADIUS host.
4. For the Acct-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 Acct-Key parameter, enter the RADIUS client password, exactly as it appears in the RADIUS `clients` file.

Specifying the accounting port

Add to the `/etc/services` file a line identifying the RADIUS daemon's accounting port. Use the following format:

```
radacct   1646/udp   #radius-accounting
```

The port number you specify must match the port number indicated by the Acct-Port parameter in the External-Auth profile's Rad-Acct-Client subprofile.

Specifying the accounting 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 accounting information. The accounting 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 accounting records.

Performing optional accounting configuration tasks

In the External-Auth profile, you can specify that the RADIUS accounting daemon generate unique accounting IDs based on the source UDP port number of accounting packets. In addition, depending on the needs of your site, you have the option of specifying one or more values in the Rad-Acct-Client subprofile of the External-Auth profile:

- Source for RADIUS accounting requests
- Timeout value
- Retry limit
- Session-report interval
- Numeric base for the session ID
- Reset time

In addition, you can set parameters in the Rad-Acct-Client subprofile that control:

- Whether the MAX TNT sends Accounting Stop packets when a connection fails authentication
- Whether the MAX TNT send Accounting Stop packets that do not contain a user name

Finally, by setting the Auth-Frm-Adr-Start parameter in the Rad-Auth-Client subprofile, you can specify whether the MAX TNT generates a second Accounting start packet when the RADIUS Framed-Address value is assigned.

Generating RADIUS accounting IDs based on source port number

RADIUS uses ID values in Request-Response matching. For each unique accounting request (including retries, if a response is not received within the configured timeout period), RADIUS assigns an 8-bit ID value. The assigned value is freed when the request is no longer pending—that is, when RADIUS matches a request with a response, or the request times out.

When the MAX TNT runs at high capacity, RADIUS can run out of unique IDs. By default, when the server reaches its limit of 256 outstanding requests, no unique values are available for the next accounting request. To overcome this limitation, you can specify that each request be identified by the UDP source port as well as by the RADIUS ID value. To configure the MAX TNT to send the source UDP port number in RADIUS Request-Response matching, set Rad-ID-Source-Unique=Port-Unique in the External-Auth profile.

Specifying the source for RADIUS accounting requests

Set the Acct-Src-Port parameter to a value representing the MAX TNT unit's UDP source port for sending RADIUS accounting requests. You may specify the same value for authentication and accounting requests.

Specifying a timeout value

To specify the number of seconds the MAX TNT waits for a response to a RADIUS accounting request, set the Acct-Timeout parameter in the Rad-Acct-Client subprofile of the External-Auth profile. You can specify a value from 1 to 10. The default value is 1.

Specifying a retry limit

When the MAX TNT is configured for RADIUS accounting, it sends Accounting Start and Stop packets to the RADIUS server to record connections. If the server does not acknowledge a packet within the number of seconds you specify for the Acct-Timeout parameter, the MAX TNT tries again, resending the packet until the server responds, or dropping the packet because the queue is full. To set the maximum number of retries for Accounting packets, set the Acct-Limit-Retry parameter to a value greater than 0 (zero). A value of 0 (the default) indicates an unlimited number of retries.

The MAX TNT always attempts at least one retry. For example, if you set the number of retries to 10, the MAX TNT makes 11 attempts: the original attempt plus 10 retries.

Specifying the interval for sending session reports

The MAX TNT can report the number of sessions by class to a RADIUS accounting server. The Acct-Sess-Interval parameter specifies the interval, in seconds, at which the MAX TNT sends session reports. You can specify a number between 0 and 65535.The default value is 0 (zero), which specifies that the MAX TNT does not send reports on session events.

(For complete information about setting up the MAX TNT for session reports, see “Classifying user sessions in RADIUS” on page 4-11.)

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 Accounting packet. The Acct-Id-Base parameter controls whether the MAX TNT presents Acct-Session-ID to the accounting server in base 10 or base 16. You can specify one of the following settings:

- Acct-Base-10 (decimal) specifies that the numeric base is 10. The default value is 10.
- Acct-Base-16 (hexadecimal) specifies that the numeric base is 16.

For example, when you set Acct-Id-Base=Acct-Base-10, the MAX TNT presents a typical session ID to the accounting server in the following format:

```
"1234567890"
```

When you set Acct-Id-Base=Acct-Base-16, the MAX TNT 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 reset time

To specify the number of seconds that must elapse before the MAX TNT returns to using the primary RADIUS accounting server., set the Acct-Reset-Time parameter. The default is 0 (zero), which specifies that the MAX TNT does not return to using the primary RADIUS accounting server.

Specifying whether to send Stop packets when authentication fails

By default, RADIUS Accounting Stop packets are sent for authenticated connections, connections that are dropped before authenticating, and connections that fail authentication. To configure the MAX TNT not to send Stop packets for connections that fail authentication, set Acct-Drop-Stop-On-Auth-Fail=Yes in the External-Auth > Rad-Acct-Client subprofile.

Specifying whether to send Stop packets with no user name

At times, the MAX TNT can send an Accounting Stop packet to the RADIUS server without having sent an Accounting Start packet. Such Stop packets have no user name. To specify that the MAX TNT should not send an Accounting Stop packet that does not contain a user name, set Acct-Stop-Only=No in the Rad-Acct-Client subprofile of the External-Auth profile.

Specifying whether to send a second RADIUS Accounting Start record

To specify that the MAX TNT sends a second RADIUS Accounting Start record when the RADIUS Framed-Address value is assigned, set Auth-Frm-Adr-Start=Yes.

Example of setting up system-wide RADIUS accounting

The configuration illustrated in Figure 4-1 uses three RADIUS accounting servers. Clients dialing in across the WAN use both framed and unframed protocols on analog and digital lines. The RADIUS daemon for each server receives client requests on UDP port 512, and the client password is `tntpass`.

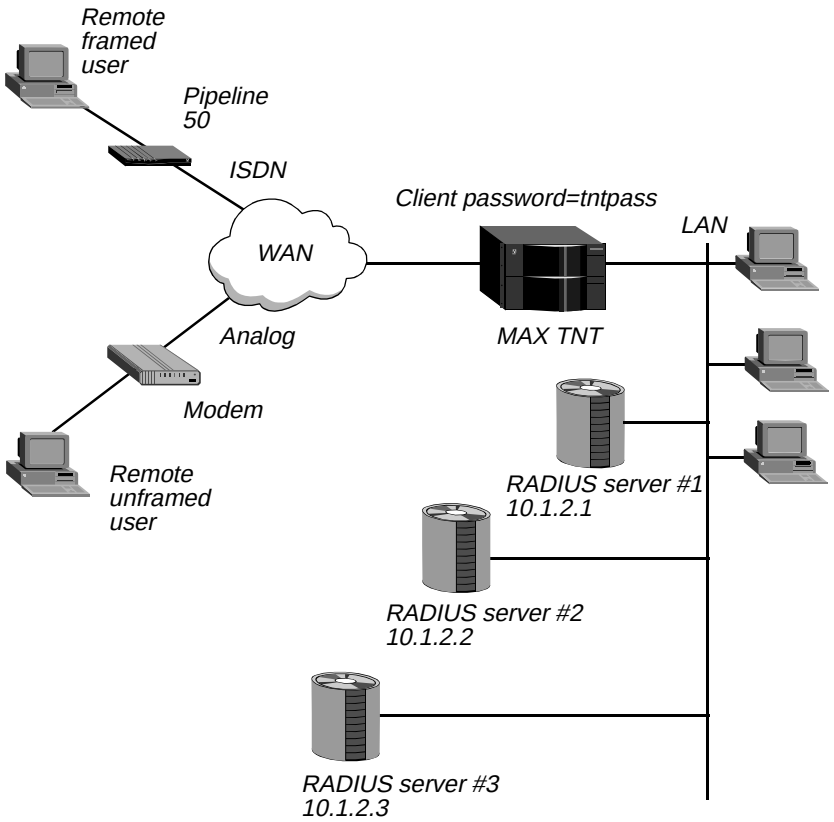

Figure 4-1. Sample network topology for setting up system-wide RADIUS accounting

In addition to the required parameters, the configuration also specifies that the MAX TNT must:

- Generate RADIUS accounting IDs based on source port number.
- Use UDP source port 500 for sending accounting requests.
- Increase the timeout value to 10 seconds.
- Increase the retry limit to 6.

To set the values for the sample configuration, you would proceed as follows:

```
admin> read external-auth
EXTERNAL-AUTH read

admin> set acct-type=radius

admin> set rad-id-source-unique=port-unique

admin> list rad-acct-client
[in EXTERNAL-AUTH:rad-acct-client (changed)]
acct-server-1=0.0.0.0
acct-server-2=0.0.0.0
acct-server-3=0.0.0.0
acct-port=0
acct-src-port=0
acct-key=""
acct-timeout=0
acct-sess-interval=0
acct-id-base=acct-base-10
acct-reset-time=0
acct-stop-only=yes
acct-limit-retry=0
acct-drop-stop-on-auth-fail=no

admin> set acct-server-1=10.1.2.1

admin> set acct-server-2=10.1.2.2

admin> set acct-server-3=10.1.2.3

admin> set acct-port=512

admin> set acct-src-port=500

admin> set acct-key=tntpass

admin> set acct-timeout=10

admin> set acct-limit-retry=6

admin> write external-auth
EXTERNAL-AUTH written
```

Setting up accounting on a per-user basis

A network reseller can serve many different ISPs, each with a different access policy. The reseller carries traffic for individual users, and must bill for usage according to the policies of the appropriate ISP. With per-user accounting, a network reseller can direct accounting information about specific users to a RADIUS server belonging to a particular ISP. Each RADIUS user profile can specify that accounting data goes to one or both of the following locations:

- The server specified by the Acct-Server parameter in the External-Auth profile's Rad-Acct-Client subprofile. This server is known as the *default server.*
- The RADIUS accounting server specified by the Ascend-User-Acct-Host attribute in the RADIUS user profile.

When an accounting event occurs, the MAX TNT sends an accounting message to the specified server. The MAX TNT places each accounting message on a list and waits for an acknowledgment from the RADIUS server. If an acknowledgment does not arrive within the time specified by the Acct-Timeout parameter, the MAX TNT resends the accounting message. RADIUS discards the oldest entry on the list when the total number of entries exceeds the maximum.

Overview of per-user accounting attributes

When you set up accounting on a per-user basis, you use the attributes described in Table 4-1.

Table 4-1. 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) Ascend-User-Acct-Base-10 is the default.
Ascend-User-Acct-Host (139)	Specifies the IP address of the RADIUS server to use for the 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 destination 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 with the `-A` argument when starting the daemon, the number of the UDP port for authentication services plus 1.

Table 4-1. Per-user accounting attributes (continued)

Attribute	Description	Possible values
Ascend-User-Acct-Time (143)	Specifies the number of seconds the MAX TNT waits for a response to a RADIUS accounting request. If the MAX TNT 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-Server parameter on the MAX TNT, to the server specified by the Ascend-User-Acct-Host attribute in RADIUS, or both.	Integer from 1 to 10. The default value is 1.
Ascend-User-Acct-Type (138)	Specifies the RADIUS accounting server to use for the connection.	Ascend-User-Acct-None (0) specifies that the MAX TNT sends accounting information to the default server specified in the External-Auth profile's Rad-Acct-Client subprofile. Ascend-User-Acct-User (1) specifies that the MAX TNT 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) specifies that the MAX TNT sends accounting information both to the RADIUS server specified by the Ascend-User-Acct-Host attribute, and to the default server. Ascend-User-Acct-None is the default.

Specifying per-user accounting attributes

To specify a RADIUS accounting server in a RADIUS user profile:

1. Set up the RADIUS user profile, as discussed in the preceding chapters.
2. Set the Ascend-User-Acct-Type attribute to specify the RADIUS accounting server for the connection.
3. Set the Ascend-User-Acct-Host attribute to the IP address of the RADIUS accounting server for the connection.
4. Set the Ascend-User-Acct-Port attribute to the UDP port number you specified for the authentication process in `/etc/services`. Or, if you used the `incr` keyword with the `-A` argument when starting the daemon, specify the sum of 1 plus the number of the UDP port for authentication services.
5. Set the Ascend-User-Acct-Key attribute to the value of the RADIUS client password, exactly as it appears in the RADIUS `clients` file.
6. Set the Ascend-User-Acct-Base attribute to specify whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16 (optional).
7. Set the Ascend-User-Acct-Time attribute to the number of seconds the MAX TNT waits for a response to a RADIUS accounting request (optional).

   If Ascend-User-Acct-Type is set to Ascend-User-Acct-User-Default, the MAX TNT sends two different packets: one to the server specified in the user profile, and one to the default server.

Example of setting up per-user accounting

In Figure 4-2, the MAX TNT sends accounting information to the RADIUS server at 200.250.56.10 for the user Emma. The destination UDP port is 1645, and the RADIUS client password is `mypassword`.

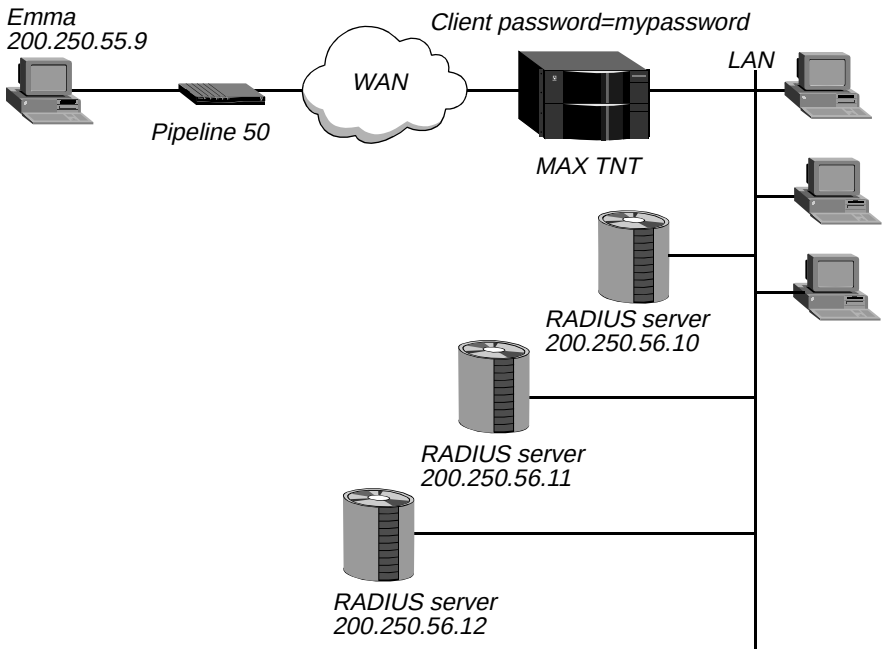

Figure 4-2. Sample network topology for setting up accounting on a per-user basis

To set up per-user accounting for the user Emma, you would configure her user profile as follows:

```
Emma Password="m2dan", User-Service=Framed-User
     Framed-Protocol=PPP,
     Framed-Address=200.250.55.9,
     Ascend-Link-Compression=Link-Comp-Stac,
     Framed-Compression=Van-Jacobson-TCP-IP,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Metric=2,
     Ascend-User-Acct-Type=Ascend-User-Acct-User,
     Ascend-User-Acct-Host=200.250.56.10,
     Ascend-User-Acct-Port=1645,
     Ascend-User-Acct-Key="mypassword"
```

Setting up accounting with dynamic IP addressing

In some networks, the RADIUS accounting 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, but not the caller's IP address. To track calls during the authentication period, you must set up one or more IP address pools as described in the *MAX TNT Network Guide*. Then, in the Rad-Auth-Client subprofile of the External-Auth profile, set Auth-Pool=Yes.

When Auth-Pool=Yes, the MAX TNT includes the caller's assigned IP address as the value of the Framed-Address attribute. The MAX TNT 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 TNT returns the IP address to pool #1. However, the address continues to appear in RADIUS accounting entries.
- If Assign-Address=No and the caller's RADIUS user profile supplies an IP address for the caller, the MAX TNT returns the IP address to pool #1. The IP address from the user profile appears in RADIUS accounting 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 accounting entries. The MAX TNT returns the address to the pool when the call disconnects.
- If Assign-Address=Yes and Must-Accept-Address-Assign=Yes on the MAX TNT, 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. The MAX TNT 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 RADIUS accounting entries. If the caller does specify an IP address, that address appears in RADIUS accounting entries.

Classifying user sessions in RADIUS

The Class and Ascend-Number-Sessions attributes enable access providers to classify their user sessions for purposes such as billing clients on the basis of the service option they choose. If you customize RADIUS properly, you can set up the MAX TNT to periodically issue accounting requests.

Using the Class attribute

If you include the Class attribute in the RADIUS user profile, the RADIUS server sends it to the MAX TNT in the Access-Accept packet when the session begins. Class then appears in Accounting-Request packets the MAX TNT sends to the RADIUS accounting server whenever a session starts and whenever a session stops. The accounting entries specify the class on a per-user and per-session basis.

Using the Ascend-Number-Sessions attribute

The Ascend-Number-Sessions attribute reports information about all user sessions (that is, on the number of current sessions of each class). The attribute has a compound value. The first part indicates 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.

Generating periodic accounting requests

On the MAX TNT, you can set the Acct-Sess-Interval parameter in the External-Auth profile's Rad-Acct-Client subprofile to send accounting requests at regular intervals. At the specified interval, the MAX TNT reports the number of open sessions by sending an Ascend-Access-Event-Request packet (code 33). The 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 to Ascend-Access-Event-Request packets from the MAX TNT. Other accounting daemons ignore it. When modifying the daemon, make sure that it recognizes an Ascend-Access-Event-Request packet in the following 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 of classifying user sessions

Suppose that the MAX TNT 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 that the MAX TNT sends to the RADIUS accounting server has three Ascend-Number-Session attributes, one for each of the class/session pairs.

Using SNMP to specify the primary accounting server

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

Every time you reset the server with the Set command, the MAX TNT generates an SNMP trap. The MAX TNT 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 specifies the Object ID and IP address for the new server. The Object ID for the accounting server is 1.3.6.1.4.1.529.13.4.1.6.*x*, where *x* is the index of the current server (1-3).

The following MIB objects support changing the current RADIUS accounting server:

```
radAcctHostIPAddress OBJECT-TYPE
   SYNTAX  IpAddress
   ACCESS  read-only
   STATUS  mandatory
   DESCRIPTION "The IP address of the Accounting server. The
           value 0.0.0.0 is returned if entry is invalid."
   ::= { radiusAcctStatsEntry 6 }
radAcctCurrentServerFlag OBJECT-TYPE
   SYNTAX      INTEGER {
                  invalid(1),
                  current(2)
               }
   ACCESS      read-write
   STATUS      mandatory
   DESCRIPTION "Value indicates whether this entry is the
                current accounting server or not. Writing any
                value will cause the current server to be reset
                to the primary server (Host #1)."
   ::= { radiusAcctStatsEntry 7 }
```

Starting the RADIUS daemon with accounting enabled

To enable accounting, start the RADIUS daemon with the `-A` argument.

When using a flat ASCII file

If you are using a flat ASCII file, enter the following command line:

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

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

If 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 if you do not specify the `-A` argument.

When using a UNIX DBM database

To start the RADIUS daemon when using a UNIX DBM database, enter the following command line:

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

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

Understanding accounting records

This section describes:

- What kind of information appears in accounting records
- Where accounting records are stored
- What kinds of packets RADIUS accounting uses
- Which attributes appear in each type of packet

What type of information appears in accounting records?

RADIUS accounting records information about WAN sessions only. Specifically, RADIUS logs information about three types of events:

- Start session. Denotes the beginning of a session with the MAX TNT. Information about this event appears in an accounting Start record.
- Stop session. Denotes the end of a session with the MAX TNT. Information about this event appears in an accounting Stop record.
- Failure-to-start session. Denotes that a login attempt has failed. Information about this event appears in an accounting Failure-to-start record.

When the MAX TNT 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 TNT transmitted and received, the protocol in use, the user name and IP address of the client, and so on. All counters are session based, and reset to 0 (zero) when the session starts. At the end of the session, the interfaces are reported as Down and show 0 (zero).

You can use RADIUS accounting to:

- Gather billing information, including who called, how long the session lasted, and how much traffic occurred during the session.
- Troubleshoot RADIUS and MAX TNT operations. Accounting records can contain information about how many login failures occurred, and can describe the characteristics of the failed attempts.

Where are accounting records stored?

The RADIUS accounting server writes each record to a log file. If you run an unmodified Ascend RADIUS daemon, the Ascend RADIUS accounting file and the Livingston RADIUS accounting file have the same name:

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

where *`host`* is the RADIUS client. Because the client of the RADIUS accounting server is your MAX TNT, *`host`* is your MAX TNT unit's symbolic host name, or its IP address in dotted decimal notation.

What kinds of packets does RADIUS accounting use?

RADIUS accounting uses two kinds of packets: Accounting Start and Accounting Stop.

Accounting Start packets

Accounting Start packets signal a Start session event. When the MAX TNT begins a terminal-server or routing session, and the call passes authentication or the user logs in, the MAX TNT sends an Accounting Start packet to the RADIUS accounting server. The packet describes the type of session in use and the name of the user opening the session.

The MAX TNT 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 TNT sends an Accounting Start packet after login. Information from an Accounting Start packet appears in a Start record in the log file.

Accounting Stop packets

Accounting Stop packets signal a Stop session or Failure-to-start session event. By default, the MAX TNT always sends an Accounting Stop packet at the end of a session, including cases in which a user fails authentication. Information from an Accounting Stop packet appears in a Stop record or Failure-to-start record in the log file.

Non-accounting attributes in Start and Stop records

An Accounting Start record or Stop record can contain attributes that are not accounting specific. Table 4-2 lists them. Of the attributes listed in Table 4-2, only the NAS-Identifier attribute can appear in a Failure-to-start record as well.

Table 4-2. Non-accounting attributes in Start and Stop records

Attribute	Description
Ascend-Dial-Number (227)	Indicates the phone number of the device that originated the connection.
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)—Stop records, Gateway mode only	Indicates the name of the Connection profile through which the Home Agent sends all packets it receives from the Mobile Client during ATMP operation.
Caller-Id (31)	Indicates the calling-party number, which is the phone number of the user that has connected to the unit.
Class (25)	Enables access providers to classify their user sessions. The default value for the Class attribute is null.
Client-Port-DNIS (30)	Indicates the called-party number, which is the phone number the user dials to connect to the MAX TNT.
Framed-Address (8)	Indicates the IP address of the user starting the session. The default value is 0.0.0.0.
Framed-Protocol (7)	Indicates the kind of protocol the connection uses.
NAS-Identifier (4)	Indicates the IP address of the MAX TNT. This attribute does not appear in an Accounting-Stop packet for a Failure-start-session event.
NAS-Port (5)	Indicates the port on which the MAX TNT received the call. NAS-Port 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 established session: NAS_Port_Type_Async (0) indicates a call the MAX TNT routes to a digital modem. NAS_Port_Type_Sync (1) indicates a synchronous ISDN connection.
User-Name (1)	Indicates the name of the user starting the session.

Accounting attributes in Start records

Table 4-3 lists the accounting-specific attributes that can appear in a Start record.

Table 4-3. Accounting-specific attributes in Start records

Attribute	Description
Acct-Authentic (45)	Indicates the method the MAX TNT used to authenticate an incoming call: RADIUS (1) indicates that RADIUS authenticated the incoming call. Local (2) indicates that the MAX TNT used a local Connection profile, TACACS profile, or TACACS+ profile, or that the MAX TNT accepted the call without authentication.
Acct-Delay-Time (41)	Indicates the number of seconds the MAX TNT 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 routing or terminal-server session reported in the Accounting packet. The string is a random number. RADIUS correlates the Accounting Start packet and Accounting Stop packet with Acct-Session-Id. Its value can range from 1 to 2,137,383,647.
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.
Ascend-Modem-PortNo (120)	Specifies the number of the port on the specified slot that terminates the call.
Ascend-Modem-ShelfNo (122)	Specifies the number of the shelf that terminates the call.
Ascend-Modem-SlotNo (121)	Specifies the number of the slot on the specified shelf that terminates the call.
Ascend-Redirect-Number (93)	Indicates the redirected number extracted from the Redirect Number Information Element (IE) in an ISDN frame.
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)	Indicates whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16.
Ascend-User-Acct-Host (139)	Indicates the IP address of the RADIUS server to use for the link.

Table 4-3. Accounting-specific attributes in Start records (continued)

Attribute	Description
Ascend-User-Acct-Key (141)	Indicates the RADIUS client password as it appears in the `clients` file.
Ascend-User-Acct-Port (140)	Indicates a destination UDP port number for the connection.
Ascend-User-Acct-Time (143)	Indicates the number of seconds the MAX TNT waits for a response to a RADIUS accounting request.
Ascend-User-Acct-Type (138)	Indicates the RADIUS accounting server(s) to use for the connection.

Accounting attributes in Stop records

Table 4-4 lists the accounting attributes that can appear in a Stop record.

Table 4-4. Accounting-specific attributes in Stop records

Attribute	Description	Conditions for inclusion
Acct-Authentic (45)	Indicates the method the MAX TNT used to authenticate an incoming call: RADIUS (1) indicates that RADIUS authenticated the incoming call. Local (2) indicates that the MAX TNT used a local Connection profile, TACACS profile, or TACACS+ profile, or that the MAX TNT accepted the call without authentication.	Session must be authenticated.
Acct-Delay-Time (41)	Indicates the number of seconds between the time an event occurred and the time the MAX TNT sent the packet. If RADIUS does not acknowledge the packet, the MAX TNT resends it. The value of Acct-Delay-Time changes to reflect the proper event time.	None.
Acct-Input-Octets (42)	Indicates the number of octets the MAX TNT received during the session. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.	Session must be authenticated. An asynchronous connection must be in use. That is, the data must be unframed.

Table 4-4. Accounting-specific attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
Acct-Input-Packets (47)	Indicates the number of packets the MAX TNT received during the session. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.	Session must be authenticated. A framed protocol must be in use.
Acct-Output-Octets (43)	Indicates the number of octets the MAX TNT sent during the session. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.	Session must be authenticated. An asynchronous connection must be in use. That is, the data must be unframed.
Acct-Output-Packets (48)	Indicates the number of packets the MAX TNT sent during the session. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.	Session must be authenticated. A framed protocol must be in use.
Acct-Session-Id (44)	Consists of a unique numeric string identified with the routing or terminal-server session reported in the Accounting packet. The string is a random number of up to seven digits. RADIUS correlates the Accounting Start packet and Accounting Stop packet with Acct-Session-Id. Its value can range from 1 to 2,137,383,647.	None.
Acct-Session-Time (46)	Indicates the number of seconds the session has been logged in.	Session must be authenticated.
Acct-Status-Type (40)	Requests that have Acct-Status-Type set to Start are Accounting Start packets. The information in these packets appears in Start records. Requests that have Acct-Status-Type set to Stop are Accounting Stop packets. The information in these packets appears in Stop or Failure-to-start records.	None.
Ascend-Connect-Progress (196)	Indicates the state of the connection before it disconnects.	None.

Table 4-4. Accounting-specific attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
Ascend-Data-Rate (197)	Indicates the rate of data received on the connection in bits per second.	None.
Ascend-Disconnect-Cause (195)	Indicates the reason a connection was taken offline.	None.
Ascend-Event-Type (150)	Indicates a cold-start notification, informing the accounting server that the MAX TNT has started up.	For a cold-start notification, the MAX TNT sends values for NAS-Identifier and Ascend-Event-Type in an Ascend-Access-Event-Request packet (code 33). The RADIUS accounting server must send back an Ascend-Access-Event-Response packet (code 34), with the correct identifier, to the MAX TNT.
Ascend-First-Dest (189)	Records the destination IP address of the first packet the MAX TNT received on a connection after authentication.	Session must be authenticated.
Ascend-Home-Agent-IP-Addr (183)	Indicates the IP address of the Home Agent associated with the Mobile Client.	Session has ended. Accounting-Request packet includes Acct-Status-Type=Stop. Session was authenticated and encapsulated by means of Ascend Tunnel Management Protocol (ATMP).
Ascend-Modem-PortNo (120)	Specifies the number of the port on the specified slot that terminates the call.	None.
Ascend-Modem-ShelfNo (122)	Specifies the number of the shelf that terminates the call.	None.
Ascend-Modem-SlotNo (121)	Specifies the number of the slot on the specified shelf that terminates the call.	None.
Ascend-Multilink-ID (187)	Reports the ID number of the Multilink bundle when the session closes.	Session must be authenticated.
Ascend-Num-In-Multilink (188)	Records the number of sessions remaining in a Multilink bundle when the session closes.	Session must be authenticated.

Table 4-4. Accounting-specific attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
Ascend-Number-Sessions (202)	Indicates 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 TNT sends the Ascend-Number-Sessions attribute in Ascend-Access-Event-Request packets. Only RADIUS daemons you customize to recognize packet code 33 respond to these request packets.
Ascend-Pre-Input-Octets (190)	Reports the number of octets the MAX TNT received before authentication. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.	Session must be authenticated. An asynchronous connection must be in use. That is, the data must be unframed.
Ascend-Pre-Input-Packets (192)	Reports the number of packets the MAX TNT received before authentication. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.	Session must be authenticated.
Ascend-Pre-Output-Octets (191)	Reports the number of octets the MAX TNT sent before authentication. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.	Session must be authenticated. An asynchronous connection must be in use. That is, the data must be unframed.
Ascend-Pre-Output-Packets (193)	Reports the number of packets the MAX TNT sent before authentication. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.	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.	None.
Ascend-Redirect-Number (93)	Indicates the redirected number extracted from the Redirect Number Information Element (IE) in an ISDN frame.	None.

Table 4-4. Accounting-specific attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
Ascend-User-Acct-Base (142)	Indicates whether the numeric base of the RADIUS Acct-Session-ID attribute is 10 or 16.	None.
Ascend-User-Acct-Host (139)	Indicates the IP address of the RADIUS server to use for the connection.	None.
Ascend-User-Acct-Key (141)	Indicates the RADIUS client password as it appears in the `clients` file.	None.
Ascend-User-Acct-Port (140)	Indicates a destination UDP port number for the connection.	None.
Ascend-User-Acct-Time (143)	Indicates the number of seconds the MAX TNT waits for a response to a RADIUS accounting request.	None.
Ascend-User-Acct-Type (138)	Indicates the RADIUS accounting server(s) to use for the connection.	None.
Ascend-Xmit-Rate (255)	Indicates the rate of data transmitted on the connection in bits per second. For ISDN calls, Ascend-Xmit-Rate indicates the transmit data rate. For analog calls, it indicates the modem baud rate at the time of the initial connection.	None.
Tunnel-Client-Endpoint (66)	Specifies a string assigned by RADIUS that specifies the name for the unit placing the call.	None.
Tunnel-ID (68)	Specifies a string assigned by RADIUS to each session using CLID or DNIS tunneling.	None.
Tunneling-Protocol (127)	Specifies whether a session used the ATMP tunneling protocol.	None.

Accounting 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)

For a brief description of each of these attributes, see Table 4-4 on page 4-17.

Proxy RADIUS accounting

The master shelf controller keeps track of all accounting Start records sent by host cards. If the shelf controller determines that a host card has gone down for any reason, it acts as proxy for the card and sends the accounting server a fail-safe Stop record for each of the card's open sessions. The host card may be brought down administratively, may be removed from the system, or may go down due to an error condition.

How proxy RADIUS accounting works

When RADIUS accounting is in use, the usual situation occurs as shown in Figure 4-3.

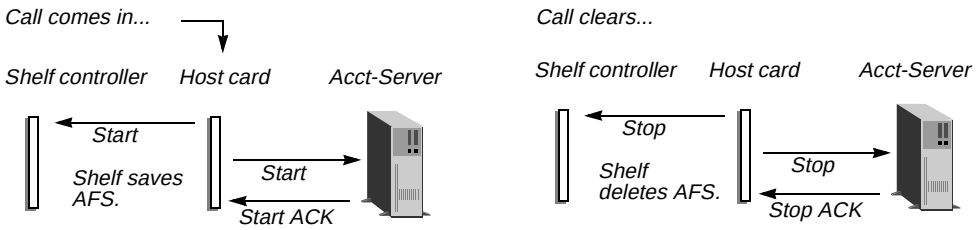

Figure 4-3. Normal RADIUS accounting (no proxy necessary)

When a call comes in, the host card first sends a Start record to the shelf controller, which stores it as an Accounting Fail-Safe (AFS) record. The host card then sends one or more Start records to the RADIUS accounting server, repeating until it receives an ACK from the server. Similarly, when the call clears, the host card sends a Stop record to the shelf controller, which causes it to delete the AFS record for that session. The host card then sends the accounting server Stop records until it receives an ACK from the server.

When RADIUS accounting is in use and the host card goes down for any reason, proxy accounting occurs as shown in Figure 4-4.

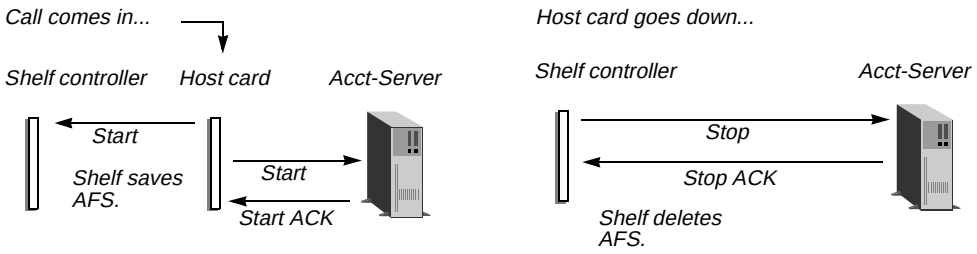

Figure 4-4. Proxy accounting (host card goes down)

In this case, when the shelf controller notes that the host card is down, it uses its own information about the host card and the stored AFS record to send a Stop record directly to the RADIUS accounting server, repeating until it receives a Stop ACK from the server. The shelf controller then deletes the AFS record for that session.

Note that if the accounting server is accessible only by means of the host card that goes down, Stop records cannot be delivered successfully.

Contents of the Stop record sent by proxy

The AFS Stop record does not contain all the information that appears in a record sent by a host card. In particular, it does not contain the input/output octet count fields or any other dynamic information related to the session. In Table 4-5, Yes indicates that the attribute is included in the Stop record, if applicable. No indicates that the attribute either is not included in the record or is set to null, as appropriate.

Table 4-5. Accounting attributes included in proxy Stop records

Attribute in regular Stop record	In proxy Stop record
Acct-Authentic	Yes
Acct-Delay-Time	Yes
Acct-Input-Octets	No
Acct-Input-Packets	No
Acct-Output-Octets	No
Acct-Output-Packets	No
Acct-Session-Id	Yes
Acct-Status-Type	Yes
Acct-Session-Time	Yes. (The session time is accurate to within a few seconds.)
Ascend-Connect-Progress	Yes

Table 4-5. Accounting attributes included in proxy Stop records (continued)

Attribute in regular Stop record	In proxy Stop record
Ascend-Data-Rate	Yes
Ascend-Disconnect-Cause	Yes. (The Disconnect reason is always 210, slot card down.)
Ascend-First-Dest	No
Ascend-Home-Agent-IP-Addr	Yes
Ascend-Home-Agent-UDP-Port	Yes
Ascend-Multilink-ID	Yes
Ascend-Num-In-Multilink	Yes
Ascend-Pre-Input-Octets	No
Ascend-Pre-Input-Packets	No
Ascend-Pre-Output-Octets	No
Ascend-Pre-Output-Packets	No
Ascend-PreSession-Time	Yes
Caller-Id	No
Class	Yes
Framed-Address	Yes
Framed-Protocol	Yes
Login-Host	Yes
Login-Service	Yes
Login-TCP-Port	Yes
NAS-Identifier	Yes
NAS-Port	Yes
NAS-Port-Type	Yes
Tunneling-Protocol	Yes
User-Name	Yes

Sample accounting records

This section provides sample Start and Stop records for the following configurations:

- A Pipeline 25 dialing into a MAX TNT
- A modem calling into a MAX TNT

The section also illustrates a Stop record sent by proxy.

A Pipeline 25 dialing into a MAX TNT

When a Pipeline 25 dials into a MAX TNT, 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 TNT */
   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 TNT */
   NAS-Port=1057 /* Call on channel 2, line 2, slot 2, shelf 1 */
   Acct-Status-Type=Stop /* Stop record */
   Acct-Delay-Time=18 /* MAX TNT 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=31200 /* Receive data rate in bits per second */
   Ascend-Xmit-Rate=48000 /* Transmit data rate in bits per seconds */
   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 TNT

If a modem dials into the MAX TNT 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 TNT */
   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 TNT */
   NAS-Port=1057 /* Call on channel 2, line 2, slot 2, shelf 1 */
   Acct-Status-Type=Stop /* Stop record */
   Acct-Delay-Time=18 /* MAX TNT 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=31200 /* Receive data rate in bits per second */
   Ascend-Xmit-Rate=48000 /* Transmit data rate in bits per seconds */
   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 */
```

An immediate-modem dialout connection

An accounting start/stop pair is generated whenever an immediate-modem dialout connection is initiated or dropped. The accounting start/stop records generated by a call include the Caller-ID attribute to indicate the called number, as shown in the following sample records:

```
Fri May 1 11:08:04 1998
   User-Name="kevtest"
   NAS-Identifier=10.11.21.30
   NAS-Port=0
   NAS-Port-Type=Sync
   Acct-Status-Type=Start
   Acct-Delay-Time=0
   Acct-Session-Id="262862705"
   Acct-Authentic=Local
   Caller-Id="8005"

Fri May  1 11:08:33 1998
   User-Name="kevtest"
   NAS-Identifier=10.11.21.30
   NAS-Port=0
   NAS-Port-Type=Sync
   Acct-Status-Type=Stop
   Acct-Delay-Time=0
   Acct-Session-Id="262862705"
   Acct-Authentic=Local
   Acct-Session-Time=29
   Acct-Input-Octets=103
   Acct-Output-Octets=20
   Acct-Input-Packets=0
   Acct-Output-Packets=0
   Ascend-Disconnect-Cause=1
   Ascend-Connect-Progress=50
   Ascend-Xmit-Rate=0
   Ascend-Data-Rate=0
   Ascend-PreSession-Time=14
   Ascend-Pre-Input-Octets=0
   Ascend-Pre-Output-Octets=0
   Ascend-Pre-Input-Packets=0
   Ascend-Pre-Output-Packets=0
   Ascend-Modem-PortNo=1
   Ascend-Modem-SlotNo=8
   Caller-Id="8005"
```

A Stop record sent by proxy

Following is an example of a shelf controller accounting proxy for an HDLC call:

```
Wed Nov 5 14:50:21 1997
    User-Name="joel-mhp"
    NAS-Identifier=200.65.212.199
    NAS-Port=2272
    NAS-Port-Type=Sync
    Acct-Status-Type=Stop
    Acct-Delay-Time=0
    Acct-Session-Id="246212864"
    Acct-Authentic=RADIUS
    Acct-Session-Time=4
    Acct-Input-Octets=0
    Acct-Output-Octets=0
    Acct-Input-Packets=0
    Acct-Output-Packets=0
    Ascend-Disconnect-Cause=210
    Ascend-Connect-Progress=67
    Ascend-Data-Rate=0
    Ascend-PreSession-Time=0
    Ascend-Pre-Input-Octets=174
    Ascend-Pre-Output-Octets=204
    Ascend-Pre-Input-Packets=7 /
    Ascend-Pre-Output-Packets=8
    Framed-Protocol=PPP
    Framed-Address=200.168.6.66
```

Setting Up Call Logging

5

Before you begin

Before you set up call logging, you must install the most recent Ascend RADIUS daemon. Follow the instructions in “Installing the RADIUS daemon” on page 2-2.

Understanding call logging

Call logging enables you to keep records for resource management or troubleshooting. When you set up call logging, you can create duplicate accounting information for sites that wish to keep accounting records separate from call-logging records. Call logging is based on RADIUS accounting.

The MAX TNT sends Start session, Stop session, a nd Failure-to-start session packets to a call-log host. The call-log information is sent independently of RADIUS accounting records. If both call logging and RADIUS accounting are in use, the information is sent in parallel.

Note: Call logging should only be used with NavisAccess.

Overview of call-logging configuration tasks

When you set up call logging, you must specify certain system-wide settings, as explained in "Performing required call-logging configuration tasks" on page 5-2. Other system-wide settings are optional, as described in "Performing optional call-logging configuration tasks" on page 5-3. In addition, depending on your needs, you can configure call logging with dynamic IP addressing. (For instructions, see "Setting up call logging with dynamic IP addressing" on page 5-6.) Finally, to start up the call-log host, follow the instructions in "Starting the RADIUS daemon with call logging enabled" on page 5-7.

Setting up system-wide call-logging values

This section explains how to configure call logging on a system-wide basis. Some steps are required. Others are optional.

Performing required call-logging 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 TNT

To set call-logging parameters that affect all users on a system-wide basis, perform the following steps at the MAX TNT configuration interface:

1. In the External-Auth profile, set Acct-Type =RADIUS.
2. Open the Call-Logging profile.
3. Set Call-Log-Enable=Yes.
4. For each Call-Log-Host parameter, specify the IP address of a call-log host.
5. For the Call-Log-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.
6. For the Call-Log-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 Call-Log-Port parameter in the Call-Logging profile.

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

Depending on the needs of your site, you have the option of specifying one or more of the following values in the Call-Logging profile:

- Timeout value
- Retry limit
- Numeric base for the session ID
- Number of seconds that must elapse before the MAX TNT returns to using the primary call-log host

In addition, you can specify whether the MAX TNT sends call-logging Stop packets that do not contain a user name.

Specifying a timeout value

To specify the number of seconds the MAX TNT waits for a response to a call-logging request, set the Call-Log-Timeout parameter in the Call-Logging profile. You can specify a value from 1 to 10. The default value is 1.

Specifying a retry limit

When the MAX TNT is configured for call logging, it sends call-logging Start and Stop packets to the call-log host to record connections. If the host does not acknowledge a packet within the number of seconds you specify for the Call-Log-Timeout parameter, the MAX TNT tries again, resending the packet until the host responds, or dropping the packet because the queue is full. To set the maximum number of retries for call-logging packets, set the Call-Log-Limit-Retry parameter to a value greater than 0 (zero). A value of 0 (the default) indicates an unlimited number of retries.

The MAX TNT always attempts at least one retry. For example, if you set the number of retries to 10, the MAX TNT makes 11 attempts: the original attempt plus 10 retries.

Specifying the numeric base for the session ID

The Acct-Session-ID attribute is a unique numeric string identified with the session reported in a call-logging packet. The Call-Log-Id-Base parameter controls whether the MAX TNT presents Acct-Session-ID to the call-log host in base 10 or base 16. You can specify one of the following settings:

- Acct-Base-10 (decimal) specifies that the numeric base is 10. The default value is 10.
- Acct-Base-16 (hexadecimal) specifies that the numeric base is 16.

For example, when you set Call-Log-Id-Base=Acct-Base-10, the MAX TNT presents a typical session ID to the call-log host in the format `"1234567890"`. When you set Call-Log-Id-Base=Acct-Base-16, the MAX TNT presents the same session ID in the format `"499602D2"`.

Note: Changing the value of Call-Log-Id-Base while sessions are active creates inconsistencies between the Start and Stop records.

Specifying the reset time

To specify the number of seconds that must elapse before the MAX TNT returns to using the primary call-log host, set the Call-Log-Reset-Time parameter. The default is 0 (zero), which specifies that the MAX TNT does not return to using the primary call-log host.

Specifying whether to send Stop packets with no user name

At times, the MAX TNT can send a call-logging Stop packet to the call-log host without having sent a call-logging Start packet. Such Stop packets have no user name. To specify that the MAX TNT should not send a call-logging Stop packet that does not contain a user name, set Call-Log-Stop-Only=No.

Example of setting up system-wide call logging

The configuration illustrated in Figure 5-1 uses three call-log hosts. Clients dialing in across the WAN use both framed and unframed protocols on analog and digital lines. The RADIUS daemon for each host receives client requests on UDP port 512, and the client password is `tntpass`.

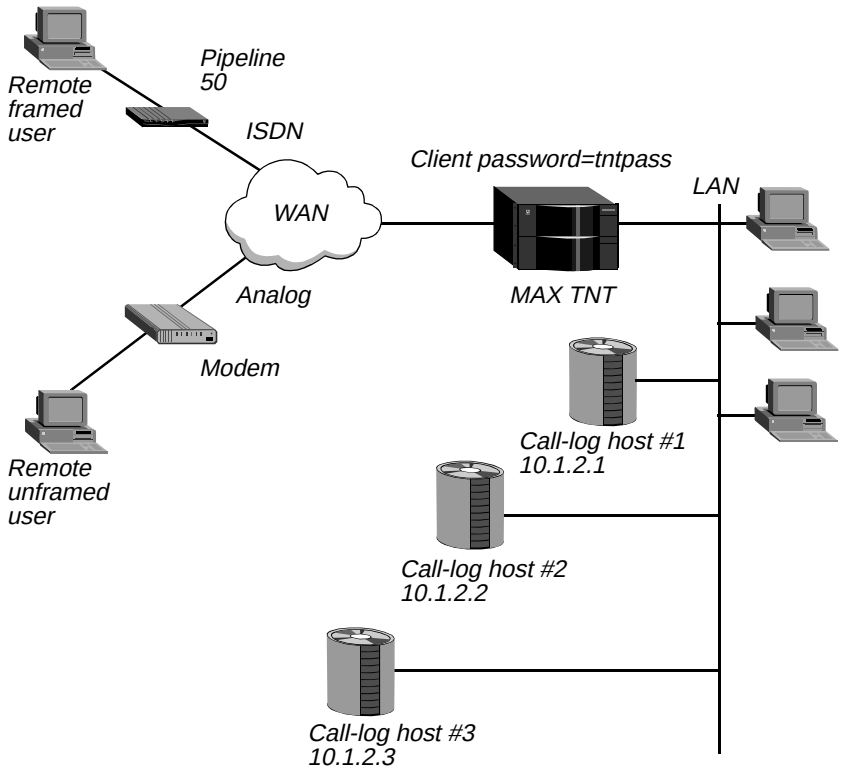

Figure 5-1. Sample network topology for setting up system-wide call logging

In addition to the required parameters, the configuration also specifies that the MAX TNT must:

- Increase the timeout value to 10 seconds.
- Increase the retry limit to 6.

To set the values for the sample configuration, you would proceed as follows:

```
admin> read external-auth
EXTERNAL-AUTH read

admin> set acct-type=radius

admin> write external-auth
EXTERNAL-AUTH written

admin> read call-logging
CALL-LOGGING read

admin> list
[in CALL-LOGGING]
call-log-enable=no
call-log-host-1=0.0.0.0
call-log-host-2=0.0.0.0
call-log-host-3=0.0.0.0
call-log-port=0
call-log-key=""
call-log-timeout=0
call-log-id-base=acct-base-10
call-log-reset-time=0
call-log-stop-only=yes
call-log-limit-retry=0

admin> set call-log-enable=yes

admin> set call-log-host-1=10.1.2.1

admin> set call-log-host-2=10.1.2.2

admin> set call-log-host-3=10.1.2.3

admin> set call-log-port=512

admin> set call-log-key=tntpass

admin> set call-log-timeout=10

admin> set call-log-limit-retry=6

admin> write call-logging
CALL-LOGGING read
```

Setting up call logging with dynamic IP addressing

In some networks, the call-log host 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, but not the caller's IP address. To track calls during the authentication period, you must set up one or more IP address pools as described in the *MAX TNT Network Guide*. Then, in the Rad-Auth-Client subprofile of the External-Auth profile, set Auth-Pool=Yes.

When Auth-Pool=Yes, the MAX TNT includes the caller's assigned IP address as the value of the Framed-Address attribute. The MAX TNT 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 TNT 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 TNT 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 TNT returns the address to the pool when the call disconnects.
- If Assign-Address=Yes and Must-Accept-Address-Assign=Yes on the MAX TNT, 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 TNT 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.

Starting the RADIUS daemon with call logging enabled

To enable call logging, start the RADIUS daemon with the `-A` argument.

When using a flat ASCII file

If you are using a flat ASCII file, enter the following 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.

When using a UNIX DBM database

To start the RADIUS daemon when using a UNIX DBM database, enter the following command line:

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

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

Understanding call-logging records

This section describes:

- What kind of information appears in call-logging records
- Where call-logging records are stored
- What kinds of packets call-logging uses
- Which attributes appear in each type of packet

What type of information appears in call-logging records?

Call-logging records information about WAN sessions only. Specifically, the call-log host logs information about three types of events:

- Start session. Denotes the beginning of a session with the MAX TNT. Information about this event appears in a call-logging Start record.
- Stop session. Denotes the end of a session with the MAX TNT. 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 TNT recognizes one of these events, it sends a call-logging request to the call-log host. When the call-log host 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 TNT transmitted and received, the protocol in use, the user name and IP address of the client, and so on. All counters are session based, and reset to 0 (zero) when the session starts. At the end of the session, the interfaces are reported as Down and show 0 (zero).

You can use call logging to:

- Gather billing information, including who called, how long the session lasted, and how much traffic occurred during the session.
- Troubleshoot RADIUS and MAX TNT operations. Call-logging records can contain information about how many login failures occurred, and can describe the characteristics of the failed attempts.

Where are call-logging records stored?

The call-log host writes each record to the following log file:

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

where *`host`* is the call-logging client. Because the client of the call-log host is your MAX TNT, *`host`* is your MAX TNT unit's symbolic host name, or its IP address in dotted decimal notation.

What kinds of packets does call logging use?

Call logging uses two kinds of packets: Start and Stop.

Start packets

Start packets signal a Start session event. When the MAX TNT begins a terminal-server or routing session, and the call passes authentication or the user logs in, the MAX TNT sends a Start packet to the call-log host. The packet describes the type of session in use and the name of the user opening the session.

The MAX TNT does not send a 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 TNT sends a Start packet after login. Information from a Start packet appears in a Start record in the log file.

Stop packets

Stop packets signal a Stop session or Failure-to-start session event. By default, the MAX TNT always sends a Stop packet at the end of a session, including cases in which a user fails authentication. Information from a Stop packet appears in a Stop record or Failure-to-start record in the log file.

Non-call-logging attributes in Start and Stop records

A Start record or Stop record can contain attributes that are not call-logging specific. Table 5-1 lists them. Of the attributes listed in Table 5-1, only the NAS-Identifier attribute can appear in a Failure-to-start record as well.

Table 5-1. Non-call-logging attributes in Start and Stop records

Attribute	Description
Ascend-Dial-Number (227)	Indicates the phone number of the device that originated the connection.
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)—Stop records, Gateway mode only	Indicates the name of the Connection profile through which the Home Agent sends all packets it receives from the Mobile Client during ATMP operation.
Caller-Id (31)	Indicates the calling-party number, which is the phone number of the user that has connected to the unit.
Class (25)	Enables access providers to classify their user sessions. The default value for the Class attribute is null.
Client-Port-DNIS (30)	Indicates the called-party number, which is the phone number the user dials to connect to the MAX TNT.
Framed-Address (8)	Indicates the IP address of the user starting the session. The default value is 0.0.0.0.
Framed-Protocol (7)	Indicates the kind of protocol the connection uses. By default, the MAX TNT does not restrict the type of protocol a user can access.
NAS-Identifier (4)	Indicates the IP address of the MAX TNT. This attribute does not appear in a Stop packet for a Failure-start-session event.
NAS-Port (5)	Indicates the port on which the MAX TNT received the call. NAS-Port does not appear in a Stop packet for a Failure-start-session event.
NAS-Port-Type (61)	Specifies the type of service in use for the established session: NAS_Port_Type_Async (0) indicates a call the MAX TNT routes to a digital modem. NAS_Port_Type_Sync (1) indicates a synchronous ISDN connection.
User-Name (1)	Indicates the name of the user starting the session.

Call-logging attributes in Start records

Table 5-2 lists the call-logging-specific attributes that can appear in a Start record.

Table 5-2. Call-logging-specific attributes in Start records

Attribute	Description
Acct-Authentic (45)	Indicates the method the MAX TNT used to authenticate an incoming call: RADIUS (1) indicates that RADIUS authenticated the incoming call. Local (2) indicates that the MAX TNT used a local Connection profile, TACACS profile, or TACACS+ profile, or that the MAX TNT accepted the call without authentication.
Acct-Delay-Time (41)	Indicates the number of seconds the MAX TNT has been trying to send the packet. In a Start packet, this value is 0 (zero).
Acct-Session-Id (44)	Consists of a unique numeric string identified with the routing or terminal-server session reported in the packet. The string is a random number. The call-log host correlates the Start packet and Stop packet with Acct-Session-Id. Its value can range from 1 to 2,137,383,647.
Acct-Status-Type (40)	Requests that have Acct-Status-Type=Start are Start packets. The information in these packets appears in Start records. Requests that have Acct-Status-Type=Stop are Stop packets. The information in these packets appears in Stop or Failure-to-start records.
Ascend-Session-Svr-Key (151)	Identifies the user session in which a client sends a disconnect or filter-change request to the call-log host.

Call-logging attributes in Stop records

Table 5-3 lists the call-logging attributes that can appear in a Stop record.

Table 5-3. Call-logging-specific attributes in Stop records

Attribute	Description	Conditions for inclusion
Acct-Authentic (45)	Indicates the method the MAX TNT used to authenticate an incoming call: RADIUS (1) indicates that RADIUS authenticated the incoming call. Local (2) indicates that the MAX TNT used a local Connection profile, TACACS profile, or TACACS+ profile, or that the MAX TNT accepted the call without authentication.	Session must be authenticated.
Acct-Delay-Time (41)	Indicates the number of seconds between the time an event occurred and the time the MAX TNT sent the packet. If the call-log host does not acknowledge the packet, the MAX TNT resends it. The value of Acct-Delay-Time changes to reflect the proper event time.	None.
Acct-Input-Octets (42)	Indicates the number of octets the MAX TNT received during the session. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.	Session must be authenticated. An asynchronous connection must be in use. That is, the data must be unframed.
Acct-Input-Packets (47)	Indicates the number of packets the MAX TNT received during the session. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.	Session must be authenticated. A framed protocol must be in use.
Acct-Output-Octets (43)	Indicates the number of octets the MAX TNT sent during the session. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.	Session must be authenticated. An asynchronous connection must be in use. That is, the data must be unframed.

Table 5-3. Call-logging-specific attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
Acct-Output-Packets (48)	Indicates the number of packets the MAX TNT sent during the session. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.	Session must be authenticated. A framed protocol must be in use.
Acct-Session-Id (44)	Consists of a unique numeric string identified with the routing or terminal-server session reported in the packet. The string is a random number of up to seven digits. The call-log host correlates the Start packet and Stop packet with Acct-Session-Id. Its value can range from 1 to 2,137,383,647.	None.
Acct-Session-Time (46)	Indicates the number of seconds the session has been logged in.	Session must be authenticated.
Acct-Status-Type (40)	Requests that have Acct-Status-Type set to Start are Start packets. The information in these packets appears in Start records. Requests that have Acct-Status-Type set to Stop are Stop packets. The information in these packets appears in Stop or Failure-to-start records.	None.
Ascend-Connect-Progress (196)	Indicates the state of the connection before it disconnects.	None.
Ascend-Data-Rate (197)	Indicates the rate of data received on the connection in bits per second.	None.
Ascend-Disconnect-Cause (195)	Indicates the reason a connection was taken offline.	None.
Ascend-Event-Type (150)	Indicates a cold-start notification, informing the call-log host that the MAX TNT has started up.	For a cold-start notification, the MAX TNT sends values for NAS-Identifier and Ascend-Event-Type in an Ascend-Access-Event-Request packet (code 33). The call-log host must send back an Ascend-Access-Event-Response packet (code 34), with the correct identifier, to the MAX TNT.

Table 5-3. Call-logging-specific attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
Ascend-First-Dest (189)	Records the destination IP address of the first packet the MAX TNT received on a connection after authentication.	Session must be authenticated.
Ascend-Home-Agent-IP-Addr (183)	Indicates the IP address of the Home Agent associated with the Mobile Client.	Session has ended. Session was authenticated and encapsulated by means of Ascend Tunnel Management Protocol (ATMP).
Ascend-Multilink-ID (187)	Reports the ID number of the Multilink bundle when the session closes.	Session must be authenticated.
Ascend-Num-In-Multilink (188)	Records the number of sessions remaining in a Multilink bundle when the session closes.	Session must be authenticated.
Ascend-Number-Sessions (202)	Indicates 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 TNT sends the Ascend-Number-Sessions attribute in Ascend-Access-Event-Request packets. Only RADIUS daemons you customize to recognize packet code 33 respond to these request packets.
Ascend-Pre-Input-Octets (190)	Reports the number of octets the MAX TNT received before authentication. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.	Session must be authenticated. An asynchronous connection must be in use. That is, the data must be unframed.
Ascend-Pre-Input-Packets (192)	Reports the number of packets the MAX TNT received before authentication. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.	Session must be authenticated.
Ascend-Pre-Output-Octets (191)	Reports the number of octets the MAX TNT sent before authentication. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.	Session must be authenticated. An asynchronous connection must be in use. That is, the data must be unframed.

Table 5-3. Call-logging-specific attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
Ascend-Pre-Output-Packets (193)	Reports the number of packets the MAX TNT sent before authentication. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.	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.	None.
Ascend-Xmit-Rate (255)	Indicates the rate of data transmitted on the connection in bits per second. For ISDN calls, Ascend-Xmit-Rate indicates the transmit data rate. For analog calls, it indicates the modem baud rate at the time of the initial 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)

For a brief description of each of these attributes, see Table 5-3 on page 5-11.

Sample call-logging records

This section provides sample Start and Stop records for the following configurations:

- A Pipeline 25 dialing into a MAX TNT
- A modem calling into a MAX TNT

A Pipeline 25 dialing into a MAX TNT

When a Pipeline 25 dials into a MAX TNT, 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 TNT */
   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 TNT */
   NAS-Port=1057 /* Call on channel 2, line 2, slot 2, shelf 1 */
   Acct-Status-Type=Stop /* Stop record */
   Acct-Delay-Time=18 /* MAX TNT 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=31200 /* Receive data rate in bits per second */
   Ascend-Xmit-Rate=48000 /* Transmit data rate in bits per seconds */
   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 TNT

If a modem dials into the MAX TNT 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 TNT */
   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 TNT */
   NAS-Port=1057 /* Call on channel 2, line 2, slot 2, shelf 1 */
   Acct-Status-Type=Stop /* Stop record */
   Acct-Delay-Time=18 /* MAX TNT 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=31200 /* Receive data rate in bits per second */
   Ascend-Xmit-Rate=48000 /* Transmit data rate in bits per seconds */
   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 */
```

Attribute and Parameter Cross Reference

A

The following tables cross reference RADIUS attributes and MAX TNT parameters.

Parameters and analogous attributes

Table A-1 cross references the Ascend RADIUS dictionary's attributes to parameters in the MAX TNT unit's menu-driven user interface. The table is arranged by parameter in alphabetical order.

Table A-1. Parameters and analogous attributes

Profile > Subprofile	**Parameter**	**Analogous attribute**
Answer-Defaults	Force-56Kbps	Ascend-Force-56
	Framed-Only	User-Service
Answer-Defaults > IP-Answer	VJ-Header-Prediction	Framed-Compression
Answer-Defaults > MP-Answer	Maximum-Channels	Ascend-Maximum-Channels
	Minimum-Channels	Ascend-Minimum-Channels
Answer-Defaults > MPP-Answer	Add-Persistence	Ascend-Add-Seconds
	Bandwidth-Monitor-Direction	Ascend-DBA-Monitor
	Decrement-Channel-Count	Ascend-Dec-Channel-Count
	Dynamic-Algorithm	Ascend-History-Weigh-Type
	Increment-Channel-Count	Ascend-Inc-Channel-Count
	Seconds-History	Ascend-Seconds-Of-History
	Sub-Persistence	Ascend-Remove-Seconds

Table A-1. Parameters and analogous attributes (continued)

Profile > Subprofile	Parameter	Analogous attribute
	Target-Utilization	Ascend-Target-Util
Answer-Defaults > PPP-Answer	Link-Compression	Ascend-Link-Compression
	MRU	Framed-MTU
Answer-Defaults >Session-Info	Idle-Timer	Ascend-Idle-Limit
	Max-Call-Duration	Ascend-Maximum-Call-Duration
	TS-Idle-Mode	Ascend-TS-Idle-Mode
	TS-Idle-Timer	Ascend-TS-Idle-Limit
Connection	CalledNumber	Client-Port-DNIS
	Called-Number-Type	Ascend-PRI-Number-Type
	CLID	Caller-Id
	Dial-Number	Ascend-Dial-Number
	Encapsulation-Protocol	Framed-Protocol
	Encapsulation-Protocol=TCP-Raw	Login-Service=TCP-Clear
	Framed-Only	User-Service
	Shared-Prof	Ascend-Shared-Profile-Enable
	Station	User-Name
	VRouter	Ascend-VRouter-Name
Connection > AppleTalk-Options	Atalk-Routing-Enabled	Ascend-Route-Appletalk
Connection> FR-Options	Circuit-Name	Ascend-FR-Circuit-Name
	DLCI	Ascend-FR-DLCI
	Frame-Relay-Profile	Ascend-FR-Profile-Name
	FR-Direct-DLCI	Ascend-FR-Direct-DLCI
	FR-Direct-Enabled	Ascend-FR-Direct
	FR-Direct-Profile	Ascend-FR-Direct-Profile
Connection > IP-Options	Address-Pool	Ascend-Assign-IP-Pool
	Client-Default-Gateway	Ascend-Client-Gateway

Table A-1. Parameters and analogous attributes (continued)

Profile > Subprofile	Parameter	Analogous attribute
	Client-DNS-Addr-Assign	Ascend-Client-Assign-DNS
	Client-DNS-Primary-Addr	Ascend-Client-Primary-DNS
	Client-DNS-Secondary-Addr	Ascend-Client-Secondary-DNS
	IF-Remote-Address	Ascend-Remote-Addr
	IP-Direct	Ascend-IP-Direct
	IP-Routing-Enabled	Ascend-Route-IP
	Local-Address	Ascend-PPP-Address
	Multicast-Allowed	Ascend-Multicast-Client
	Multicast-Group-Leave-Delay	Ascend-Multicast-GLeave-Delay
	Multicast-Rate-Limit	Ascend-Multicast-Rate-Limit
	Remote-Address	Framed-Address
	RIP	Framed-Routing
	Source-IP-Check	Ascend-Source-IP-Check
	VJ-Header-Prediction	Framed-Compression
Connection > IP-Options > TOS-Options	Active	None
	Apply-To	Ascend-IP-TOS-Apply-To
	Precedence	Ascend-IP-TOS-Precedence
	Type-of-Service	Ascend-IP-TOS
Connection> IPX-Options	IPX-Routing-Enabled	Ascend-Route-IPX
	Peer-Mode	Ascend-IPX-Peer-Mode
	RIP	Framed-Routing
Connection > MP-Options	Base-Channel-Count	Ascend-Base-Channel-Count
	Maximum-Channels	Ascend-Maximum-Channels
	Minimum-Channels	Ascend-Minimum-Channels
Connection > MPP-Options	Add-Persistence	Ascend-Add-Seconds
	Bandwidth-Monitor-Direction	Ascend-DBA-Monitor

Table A-1. Parameters and analogous attributes (continued)

Profile > Subprofile	Parameter	Analogous attribute
	Decrement-Channel-Count	Ascend-Dec-Channel-Count
	Dynamic-Algorithm	Ascend-History-Weigh-Type
	Increment-Channel-Count	Ascend-Inc-Channel-Count
	Seconds-History	Ascend-Seconds-Of-History
	Sub-Persistence	Ascend-Remove-Seconds
	Target-Utilization	Ascend-Target-Util
Connection > PPP-Options	Link-Compression	Ascend-Link-Compression
	MRU	Framed-MTU
	Recv-Password	Password Ascend-Receive-Secret
	Send-Auth-Mode	Ascend-Send-Auth
	Send-Password	Ascend-Send-Passwd Ascend-Send-Secret
Connection > Session-Options	Backup	Ascend-Backup
	Idle-Timer	Ascend-Idle-Limit
	Max-Call-Duration	Ascend-Maximum-Call-Duration
	RX-Data-Rate-Limit	Ascend-Dsl-CIR-Recv-Limit
	Ses-ADSL-CAP-Down-Rate	Ascend-DSL-Downstream-Limit
	Ses-ADSL-CAP-Up-Rate	Ascend-DSL-Upstream-Limit
	Ses-Rate-Mode	Ascend-Dsl-Rate-Mode
	Ses-Rate-Type	Ascend-Dsl-Rate-Type
	TS-Idle-Mode	Ascend-TS-Idle-Mode
	TS-Idle-Timer	Ascend-TS-Idle-Limit
	TX-Data-Rate-Limit	Ascend-Dsl-CIR-Xmit-Limit
Connection> TCP-Clear-Options	Host	Login-Host
	Port	Login-TCP-Port
Connection > Telco-Options	Billing-Number	Ascend-Billing-Number

Table A-1. Parameters and analogous attributes (continued)

Profile > Subprofile	Parameter	Analogous attribute
	Callback	Ascend-Callback
	Call-By-Call	Ascend-Call-By-Call
	Call-Type	Ascend-Call-Type
	Data-Service	Ascend-Data-Svc
	Delay-Callback	Ascend-Callback-Delay
	Dialout-Allowed	Ascend-Dialout-Allowed
	Expect-Callback	Ascend-Expect-Callback
	Force-56Kbps	Ascend-Force-56
	FT1-Caller	Ascend-FT1-Caller
	Nailed-Groups	Ascend-Group
	Transit-Number	Ascend-Transit-Number
Connection > Tunnel-Options	Password	Tunnel-Password
	Home-Network-Name	Ascend-Home-Network-Name
	Primary-Tunnel-Server	Tunnel-Server-Endpoint
	Secondary-Tunnel-Server	Ascend-Secondary-Home-Agent
	Tunneling-Protocol	Tunnel-Type
	UDP-Port	Ascend-Home-Agent-UDP-Port
Connection > UsrRad-Options	Acct-Host	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
	Acct-Type	Ascend-User-Acct-Type
External-Auth	Acct-Type	Ascend-User-Acct-Type
External-Auth > Rad-Acct-Client	Acct-Id-Base	Ascend-User-Acct-Base
	Acct-Key	Ascend-User-Acct-Key

Table A-1. Parameters and analogous attributes (continued)

Profile > Subprofile	Parameter	Analogous attribute
	Acct-Port	Ascend-User-Acct-Port
	Acct-Server-1 Acct-Server-2 Acct-Server-3	Ascend-User-Acct-Host
	Acct-Timeout	Ascend-User-Acct-Time
External-Auth> Rad-Auth-Client	Auth-Rsp-Required	Ascend-Require-Auth
Filter> Input-Filters/Output-Filters> Gen-Filter	Filter parameters	Ascend-Call-Filter Ascend-Data-Filter
Filter> Input-Filters/Output-Filters> IP-Filter	Filter parameters	Ascend-Call-Filter Ascend-Data-Filter
Filter> Input-Filters/Output-Filters> TOS-Filter	Filter parameters	Ascend-Filter
Frame-Relay	Billing-Number	Ascend-Billing-Number
	Called-Number-Type	Ascend-PRI-Number-Type
	Call-By-Call-ID	Ascend-Call-By-Call
	DCEN392-Val	Ascend-FR-DCE-N392
	DCEN393-Val	Ascend-FR-DCE-N393
	Link-Mgmt	Ascend-FR-Link-Mgt
	Link-Mgmt-DLCI	Ascend-FR-Link-Status-DLCI
	Link-Type	Ascend-FR-Type
	MRU	Framed-MTU
	N391-Val	Ascend-FR-N391
	N392-Val	Ascend-FR-DTE-N392
	N393-Val	Ascend-FR-DTE-N393
	Nailed-Up-Group	Ascend-FR-Nailed-Grp
	T391-Val	Ascend-FR-T391
	T392-Val	Ascend-FR-T392
	Transit-Number	Ascend-Transit-Number
IP-Global	Static-Pref	Ascend-Route-Preference

Table A-1. Parameters and analogous attributes (continued)

Profile > Subprofile	Parameter	Analogous attribute
IP-Interface	IP-Address	NAS-Identifier
	Multicast-Allowed	Ascend-Multicast-Client
	Multicast-Rate-Limit	Ascend-Multicast-Rate-Limit
IP-Route	IP-Route parameters	Framed-Route
	Metric	Ascend-Metric
IPX-Route	IPX-Route parameters	Ascend-IPX-Route
T1 > Line-Interface > Channel-Config	Nailed-Group	Ascend-Group
Terminal Server > Immediate-Mode-Options	Host	Login-Host
	Port	Login-TCP-Port
	Service	Login-Service
Terminal Server > Menu-Mode-Options	Host-*n* (*n*=1-4) Text-*n* (*n*=1-4)	Ascend-Host-Info
Terminal-Server > Terminal-Mode-Configuration	Banner	Reply-Message
	Rlogin	Login-Service=Rlogin
	TCP	Login-Service=TCP-Clear
Terminal-Server> Terminal-Mode-Configuration> Telnet-Options	Telnet	Login-Service=Telnet

Attributes and parameters in numerical order

Table A-2 cross references the Ascend RADIUS dictionary's attributes to parameters in MAX TNT unit's menu-driven user interface. The table is arranged by attribute in numerical order.

Table A-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-Password
3	Challenge-Response	Text string	None
4	NAS-Identifier	IP address	IP-Address
5	NAS-Port	Zero-based, bit encoded number	None
6	User-Service	Login-User (1) Framed-User (2) Dialout-Framed-User (5) (3, 4, and 6 are not supported)	Framed-Only
7	Framed-Protocol	PPP (1) SLIP (2) ARA (255) MPP (256) FR (261) FR-CIR (263) ATM-1483 (264) ATM-FR-CIR (265)	Encapsulation-Protocol
8	Framed-Address	IP address	Remote-Address
9	Framed-Netmask	IP address	Netmask-Remote
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	Text string	None
12	Framed-MTU	Integer	MRU

Table A-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
13	Framed-Compression	Van-Jacobson-TCP-IP (1) (No other values supported)	VJ-Header-Prediction
14	Login-Host	IP address	Host
15	Login-Service	Telnet (0) Rlogin (1) TCP-Clear (2)	Service
16	Login-TCP-Port	Integer	Port
17	Change-Password	Text string	None
18	Reply-Message	Text string	Banner (terminal-server users only)
21	Ascend-PW-Expiration	Date	None
22	Framed-Route	*host_ipaddr* */subnet_mask* *router_ ipaddr* *metric* *private* *profile_name*	Dest-Address Gateway-Address Metric Private-Route Name
25	Class	Text string	None
26	Vendor-Specific	Text string	None
27	Session-Timeout	Integer	None
28	Idle-Timeout	Integer	None
30	Client-Port-DNIS	Text string	CalledNumber
31	Caller-Id	Text string	CLID
40	Acct-Status-Type	Start (1) Stop (2)	None
41	Acct-Delay-Time	Integer	None
42	Acct-Input-Octets	Integer	None
43	Acct-Output-Octets	Integer	None
44	Acct-Session-Id	Text string	None
45	Acct-Authentic	RADIUS (1) Local (2)	None

Table A-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
46	Acct-Session-Time	Integer	None
47	Acct-Input-Packets	Integer	None
48	Acct-Output-Packets	Integer	None
61	NAS-Port-Type	NAS_Port_Type_Async (0) NAS_Port_Type_Sync (1)	None
64	Tunnel-Type	PPTP (1), L2TP (3), ATMP (4)	Tunneling-Protocol
65	Tunnel-Medium-Type	IP (1)	None
66	Tunnel-Client-Endpoint	Text string	None
67	Tunnel-Server-Endpoint	IP address or hostname	Primary-Tunnel-Server
68	Tunnel-ID	Text string	None
69	Tunnel-Password	Text string	Password
88	Ascend-IP-TOS	Ascend-IP-TOS IP-TOS-Normal (0) Ascend-IP-TOS IP-TOS-Disabled (1) Ascend-IP-TOS IP-TOS-Cost (2) Ascend-IP-TOS IP-TOS-Reliability (4) Ascend-IP-TOS-IP-TOS-Throughput (8) Ascend-IP-TOS IP-TOS-Latency (16)	Type-of-Service
89	Ascend-IP-TOS-Precedence	IP-TOS-Precedence-Pri-Normal (0) IP-TOS-Precedence-Pri-One (32) IP-TOS-Precedence-Pri-Two (64) IP-TOS-Precedence-Pri-Three (96) IP-TOS-Precedence-Pri-Four (128) IP-TOS-Precedence-Pri-Five (160) IP-TOS-Precedence-Pri-Six (192) IP-TOS-Precedence-Pri-Seven (224)	Precedence
90	Ascend-IP-TOS-Apply-To	IP-TOS-Apply-To-Incoming (1024) IP-TOS-Apply-To-Outgoing (2048) IP-TOS-Apply-To-Both (3072)	Apply-To

Table A-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
91	Ascend-Filter	*dir* dstip *dest_ipaddr\subnet_mask* srcip *src_ipaddr\subnet_mask* *proto* dstport *cmp value* srcport *cmp value* precedence *value* type-of-service *value*	None Dest-Address Dest-Address-Mask Source-Address Source-Address-Mask Protocol Dst-Port-Cmp Dest-Port Src-Port-Cmp Source-Port Precedence Type-of-Service
92	Ascend-Dsl-Rate-Type	Rate-Type-Disabled Rate-Type-AdslCap Rate-Type-Sdsl Rate-Type-AdslDmt	Ses-Rate-Type
93	Ascend-Redirect-Number	Text string	None
94	Ascend-ATM-Vpi	Integer	None
95	Ascend-ATM-Vci	Integer	None
96	Ascend-Source-IP-Check	Source-IP-Check-No (0) Source-IP-C heck-Yes (1)	Source-IP-Check
97	Ascend-Dsl-Rate-Mode	Rate-Mode-AutoBaud Rate-Mode-Single	Ses-Rate-Mode
98	Ascend-DSL-Upstream-Limit	sdsl-144000 (0) sdsl-272000 (1) sdsl-400000 (2) sdsl-528000 (3) sdsl-784000 (4) sdsl-1168000 (5) sdsl-1552000 (6) sdsl-2320000 (7)	Ses-ADSL-CAP-Up-Rate

Table A-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
99	Ascend-DSL-Downstream-Limit	adslcap-dn-7168000 (0) adslcap-dn-6272000 (1) adslcap-dn-5120000 (2) adslcap-dn-4480000 (3) adslcap-dn-3200000 (4) adslcap-dn-2688000 (5) adslcap-dn-2560000 (6) adslcap-dn-2240000 (7) adslcap-dn-1920000 (8) adslcap-dn-1600000 (9) adslcap-dn-1280000 (10) adslcap-dn-960000 (11) adslcap-dn-640000 (12)	Ses-ADSL-CAP-Down-Rate
100	Ascend-Dsl-CIR-Recv-Limit	Integer	RX-Data-Rate-Limit
101	Ascend-Dsl-CIR-Xmit-Limit	Integer	TX-Data-Rate-Limit
102	Ascend-VRouter-Name	Text string	VRouter
103	Ascend-Source-Auth	IP address and billing code	None
104	Ascend-Private-Route	Destination IP address and next-hop router IP address.	Private-Route
106	Ascend-FR-Link-Status-DLCI	Integer	Link-Mgmt-DLCI
108	Ascend-Callback-Delay	Integer	Delay-Callback
111	Ascend-Multicast-GLeave-Delay	Integer	Multicast-Group-Leave-Delay
118	Ascend-Route-Appletalk	Route-Appletalk-No (0) Route-Appletalk-Yes (1)	Atalk-Routing-Enabled
120	Ascend-Modem-PortNo	Integer	None
121	Ascend-Modem-SlotNo	Integer	None
122	Ascend-Modem-ShelfNo	Integer	None
125	Ascend-Maximum-Call-Duration	Integer	Max-Call-Duration
126	Ascend-Route Preference	Integer	Static-Pref
127	Tunneling-Protocol	Integer	None

Table A-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
128	Ascend-Shared-Profile-Enable	Shared-Profile-No (0) Shared-Profile-Yes (1)	Shared-Prof
130	Ascend-Secondary-Home-Agent	IP address or hostname	Secondary-Tunnel-Server
131	Ascend-Dialout-Allowed	Dialout-Not-Allowed (0) Dialout-Allowed (1)	Dialout-Allowed
132	Ascend-Client-Gateway	IP address	Client-Default-Gateway
133	Ascend-BACP-Enable	BACP-No (0) BACP-Yes (1)	None
135	Ascend-Client-Primary-DNS	IP address	Client-DNS-Primary-Addr
136	Ascend-Client-Secondary-DNS	IP address	Client-DNS-Secondary-Addr
137	Ascend-Client-Assign-DNS	DNS-Assign-No (0) DNS-Assign-Yes (1)	Client-DNS-Addr-Assign
138	Ascend-User-Acct-Type	Ascend-User-Acct-None (0) Ascend-User-Acct-User (1) Ascend-User-Acct-User-Default (2)	Acct-Type
139	Ascend-User-Acct-Host	IP address	Acct-Host Acct-Server-*n*
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	None
145	Ascend-Assign-IP-Server	IP address	None
146	Ascend-Assign-IP-Global-Pool	Text string	None
149	Ascend-Expect-Callback	Expect-Callback-No (0) Expect-Callback-Yes (1)	Expect-Callback

Table A-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
150	Ascend-Event-Type	Ascend-Coldstart (1) Ascend-Session-Event (2)	None
151	Ascend-Session-Svr-Key	Text string	None
152	Ascend-Multicast-Rate-Limit	Integer	Multicast-Rate-Limit
153	Ascend-IF-Netmask	IP address	None
154	Ascend-Remote-Addr	IP address	IF-Remote-Address
155	Ascend-Multicast-Client	Multicast-No (0) Multicast-Yes (1)	Multicast-Allowed
156	Ascend-FR-Circuit-Name	Text string	Circuit-Name
158	Ascend-FR-Nailed-Grp	Integer	Nailed-Up-Group
159	Ascend-FR-Type	Ascend-FR-DTE (0) Ascend-FR-DCE (1) Ascend-FR-NNI (2)	Link-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-Val
162	Ascend-FR-DCE-N392	Integer	DCEN392-Val
163	Ascend-FR-DTE-N392	Integer	N392-Val
164	Ascend-FR-DCE-N393	Integer	DCEN393-Val
165	Ascend-FR-DTE-N393	Integer	N393-Val
166	Ascend-FR-T391	Integer	T391-Val
167	Ascend-FR-T392	Integer	T392-Val
169	Ascend-TS-Idle-Limit	Integer	TS-Idle-Timer
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)	Bandwidth-Monitor-Direction

Table A-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
172	Ascend-Base-Channel-Count	Integer	Base-Channel-Count
173	Ascend-Minimum-Channels	Integer	Minimum-Channels
174	Ascend-IPX-Route	*profile_name* *network#* *node#* *socket#* *server_type* *hop_count* *tick_count* *name*	Profile-Name Dest-Network Server-Node Server-Socket Server-Type Hops Ticks 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	Nailed-Group Nailed-Groups
179	Ascend-FR-DLCI	Integer from 16 to 991	DLCI
180	Ascend-FR-Profile-Name	Text string	Frame-Relay-Profile
181	Ascend-ARA-PW	Text string	None
183	Ascend-Home-Agent-IP-Addr	IP address	None
185	Ascend-Home-Network-Name	Text string	Home-Network-Name
186	Ascend-Home-Agent-UDP-Port	Integer	UDP-Port
187	Ascend-Multilink-ID	Integer	None
188	Ascend-Num-In-Multilink	Integer	None
189	Ascend-First-Dest	IP address	None
190	Ascend-Pre-Input-Octets	Integer	None
191	Ascend-Pre-Output-Octets	Integer	None

Table A-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
192	Ascend-Pre-Input-Packets	Integer	None
193	Ascend-Pre-Output-Packets	Integer	None
194	Ascend-Maximum-Time	Integer	None
195	Ascend-Disconnect-Cause	Integer	None
196	Ascend-Connect-Progress	Integer	None
197	Ascend-Data-Rate	Integer	None
198	Ascend-PreSession-Time	Integer	None
199	Ascend-Token-Idle	Integer	None
200	Ascend-Token-Immediate	Tok-Imm-No (0) Tok-Imm-Yes (1)	None
201	Ascend-Require-Auth	Not-Require-Auth (0) Require-Auth (1)	Auth-Rsp-Required
202	Ascend-Number-Sessions	Text string	None
203	Ascend-Authen-Alias	Text string	None
204	Ascend-Token-Expiry	Integer	None
205	Ascend-Menu-Selector	Text string	None
206	Ascend-Menu-Item	Text string	None
207	Ascend-PW-Warntime	Integer	None
208	Ascend-PW-Lifetime	Integer	None
209	Ascend-IP-Direct	IP address	IP-Direct
210	Ascend-PPP-VJ-Slot-Comp	VJ-Slot-Comp-No (1)	None
211	Ascend-PPP-VJ-1172	PPP-VJ-1172 (1)	None
212	Ascend-PPP-Async-Map	Integer	None
213	Ascend-Third-Prompt	Text string	Third-Login-Prompt
214	Ascend-Send-Secret	Text string	Send-Password
215	Ascend-Receive-Secret	Text string	Recv-Password

Table A-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
216	Ascend-IPX-Peer-Mode	IPX-Peer-Router (0) IPX-Peer-Dialin (1)	Peer-Mode
217	Ascend-IP-Pool-Definition	Text string	Pool-Base-Address Assign-Count
218	Ascend-Assign-IP-Pool	Integer	Address-Pool
219	Ascend-FR-Direct	FR-Direct-No (0) FR-Direct-Yes (1)	FR-Direct-Enabled
220	Ascend-FR-Direct-Profile	Text string	FR-Direct-Profile
221	Ascend-FR-Direct-DLCI	Integer	FR-Direct-DLCI
224	Ascend-IPX-Alias	Text string	None
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)	Called-Number-Type
227	Ascend-Dial-Number	Text string	Dial-Number
228	Ascend-Route-IP	Route-IP-No (0) Route-IP-Yes (1)	IP-Routing-Enabled
229	Ascend-Route-IPX	Route-IPX-No (0) Route-IPX-Yes (1)	IPX-Routing-Enabled
231	Ascend-Send-Auth	Send-Auth-None (0) Send-Auth-PAP (1) Send-Auth-CHAP (2)	Send-Auth-Mode
232	Ascend-Send-Passwd	Text string	Send-Password
233	Ascend-Link-Compression	Link-Comp-None (0) Link-Comp-Stac (1) Link-Comp-Stac-Draft-9 (2) Link-Comp-MS-Stac (3)	Link-Compression
234	Ascend-Target-Util	Integer	Target-Utilization
235	Ascend-Maximum-Channels	Integer	Maximum-Channels
236	Ascend-Inc-Channel-Count	Integer	Increment-Channel-Count

Table A-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
237	Ascend-Dec-Channel-Count	Integer	Decrement-Channel-Count
238	Ascend-Seconds-Of-History	Integer	Seconds-History
239	Ascend-History-Weigh-Type	History-Constant (0) History-Linear (1) History-Quadratic (2)	Dynamic-Algorithm
240	Ascend-Add-Seconds	Integer	Add-Persistence
241	Ascend-Remove-Seconds	Integer	Sub-Persistence
242	Ascend-Data-Filter	**IP filter:** *dir* *action* dstip *dest_ipaddr\subnet_mask* srcip *src_ipaddr\subnet_mask* *proto* dstport *cmp value* srcport *cmp value* *est*	**IP filter:** None None Dest-Address Dest-Address-Mask Source-Address Source-Address-Mask Protocol Dst-Port-Cmp Dest-Port Src-Port-Cmp Source-Port TCP-Estab
		Generic filter: *dir* *action* *offset* *mask* *value* *compare* more	**Generic filter:** None None Offset Mask Value Comp-Neq More

Table A-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
243	Ascend-Call-Filter	**IP filter:** *dir* *action* dstip *dest_ipaddr\subnet_mask* srcip *src_ipaddr\subnet_mask* *proto* dstport *cmp value* srcport *cmp value* *est*	**IP filter:** None None Dest-Address Dest-Address-Mask Source-Address Source-Address-Mask Protocol Dst-Port-Cmp Dest-Port Src-Port-Cmp Source-Port TCP-Estab
		Generic filter: *dir* *action* *offset* *mask* *value* *compare* more	**Generic filter:** None None Offset Mask Value Comp-Neq More
244	Ascend-Idle-Limit	Integer	Idle-Timer
245	Ascend-Preempt-Limit	Integer	None
246	Ascend-Callback	Callback-No (0) Callback-Yes (1)	Callback

Table A-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)	Data-Service

Table A-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-56Kbps
249	Ascend-Billing-Number	Text string	Billing-Number
250	Ascend-Call-By-Call	Integer	Call-By-Call
251	Ascend-Transit-Number	Text string	Transit-Number
252	Ascend-Host-Info	Text string	Host-*n* Text-*n*
253	Ascend-PPP-Address	IP address	Local-Address
254	Ascend-MPP-Idle-Percent	Integer	None
255	Ascend-Xmit-Rate	Integer	None

Attributes and parameters in alphabetical order

Table A-3 cross references the Ascend RADIUS dictionary's attributes to parameters in MAX TNT unit's menu-driven user interface. The table is arranged by attribute in alphabetical order.

Table A-3. Attributes and analogous parameters in alphabetical order

Attribute name	Attribute number	Attribute values	Analogous parameter
Acct-Authentic	45	RADIUS (1) Local (2)	None
Acct-Delay-Time	41	Integer	None
Acct-Input-Octets	42	Integer	None
Acct-Input-Packets	47	Integer	None
Acct-Output-Octets	43	Integer	None
Acct-Output-Packets	48	Integer	None
Acct-Session-Id	44	Text string	None
Acct-Session-Time	46	Integer	None
Acct-Status-Type	40	Start (1) Stop (2)	None

Table A-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-Add-Seconds	240	Integer	Add-Persistence
Ascend-ARA-PW	181	Text string	Future-Password
Ascend-Assign-IP-Client	144	IP address	None
Ascend-Assign-IP-Global-Pool	146	Text string	None
Ascend-Assign-IP-Pool	218	Integer	Address-Pool
Ascend-Assign-IP-Server	145	IP address	None
Ascend-ATM-Vci	95	Integer	None
Ascend-ATM-Vpi	94	Integer	None
Ascend-Authen-Alias	203	Text string	None
Ascend-Backup	176	Text string	Backup
Ascend-BACP-Enable	133	BACP-No (0) BACP-Yes (1)	None
Ascend-Base-Channel-Count	172	Integer	Base-Channel-Count
Ascend-Billing-Number	249	Text string	Billing-Number
Ascend-Callback	246	Callback-No (0) Callback-Yes (1)	Callback
Ascend-Callback-Delay	108	Integer	Delay-Callback
Ascend-Call-By-Call	250	Integer	Call-By-Call
Ascend-Call-Filter	243	**IP filter:** *dir* *action* dstip *dest_ipaddr\subnet_mask* srcip *src_ipaddr\subnet_mask* *proto* dstport *cmp value* srcport *cmp value* *est*	**IP filter:** None None Dest-Address Dest-Address-Mask Source-Address Source-Address-Mask Protocol Dst-Port-Cmp Dest-Port Src-Port-Cmp Source-Port TCP-Estab

Table A-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
		Generic filter: *dir* *action* *offset* *mask* *value* *compare* more	**Generic filter:** None None Offset Mask Value Comp-Neq More
Ascend-Call-Type	177	Nailed (1) Nailed/Mpp (2) Perm/Switched (3)	Call-Type
Ascend-Client-Assign-DNS	137	DNS-Assign-No (0) DNS-Assign-Yes (1)	Client-DNS-Addr-Assign
Ascend-Client-Gateway	132	IP address	Client-Default-Gateway
Ascend-Client-Primary-DNS	135	IP address	Client-DNS-Primary-Addr
Ascend-Client-Secondary-DNS	136	IP address	Client-DNS-Secondary-Addr
Ascend-Connect-Progress	196	Integer	None
Ascend-Data-Filter	242	**IP filter:** *dir* *action* dstip *dest_ipaddr\subnet_mask* srcip *src_ipaddr\subnet_mask* *proto* dstport *cmp value* srcport *cmp value* *est*	**IP filter:** None None Dest-Address Dest-Address-Mask Source-Address Source-Address-Mask Protocol Dst-Port-Cmp Dest-Port Src-Port-Cmp Source-Port TCP-Estab

Table A-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
		Generic filter: *dir* *action* *offset* *mask* *value* *compare* more	**Generic filter:** None None Offset Mask Value Comp-Neq More
Ascend-Data-Rate	197	Integer	None
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)	Data-Service

Table A-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-Data-Svc (*continued*)	247	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)	Data-Service
Ascend-DBA-Monitor	171	DBA-Transmit (0) DBA-Transmit-Recv (1) DBA-None (2)	Bandwidth-Monitor-Direction
Ascend-Dec-Channel-Count	237	Integer	Decrement-Channel-Count
Ascend-Dial-Number	227	Text string	Dial-Number
Ascend-Dialout-Allowed	131	Dialout-Not-Allowed (0) Dialout-Allowed (1)	Dialout-Allowed
Ascend-Disconnect-Cause	195	Integer	None
Ascend-Dsl-CIR-Recv-Limit	100	Integer	RX-Data-Rate-Limit
Ascend-Dsl-CIR-Xmit-Limit	101	Integer	TX-Data-Rate-Limit
Ascend-DSL-Downstream-Limit	99	adslcap-dn-7168000 (0) adslcap-dn-6272000 (1) adslcap-dn-5120000 (2) adslcap-dn-4480000 (3) adslcap-dn-3200000 (4) adslcap-dn-2688000 (5) adslcap-dn-2560000 (6) adslcap-dn-2240000 (7) adslcap-dn-1920000 (8) adslcap-dn-1600000 (9) adslcap-dn-1280000 (10) adslcap-dn-960000 (11) adslcap-dn-640000 (12)	Ses-ADSL-CAP-Down-Rate

Table A-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-Dsl-Rate-Mode	97	Rate-Mode-AutoBaud Rate-Mode-Single	Ses-Rate-Mode
Ascend-Dsl-Rate-Type	92	Rate-Type-Disabled Rate-Type-AdslCap Rate-Type-Sdsl Rate-Type-AdslDmt	Ses-Rate-Type
Ascend-DSL-Upstream-Limit	98	sdsl-144000 (0) sdsl-272000 (1) sdsl-400000 (2) sdsl-528000 (3) sdsl-784000 (4) sdsl-1168000 (5) sdsl-1552000 (6) sdsl-2320000 (7)	Ses-ADSL-CAP-Up-Rate
Ascend-Event-Type	150	Ascend-Coldstart (1) Ascend-Session-Event (2)	None
Ascend-Expect-Callback	149	Expect-Callback-No (0) Expect-Callback-Yes (1)	Expect-Callback
Ascend-Filter	91	*dir* dstip *dest_ipaddr\subnet_mask* srcip *src_ipaddr\subnet_mask* *proto* dstport *cmp value* srcport *cmp value* precedence *value* type-of-service *value*	None Dest-Address Dest-Address-Mask Source-Address Source-Address-Mask Protocol Dst-Port-Cmp Dest-Port Src-Port-Cmp Source-Port Precedence Type-of-Service
Ascend-First-Dest	189	IP address	None
Ascend-Force-56	248	Force-56-No (0) Force-56-Yes (1)	Force-56Kbps
Ascend-FR-Circuit-Name	156	Text string	Circuit-Name
Ascend-FR-DCE-N392	162	Integer	DCEN392-Val
Ascend-FR-DCE-N393	164	Integer	DCEN393-Val

Table A-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-FR-Direct	219	FR-Direct-No (0) FR-Direct-Yes (1)	FR-Direct-Enabled
Ascend-FR-Direct-DLCI	221	Integer	FR-Direct-DLCI
Ascend-FR-Direct-Profile	220	Text string	FR-Direct-Profile
Ascend-FR-DLCI	179	Integer from 16 to 991	DLCI
Ascend-FR-DTE-N392	163	Integer	N392-Val
Ascend-FR-DTE-N393	165	Integer	N393-Val
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-Link-Status-DLCI	106	Integer	Link-Mgmt-DLCI
Ascend-FR-N391	161	Integer	N391-Val
Ascend-FR-Nailed-Grp	158	Integer	Nailed-Up-Group
Ascend-FR-Profile-Name	180	Text string	Frame-Relay-Profile
Ascend-FR-T391	166	Integer	T391-Val
Ascend-FR-T392	167	Integer	T392-Val
Ascend-FR-Type	159	Ascend-FR-DTE (0) Ascend-FR-DCE (1) Ascend-FR-NNI (2)	Link-Type
Ascend-FT1-Caller	175	FT1-No (0) FT1-Yes (1)	FT1-Caller
Ascend-Group	178	Single integer or comma-separated group of integers	Nailed-Group Nailed-Groups
Ascend-History-Weigh-Type	239	History-Constant (0) History-Linear (1) History-Quadratic (2)	Dynamic-Algorithm
Ascend-Home-Agent-IP-Addr	183	IP address	None
Ascend-Home-Agent-UDP-Port	186	Integer	UDP-Port

Table A-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-Home-Network-Name	185	Text string	Home-Network-Name
Ascend-Host-Info	252	Text string	Host-*n* Text-*n*
Ascend-Idle-Limit	244	Integer	Idle-Timer
Ascend-IF-Netmask	153	IP address	None
Ascend-Inc-Channel-Count	236	Integer	Increment-Channel-Count
Ascend-IP-Direct	209	IP address	IP-Direct
Ascend-IP-Pool-Definition	217	Text string	Pool-Base-Address Assign-Count
Ascend-IP-TOS	88	Ascend-IP-TOS IP-TOS-Normal (0) Ascend-IP-TOS IP-TOS-Disabled (1) Ascend-IP-TOS IP-TOS-Cost (2) Ascend-IP-TOS IP-TOS-Reliability (4) Ascend-IP-TOS-IP-TOS-Throughput (8) Ascend-IP-TOS IP-TOS-Latency (16)	Type-of-Service
Ascend-IP-TOS-Apply-To	90	IP-TOS-Apply-To-Incoming (1024) IP-TOS-Apply-To-Outgoing (2048) IP-TOS-Apply-To-Both (3072)	Apply-To
Ascend-IP-TOS-Precedence	89	IP-TOS-Precedence-Pri-Normal (0) IP-TOS-Precedence-Pri-One (32) IP-TOS-Precedence-Pri-Two (64) IP-TOS-Precedence-Pri-Three (96) IP-TOS-Precedence-Pri-Four (128) IP-TOS-Precedence-Pri-Five (160) IP-TOS-Precedence-Pri-Six (192) IP-TOS-Precedence-Pri-Seven (224)	Precedence
Ascend-IPX-Alias	224	Text string	None
Ascend-IPX-Peer-Mode	216	IPX-Peer-Router (0) IPX-Peer-Dialin (1)	Peer-Mode

Table A-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-IPX-Route	174	*profile_name* *network#* *node#* *socket#* *server_type* *hop_count* *tick_count* *name*	Profile-Name Dest-Network Server-Node Server-Socket Server-Type Hops Ticks Name
Ascend-Link-Compression	233	Link-Comp-None (0) Link-Comp-Stac (1) Link-Comp-Stac-Draft-9 (2) Link-Comp-MS-Stac (3)	Link-Compression
Ascend-Maximum-Call-Duration	125	Integer	Max-Call-Duration
Ascend-Maximum-Channels	235	Integer	Maximum-Channels
Ascend-Maximum-Time	194	Integer	None
Ascend-Menu-Item	206	Text string	None
Ascend-Menu-Selector	205	Text string	None
Ascend-Metric	225	Integer	Metric
Ascend-Minimum-Channels	173	Integer	Minimum-Channels
Ascend-Modem-PortNo	120	Integer	None
Ascend-Modem-ShelfNo	122	Integer	None
Ascend-Modem-SlotNo	121	Integer	None
Ascend-MPP-Idle-Percent	254	Integer	None
Ascend-Multicast-Client	155	Multicast-No (0) Multicast-Yes (1)	Multicast-Allowed
Ascend-Multicast-GLeave-Delay	111	Integer	Multicast-Group-Leave-Delay
Ascend-Multicast-Rate-Limit	152	Integer	Multicast-Rate-Limit
Ascend-Multilink-ID	187	Integer	None
Ascend-Number-Sessions	202	Text string	None

Table A-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-Num-In-Multilink	188	Integer	None
Ascend-PPP-Address	253	IP address	Local-Address
Ascend-PPP-Async-Map	212	Integer	None
Ascend-PPP-VJ-1172	211	PPP-VJ-1172 (1)	None
Ascend-PPP-VJ-Slot-Comp	210	VJ-Slot-Comp-No (1)	None
Ascend-Preempt-Limit	245	Integer	None
Ascend-Pre-Input-Octets	190	Integer	None
Ascend-Pre-Input-Packets	192	Integer	None
Ascend-Pre-Output-Octets	191	Integer	None
Ascend-Pre-Output-Packets	193	Integer	None
Ascend-PreSession-Time	198	Integer	None
Ascend-PRI-Number-Type	226	Unknown-Number (0) Intl-Number (1) National-Number (2) Local-Number (4) Abbrev-Number (5)	Called-Number-Type
Ascend-Private-Route	104	Destination IP address and next-hop router IP address.	Private-Route
Ascend-PW-Expiration	21	Date	None
Ascend-PW-Lifetime	208	Integer	None
Ascend-PW-Warntime	207	Integer	None
Ascend-Receive-Secret	215	Text string	Recv-Password
Ascend-Redirect-Number	93	Text string	None
Ascend-Remote-Addr	154	IP address	IF-Remote-Address
Ascend-Remove-Seconds	241	Integer	Sub-Persistence
Ascend-Require-Auth	201	Not-Require-Auth (0) Require-Auth (1)	Auth-Rsp-Required
Ascend-Route-Appletalk	118	Route-Appletalk-No (0) Route-Appletalk-Yes (1)	Atalk-Routing-Enabled

Table A-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-Route-IP	228	Route-IP-No (0) Route-IP-Yes (1)	IP-Routing-Enabled
Ascend-Route-IPX	229	Route-IPX-No (0) Route-IPX-Yes (1)	IPX-Routing-Enabled
Ascend-Route-Preference	126	Integer	Static-Pref
Ascend-Secondary-Home-Agent	130	IP address or hostname	Secondary-Tunnel-Server
Ascend-Seconds-Of-History	238	Integer	Seconds-History
Ascend-Send-Auth	231	Send-Auth-None (0) Send-Auth-PAP (1) Send-Auth-CHAP (2)	Send-Auth-Mode
Ascend-Send-Passwd	232	Text string	Send-Password
Ascend-Send-Secret	214	Text string	Send-Password
Ascend-Session-Svr-Key	151	Text string	None
Ascend-Shared-Profile-Enable	128	Shared-Profile-No (0) Shared-Profile-Yes (1)	Shared-Prof
Ascend-Source-Auth	103	IP address and billing code	None
Ascend-Source-IP-Check	96	Source-IP-Check-No (0) Source-IP-C heck-Yes (1)	Source-IP-Check
Ascend-Target-Util	234	Integer	Target-Utilization
Ascend-Third-Prompt	213	Text string	Third-Login-Prompt
Ascend-Token-Expiry	204	Integer	None
Ascend-Token-Idle	199	Integer	None
Ascend-Token-Immediate	200	Tok-Imm-No (0) Tok-Imm-Yes (1)	None
Ascend-Transit-Number	251	Text string	Transit-Number
Ascend-TS-Idle-Limit	169	Integer	TS-Idle-Timer
Ascend-TS-Idle-Mode	170	TS-Idle-None (0) TS-Idle-Input (1) TS-Idle-Input-Output (2)	TS-Idle-Mode

Table A-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
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 Acct-Server-*n*
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-Type
Ascend-VRouter-Name	102	Text string	VRouter
Ascend-Xmit-Rate	255	Integer	None
Caller-Id	31	Text string	CLID
Challenge-Response	3	Text string	None
Change-Password	17	Text string	None
Class	25	Text string	None
Client-Port-DNIS	30	Text string	calledNumber
Filter-ID	11	Text string	None
Framed-Address	8	IP address	Remote-Address
Framed-Compression	13	Van-Jacobson-TCP-IP (1) (No other values supported)	VJ-Header-Prediction
Framed-MTU	12	Integer	MRU
Framed-Netmask	9	IP address	Netmask-Remote
Framed-Protocol	7	PPP (1) SLIP (2) ARA (255) MPP (256) FR (261) FR-CIR (263) ATM-1483 (264) ATM-FR-CIR (265)	Encapsulation-Protocol

Table A-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Framed-Route	22	*host_ipaddr/subnet_mask* *router_ ipaddr* *metric* *private* *profile_name*	Dest-Address Gateway-Address Metric Private-Route Name
Framed-Routing	10	None (0) Broadcast (1) Listen (2) Broadcast-Listen (3) Broadcast-v2 (4) Listen-v2 (5) Broadcast-Listen-v2 (6)	RIP
Idle-Timeout	28	Integer	None
Login-Host	14	IP address	Host
Login-Service	15	Telnet (0) Rlogin (1) TCP-Clear (2)	Service
Login-TCP-Port	16	Integer	Port
NAS-Identifier	4	IP address	IP-Address
NAS-Port	5	Zero-based, bit encoded number	None
NAS-Port-Type	61	NAS_Port_Type_Async (0) NAS_Port_Type_Sync (1)	None
Password (User-Password)	2	Text string	Recv-Password
Reply-Message	18	Text string	Banner (terminal-server users only)
Session-Timeout	27	Integer	None
Tunnel-Client-Endpoint	66	Text string	None
Tunnel-ID	68	Text string	None
Tunneling-Protocol	127	Integer	None
Tunnel-Medium-Type	65	IP (1)	None
Tunnel-Password	184	Text string	Password

Table A-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Tunnel-Server-Endpoint	67	IP address or hostname	Primary-Tunnel-Server
Tunnel-Type	64	PPTP (1), L2TP (3), ATMP (4)	Tunneling-Protocol
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)	Framed-Only
Vendor-Specific	26	Text string	None

Attribute and Packet Cross Reference

B

The following tables contain a list of packets and RADIUS attributes associated with authentication, connection setup, and user sessions. For information about attributes associated with accounting, see “Understanding accounting records” on page 4-13.

Access-Request (1)

By default, when it receives an incoming call, the MAX TNT first checks its local Connection profiles. If it doesn't find a Connection profile for the call, and you have configured the MAX TNT to communicate with RADIUS, the MAX TNT sends an Access-Request packet to the RADIUS server. The Access-Request packet includes the caller's name and password, and might also include the other attributes shown in Table B-1.

Table B-1. Access-Request attributes

Attribute	Description	Default value
Ascend-Send-Passwd (232)	Specifies the password the MAX TNT sends to the remote end of a connection on outgoing calls.	Null
Ascend-Send-Secret (214)	Directs the system to encrypt the password when passing it between the RADIUS server and the MAX TNT on outgoing calls.	Null
Caller-Id (31)	Specifies the calling-party number, indicating the phone number of the user that wants to connect to the unit.	Null
Challenge-Response (3)	Specifies the password that a CHAP user enters in response to a password challenge.	Null
Class (25)	Enables access providers to classify their user sessions for purposes such as billing users on the basis of the service option they choose. The Class attribute appears in Access-Request packets under CLID authentication.	Null
Client-Port-DNIS (30)	Specifies the called-party number, indicating the phone number the user dialed to connect to the MAX TNT.	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-Send67=No in the Rad-Auth-Client subprofile of the External-Auth profile.	No restrictions on the type of protocol a link can use
NAS-Identifier (4)	Specifies the IP address of the MAX TNT.	0.0.0.0/0
NAS-Port (5)	Specifies the port on which the unit received a call.	Specified in the `/etc/services` file
NAS-Port-Type (61)	Specifies the type of service in use for the session.	NAS_Port_Type_Async
Password (2)	Specifies the user's password for a call.	Null
User-Name (1)	Specifies the user's name.	Null
User-Service (6)	Specifies whether the link can use framed or unframed services. This attribute does not appear in an Access-Request packet if Auth-Send67=No in the Rad-Auth-Client subprofile of the External-Auth profile.	No restrictions on the services that a link can use

Access-Accept (2)

If the attribute values the MAX TNT 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 B-2 lists the RADIUS attributes defined in IETF RFC 2058 and supported by the Ascend RADIUS daemon.

Table B-2. RFC 2058 Access-Accept attributes supported by Ascend

Attribute	Description	Default value
Caller-Id (31)	Specifies the calling-party number, indicating the phone number of the user that wants to connect to the MAX TNT.	Null
Change-Password (17)	Used internally by the MAX TNT and the RADIUS server to change an expired password. When a user enters an expired password, RADIUS prompts the user for a new password. When the user enters the new password, the MAX TNT 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.	None (Attribute does not appear in a user profile.)
Class (25)	Enables access providers to classify their user sessions for purposes such as billing users on the basis of the service option they choose. If you include the Class attribute in the RADIUS user profile, the RADIUS server sends it to the MAX TNT in the Access-Accept packet when the session begins.	Null
Client-Port-DNIS (30)	Specifies the called-party number, indicating the phone number the user dialed to connect to the MAX TNT.	Null
Filter-ID (11)	Specifies the name of a local Filter profile that defines a data filter.	Null
Framed-Address (8)	Specifies the IP address of the remote user or calling device.	0.0.0.0
Framed-Compression (13)	Turns TCP/IP header compression on or off.	On
Framed-MTU (12)	Specifies the maximum number of bytes the MAX TNT can receive in a single packet on a PPP, MP, MP+, or Frame Relay link.	1524

Table B-2. RFC 2058 Access-Accept attributes supported by Ascend (continued)

Attribute	Description	Default value
Framed-Netmask (9)	Specifies the subnet mask associated with the IP address of a station or router at the remote end of the link.	0.0.0.0
Framed-Protocol (7)	Specifies the type of protocol a link can use.	No restrictions on the type of protocol a link can use
Framed-Route (22)	Specifies 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
Framed-Routing (10)	Specifies whether or not the MAX TNT sends RIP packets, receives RIP packets, or both.	Neither send nor receive RIP packets.
Idle-Timeout (28)	Specifies the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt.	120
Login-Host (14)	Specifies the host to which the MAX TNT automatically connects when you set User-Service=Login-User and specify a value for the Login-Service attribute.	0.0.0.0 (no host)
Login-Service (15)	Specifies the type of terminal-service connection to an IP host that occurs immediately after authentication.	No immediate access to any type of terminal-server session
Login-TCP-Port (16)	Specifies the port number to which a TCP session connects.	Null
Session-Timeout (27)	Specifies the maximum number of seconds of service to be provided to the user before termination of the session or prompt.	0
Tunnel-Medium-Type (65)	Specifies the media to use for the tunnel.	IP (1)
Tunnel-Password (69)	Specifies the password that the Foreign Agent sends to the Home Agent during ATMP operation.	Null
Tunnel-Server-Endpoint (67)	Specifies the IP address or hostname of the Ascend Tunnel Management Protocol (ATMP) primary Home Agent, L2TP Network Server (LNS) endpoint, or PPTP Network Server (PNS) endpoint.	0.0.0.0 (IP address) 5150 (UDP port)
Tunnel-Type (64)	Specifies the tunneling protocol to use.	None.

Table B-2. RFC 2058 Access-Accept attributes supported by Ascend (continued)

Attribute	Description	Default value
User-Service (6)	Specifies whether the link can use framed or unframed services. You can specify Framed-User, Login-User, or Dialout-Framed-User.	No restrictions on the services a link can use
Vendor-Specific (26)	Encapsulates attributes introduced by vendors.	Null

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

Table B-3. Ascend RADIUS Access-Accept attributes

Attribute	Description	Default value
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 TNT begins adding bandwidth to a session.	5
Ascend-ARA-PW (181)	Indicates the password of the incoming caller over ARA.	Null
Ascend-Assign-IP-Client (144)	Specifies the IP address of an Ascend unit that can use global IP address pools.	0.0.0.0
Ascend-Assign-IP-Global-Pool (146)	Specifies the global address pool from which RADIUS should assign a user an address.	Null
Ascend-Assign-IP-Pool (218)	Specifies the address pool that incoming calls use.	1
Ascend-Assign-IP-Server (145)	Specifies the IP address of the host running `radipad`.	0.0.0.0
Ascend-ATM-Vci (95)	Specifies the Virtual Channel Identifier for the connection.	32
Ascend-ATM-Vpi (94)	Specifies the Virtual Path Identifier for the connection.	0
Ascend-Authen-Alias (203)	Sets the MAX TNT unit's login name during PPP authentication.	Value of the Name parameter in the System profile
Ascend-Backup (176)	Specifies the name of a backup profile for a nailed-up link.	Null

Table B-3. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default value
Ascend-BACP-Enable (133)	Specifies whether you have enabled Bandwidth Allocation Control Protocol (BACP) for the link.	BACP-No (disabled)
Ascend-Base-Channel-Count (172)	Specifies the initial number of channels the MAX TNT sets up when originating calls for a PPP, MP, or MP+ multichannel link.	1
Ascend-Billing-Number (249)	Specifies a billing number for charges you incur on the line.	Null
Ascend-Callback (246)	Enables or disables callback.	Disable callback.
Ascend-Callback-Delay (108)	Specifies the number of seconds the MAX TNT waits before calling back a remote user.	0 (zero)
Ascend-Call-By-Call (250)	Specifies the T1 PRI service that the MAX TNT uses when placing a call.	ACCUNET Switched Digital Services from AT&T
Ascend-Call-Filter (243)	Defines a call filter.	Null
Ascend-Call-Type (177)	Specifies the type of nailed-up connection in use.	Nailed
Ascend-Client-Assign-DNS (137)	Specifies whether the MAX TNT sends the Ascend-Client-Primary-DNS and Ascend-Client-Secondary-DNS values during connection negotiation.	DNS-Assign-No
Ascend-Client-Gateway (132)	Specifies the default route for IP packets coming from the user on this connection.	0.0.0.0
Ascend-Client-Primary-DNS (135)	Specifies a primary DNS server address to send to any client connecting to the MAX TNT.	0.0.0.0
Ascend-Client-Secondary-DNS (136)	Specifies a secondary DNS server address to send to any client connecting to the MAX TNT.	0.0.0.0
Ascend-Data-Filter (242)	Defines a data filter.	Null
Ascend-Data-Svc (247)	Specifies the type of data service the link uses.	Switched-56

Table B-3. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default value
Ascend-DBA-Monitor (171)	Specifies how the MAX TNT monitors traffic on an MP+ call.	DBA-Transmit (Add or subtract bandwidth based on the amount of data transmitted.)
Ascend-Dec-Channel-Count (237)	Specifies the number of channels the MAX TNT removes when bandwidth changes during a call.	1
Ascend-Dial-Number (227)	Specifies the phone number the MAX TNT dials to reach the router or node at the remote end of the link.	Null
Ascend-Dialout-Allowed (131)	Specifies whether the user associated with the RADIUS user profile can dial out by means of one of the MAX TNT unit's digital modems.	Dialout-Not Allowed
Ascend-Dsl-CIR-Recv-Limit (100)	Specifies the maximum data rate (in k-bits per second) to be received across the connection.	0 (zero)
Ascend-Dsl-CIR-Xmit-Limit (101)	Specifies the maximum data rate (in k-bits per second) to be transmitted across the connection.	0 (zero)
Ascend-DSL-Downstream-Limit (99)	Specifies the per-session downstream data rate.	adslcap-dn-2560000 (6)
Ascend-Dsl-Rate-Type (92)	Specifies the per-session modem type for rate control.	Rate-Type-Disabled
Ascend-Dsl-Rate-Mode (97)	Specifies the per-session DSL data rate mode.	Rate-Mode-AutoBaud
Ascend-DSL-Upstream-Limit (98)	Specifies the per-session upstream data rate.	None
Ascend-Expect-Callback (149)	Specifies whether a user calling out should expect the remote end to call back.	Expect-Callback-No
Ascend-Filter (91)	Specifies a string-format filter, which can include an IP TOS filter specification.	Null
Ascend-First-Dest (189)	Specifies the destination IP address of the first packet the MAX TNT receives over a connection after the connection has been authenticated.	None (Attribute does not appear in a user profile.)

Table B-3. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default value
Ascend-Force-56 (248)	Specifies whether the MAX TNT uses only the 56-Kbps portion of a channel even when all 64 Kbps appear to be available.	Force-56-No (Attempt to use all 64 Kbps.)
Ascend-FR-Circuit-Name (156)	Specifies the Permanent Virtual Connection (PVC) for which the user profile is an endpoint.	Null
Ascend-FR-DCE-N392 (162)	Specifies the number of errors, occurring during Ascend-FR-DCE-N393-monitored events, that cause the network side to declare the user side's procedures inactive.	3
Ascend-FR-DCE-N393 (164)	Specifies the maximum value of the DCE-monitored event count.	4
Ascend-FR-Direct (219)	Specifies whether the MAX TNT uses a Frame Relay Direct configuration for Frame Relay packets.	FR-Direct-No
Ascend-FR-Direct-DLCI (221)	Identifies the user profile to the Frame Relay switch for Frame Relay Direct.	16
Ascend-FR-Direct-Profile (220)	Specifies the name of the Frame Relay profile for Frame Relay Direct.	Null
Ascend-FR-DLCI (179)	Specifies a Data Link Connection Indicator (DLCI) number for a Frame Relay gateway or switch.	16
Ascend-FR-DTE-N392 (163)	Specifies the number of errors, occurring during Ascend-FR-DTE-N393-monitored events, that causes the network side to declare the user side's procedures inactive.	3
Ascend-FR-DTE-N393 (165)	Specifies the maximum value of the DTE-monitored event count.	4
Ascend-FR-Link-Mgt (160)	Specifies the type of Frame Relay link management in use for the profile.	Ascend-FR-No-Link-Mgt
Ascend-FR-Link-Status-DLCI (106)	Specifies the DLCI to use for link management on the Frame Relay datalink.	0 (zero)

Table B-3. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default value
Ascend-FR-N391 (161)	Specifies the interval at which the MAX TNT requests a Full Status Report.	6
Ascend-FR-Nailed-Grp (158)	Specifies the nailed-channel number for a Frame Relay datalink.	1
Ascend-FR-Profile-Name (180)	Specifies the name of the Frame Relay profile to use when the MAX TNT is configured as a Frame Relay gateway or Frame Relay switch.	Null
Ascend-FR-T391 (166)	Sets the Link Integrity Verification polling time.	10
Ascend-FR-T392 (167)	Sets 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 TNT does not receive a Status Enquiry message within the number of seconds specified by this attribute.	15
Ascend-FR-Type (159)	Specifies the kind of logical interface between the MAX TNT and the Frame Relay network on the datalink.	Ascend-FR-DTE (UNI-to-DTE connection)
Ascend-FT1-Caller (175)	Specifies whether the MAX TNT initiates or waits for the remote end to initiate an FT1-B&O call.	FT1-No (Wait for the remote end to initiate the call.)
Ascend-Group (178)	Points to the nailed-up channels that the WAN link uses.	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-Quadratic
Ascend-Home-Agent-UDP-Port (186)	Specifies the UDP port number to use when the Foreign Agent sends ATMP packets to the Home Agent.	5150
Ascend-Home-Network-Name (185)	Specifies the name of the Connection profile through which the Home Agent sends all packets it receives from the Mobile Client during ATMP operation.	Null

Table B-3. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default value
Ascend-Host-Info (252)	Specifies the IP address and description of up to 10 hosts to which a user can establish a Telnet session.	0.0.0.0/0 (address) Null (description)
Ascend-Idle-Limit (244)	Specifies the number of seconds the MAX TNT waits before clearing a call when a session is inactive.	120
Ascend-IF-Netmask (153)	Specifies the subnet mask in use for the local numbered interface.	0.0.0.0
Ascend-Inc-Channel-Count (236)	Specifies the number of channels the MAX TNT adds when bandwidth changes during a call.	1
Ascend-IP-Direct (209)	Specifies the IP address to which the MAX TNT redirects packets from the user.	0.0.0.0. (no IP redirection)
Ascend-IP-Pool-Definition (217)	Specifies the pool number, first IP address, and the number of addresses in an IP address pool.	1 (pool number) 0.0.0.0 (first IP address) 0 (number of IP addresses)
Ascend-IP-TOS (88)	Specifies the Type-of-Service (TOS) of the data stream.	IP-TOS-Normal (0)
Ascend-IP-TOS-Apply-To (90)	Specifies in which direction Type-of-Service (TOS) is enabled.	IP-TOS-Apply-To-Incoming (1024)
Ascend-IP-TOS-Precedence (89)	Specifies the priority level of the data stream.	IP-TOS-Precedence-Pri-Normal (0)
Ascend-IPX-Alias (224)	Specifies an IPX network number to use when connecting to IPX routers that require numbered interfaces.	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 (Ethernet client with its own IPX network address)

Table B-3. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default value
Ascend-IPX-Route (174)	Defines a static IPX route.	*profile_name*=null *network#*=00000000 *node#*= 0000000000001 *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, MP, or MP+ link.	Off
Ascend-Maximum-Call-Duration (125)	Specifies the maximum number of minutes that the MAX TNT allows individual channels in a call to stay connected, regardless of the data traffic over the connection	0 (zero)
Ascend-Maximum-Channels (235)	Specifies the maximum number of channels allowed on an MP+ call.	1
Ascend-Maximum-Time (194)	Specifies the maximum number of seconds that the MAX TNT allows the call to stay connected, regardless of the data traffic over the connection.	0 (zero–no time limit)
Ascend-Menu-Item (206)	Defines a single menu item for a user profile.	Standard terminal-server menu
Ascend-Menu-Selector (205)	Specifies a string as a prompt for user input in the terminal-server menu interface.	`Enter Selection (1-`*num*`, q)`, where *num* is the number of items on the menu.
Ascend-Metric (225)	Specifies the virtual hop count of the route.	7
Ascend-Minimum-Channels (173)	Specifies the minimum number of channels an MP+ call maintains.	1
Ascend-MPP-Idle-Percent (254)	Specifies a percentage of bandwidth utilization below which the MAX TNT clears a single-channel MP+ call.	0 (zero)
Ascend-Multicast-Client (155)	Specifies whether the user is a multicast client of the MAX TNT.	Multicast-No

Table B-3. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default value
Ascend-Multicast-GLeave-Delay (111)	Specifies the number of seconds the MAX TNT waits before forwarding an IGMP version 2 `leave group` message from a multicast client.	0 (zero)
Ascend-Multicast-Rate-Limit (152)	Specifies how many seconds the MAX TNT waits before accepting another packet from a multicast client.	100
Ascend-Multilink-ID (187)	Specifies the ID number of the Multilink bundle when the session closes. A Multilink bundle is a multichannel MP or MP+ call.	None (Attribute does not appear in a user profile.)
Ascend-Num-In-Multilink (188)	Specifies the number of sessions remaining in a Multilink bundle when the session closes.	None (Attribute does not appear in a user profile.)
Ascend-PPP-Address (253)	Specifies the IP address of the local numbered interface to the WAN.	0.0.0.0
Ascend-PPP-Async-Map (212)	Gives the MAX TNT the async control-character map for the PPP, MP, or MP+ session.	Standard async control character
Ascend-PPP-VJ-1172 (211)	Specifies whether the MAX TNT should use the 0037h value for the VJ compression type.	VJ compression type 002dh
Ascend-PPP-VJ-Slot-Comp (210)	Specifies whether the MAX TNT should use slot compression when sending VJ-compressed packets.	VJ-Slot-Comp-Yes (slot compression)
Ascend-Preempt-Limit (245)	Specifies the number of idle seconds the MAX TNT waits before using one of the channels of an idle link for a new call.	60
Ascend-Pre-Input-Octets (190)	Records the number of input octets before authentication for asynchronous sessions. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.	None (Attribute does not appear in a user profile.)

Table B-3. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default value
Ascend-Pre-Input-Packets (192)	Specifies the number of input packets before authentication for framed sessions. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.	None (Attribute does not appear in a user profile.)
Ascend-Pre-Output-Octets (191)	Specifies the number of output octets before authentication for asynchronous sessions. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet.	None (Attribute does not appear in a user profile.)
Ascend-Pre-Output-Packets (193)	Records the number of output packets before authentication for framed sessions. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets.	None (Attribute does not appear in a user profile.)
Ascend-PRI-Number-Type (226)	Specifies the type of phone number the MAX TNT dials.	National-Number
Ascend-Private-Route (104)	Specifies a destination IP address and next-hop router IP address for a private route.	0.0.0.0 — 0.0.0.0
Ascend-PW-Expiration (21)	Specifies an expiration date for the user's password.	No expiration date
Ascend-PW-Lifetime (208)	Specifies on a per-user basis the number of days that a password is valid.	Value of the Lifetime-In-Days attribute in the Ascend dictionary
Ascend-PW-Warntime (207)	Specifies the number of days before password expiration that the RADIUS server sends a message informing the user that the password will expire.	0 (zero)
Ascend-Receive-Secret (215)	Specifies a value received from a dial-in user to verify an encrypted password.	Null
Ascend-Remote-Addr (154)	Specifies the IP address of the link's remote interface to the WAN.	0.0.0.0

Table B-3. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default value
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 TNT begins removing bandwidth from a session.	10
Ascend-Require-Auth (201)	Specifies whether additional authentication is required for calls that have passed CLID or called-number authentication.	Not-Require-Auth (additional authentication not required)
Ascend-Route-Appletalk (118)	Specifies whether AppleTalk routing is allowed for the user profile.	Route-Appletalk-No
Ascend-Route-IP (228)	Enables or disables the routing of IP data packets over the link.	Enable IP routing.
Ascend-Route-IPX (229)	Enables or disables IPX routing.	Disable IPX routing.
Ascend-Route-Preference (126)	Specifies the preference for a route defined by the Framed-Address attribute in a user profile.	60
Ascend-Secondary-Home-Agent (130)	Specifies the secondary Home Agent the Foreign Agent tries to reach when the primary Home Agent (Tunnel-Server-Endpoint) is unavailable. Also indicates the UDP port the Foreign Agent uses for the link.	0.0.0.0 (IP address) 5150 (UDP port)
Ascend-Seconds-Of-History (238)	Specifies the number of seconds the MAX TNT uses as a sample for calculating average line utilization (ALU) of transmitted data.	15
Ascend-Send-Auth (231)	Specifies the protocol to use for name-password authentication.	Do not use an authentication protocol.
Ascend-Send-Passwd (232)	Specifies the password the MAX TNT sends to the remote end of a connection on outgoing calls.	Null
Ascend-Send-Secret (214)	When used in place of the Ascend-Send-Passwd attribute, directs the system to encrypt the password when passing it between the RADIUS server and the MAX TNT.	Null

Table B-3. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default value
Ascend-Shared-Profile-Enable (128)	Specifies whether multiple incoming callers can share a single RADIUS user profile.	Shared-Profile-No
Ascend-Source-Auth (103)	Specifies a source IP address and associated billing code.	Null
Ascend-Source-IP-Check (96)	Enables or disables anti-spoofing for the session	Disable anti-spoofing feature.
Ascend-Target-Util (234)	Specifies the percentage of bandwidth utilization at which the MAX TNT adds or subtracts bandwidth dynamically.	70
Ascend-Third-Prompt (213)	Specifies an additional prompt for user input after the login and password prompts.	Do not display an additional prompt.
Ascend-Token-Expiry (204)	Sets the lifetime of a cached token (that is, the lifetime of token-card authentication).	0 (zero–token caching 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.	Value of Ascend-Token-Expiry
Ascend-Token-Immediate (200)	Establishes how RADIUS treats the password received from a Login-User when the user profile specifies a token-card server.	Tok-Imm-No (Do not use a cached token.)
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.	Null
Ascend-TS-Idle-Limit (169)	Specifies the number of seconds that a terminal-server connection must be idle before the MAX TNT disconnects the session.	120
Ascend-TS-Idle-Mode (170)	Specifies whether the MAX TNT uses a terminal-server idle timer and, if so, whether both the user and host must be idle before the MAX TNT disconnects the session.	TS-Idle-Input (Disconnect the session if the user is idle for a length of time greater than Ascend-TS-Idle-Limit.)
Ascend-VRouter-Name (102)	Specifies the name of a defined Virtual Router (VRouter).	Null

Access-Reject (3)

If the attribute values submitted to RADIUS do not match the attribute values in the user profile, the RADIUS server does not authenticate the call. It returns an Access-Reject packet containing one or more of the values listed in Table B-4.

Table B-4. Access-Reject attributes

Attribute	Description	Default value
Login-TCP-Port (16)	Specifies the port number to which a TCP session connects.	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.	Null

Access-Password-Request (7)

Table B-5 lists the attributes that appear in an Access-Password-Request packet.

Table B-5. Access-Password-Request attributes

Attribute	Description	Default value
Change-Password (17)	Specifies an expired password. The Change-Password attribute is used internally by the MAX TNT and the RADIUS server.	None
Password (2)	Specifies a new password. 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.	Null
User-Name (1)	Specifies the user's name.	Null

Access-Password-Ack (8)

The Access-Password-Ack packet contains no attributes. The RADIUS server sends it to the MAX TNT to signal that a new password has been accepted.

Access-Password-Reject (9)

The Access-Password-Reject packet contains the Reply-Message (18) attribute.

Access-Challenge (11)

An Access-Challenge packet can contain the Reply-Message (18) attribute, which specifies text prompting the user to enter a password in response to a challenge.

Access-Password-Expired (32)

An Access-Password-Expired packet contains the Reply-Message (18).

Ascend-Access-Event-Request (33)

The MAX TNT can report the number of sessions by class to the RADIUS authentication server and to the RADIUS accounting server. The MAX TNT reports the number of sessions by sending an Ascend-Access-Event-Request (33) packet type at a user-defined interval specified by one of the following parameters:

- Auth-Sess-Interval in the Rad-Auth-Client subprofile of the External-Auth profile
- Acct-Sess-Interval in the Rad-Acct-Client subprofile of the External-Auth profile

Table B-6 lists the attributes in an Ascend-Access-Event-Request packet.

Table B-6. Ascend-Access-Event-Request attributes

Attribute	Description	Default value
NAS-Identifier (4) (authentication and accounting requests)	Specifies the IP address of the MAX TNT.	0.0.0.0/0
Password (2) (authentication requests only)	Specifies the user's password for an incoming or outgoing call.	Null
Ascend-Event-Type (150) (authentication and accounting requests)	Specifies that the MAX TNT is informing the RADIUS server of a coldstart (for an accounting request) or sending a session report (for an authentication request).	Ascend-Coldstart (1) for an accounting request and Ascend-Session-Event (2) for an authentication request
Ascend-Number-Sessions (202) (authentication and accounting requests)	Specifies the number of active user sessions of a given class. In the case of multichannel calls, such as MP+ calls, each separate connection counts as a session.	0 (zero)

Ascend-Access-Event-Response (34)

Table B-7 lists the attributes in an Ascend-Access-Event-Response packet.

Table B-7. Ascend-Access-Event-Response attributes

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

Ascend-Disconnect-Request (40)

Table B-8 lists the attributes in an Ascend-Disconnect-Request packet.

Table B-8. Ascend-Disconnect-Request attributes

Attribute	Description	Default value
User-Name (1)	The MAX TNT disconnects all routing sessions associated with this user name. If you specify Framed-Address as well, the MAX TNT disconnects only routing sessions associated with both attributes.	Null
Framed-Address (8)	The MAX TNT disconnects all routing sessions associated with this address. If you specify User-Name as well, the MAX TNT disconnects only routing sessions associated with both attributes. The MAX TNT ignores the default address of 0.0.0.0.	0.0.0.0
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 TNT ignores numbers outside the valid range. The number you specify must match the session reference number used in SNMP accounting or RADIUS accounting.	No default
Ascend-Session-Svr-Key (151)	Specifies the session key that identifies the user session. You can specify up to 16 characters.	Null

Ascend-Disconnect-Ack (41)

If RADIUS found at least one session it could disconnect, the response code is 41 (Disconnect-Request-Ack). RADIUS does not return any attributes in the response.

Ascend-Disconnect-Nak (42)

If RADIUS did not find at least one session it could disconnect, the response code is 42 (Disconnect-Request-Nak). RADIUS does not return any attributes in the response.

Ascend-Change-Filters-Request (43)

In a Change-Filter-Request packet, the attributes listed in Table B-9 control filter changes.

Table B-9. Ascend-Change-Filters-Request attributes

Attribute	Description	Default value
User-Name (1)	The MAX TNT changes the filters for all routing sessions associated with this user name. If you specify Framed-Address as well, the MAX TNT changes filters only for routing sessions associated with both attributes.	Null
Framed-Address (8)	The MAX TNT changes the filters for all routing sessions associated with this address. If you specify User-Name as well, the MAX TNT changes filters only for routing sessions associated with both attributes. The MAX TNT ignores the default address of 0.0.0.0.	0.0.0.0
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 TNT ignores numbers outside the valid range. The number you specify must match the session reference number used in SNMP accounting or RADIUS accounting.	No default
Ascend-Data-Filter (242)	Specifies the data filter to use.	Null
Ascend-Call-Filter (243)	Specifies the call filter to use.	Null
Ascend-Session-Svr-Key (151)	Specifies the session key that identifies the user session. You can specify up to 16 characters.	Null

Ascend-Change-Filters-Ack (44)

If RADIUS found at least one routing session whose filters it could change, the response code is 44 (Change-Filter-Request-Ack). RADIUS does not return any attributes in the response.

Ascend-Change-Filters-Nak (45)

If RADIUS did not find at least one routing session whose filters it could change, the response code is 45 (Change-Filter-Request-Nak).

Troubleshooting

C

This chapter presents strategies for how to diagnose and resolve problems that might occur when you set up and use the MAX TNT with RADIUS. It consists of the following sections:

RADIUS authentication problems

If RADIUS is not properly authenticating dial-in users, you must carry out the following tasks until you locate the source of the problem:

1 Isolate the problem to the RADIUS server.

2 Check the RADIUS configuration and program files.

3 Check the MAX TNT parameters for proper configuration.

4 Run the RADIUS daemon in debug mode.

5 Check the log file.

6 Determine whether all users are failing authentication.

Isolating the problem to the RADIUS server

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, your RADIUS configuration is the source of the problem.

Checking the RADIUS configuration and program files

Check the RADIUS files for proper installation and configuration:

1. Make sure that you have copied the `dictionary`, `users`, and `clients` files into the `/etc/raddb` directory. If you modify the `clients` file, you must restart the RADIUS daemon.
2. Verify that you are using the latest version of the Ascend RADIUS daemon.
3. Confirm that there are no syntax errors in the user profile. A comma must appear at the end of every line, except the first and last lines. The Default entry in the `users` file must be the last entry in the file. You need not specify an attribute in a profile unless you want to change the value from its default setting.
4. Check whether you are attempting to authenticate a UNIX user with CHAP. 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.

Checking the MAX TNT parameters

In the External-Auth profile on the MAX TNT, make sure that Auth-Type=RADIUS. Then, open the Rad-Auth-Client subprofile, and verify the following settings:

1. The Auth-Server-*n* parameter must specify the correct IP address of the RADIUS server.
2. The Auth-Port parameter must specify the RADIUS daemon's authentication port as entered in the `/etc/services` file.
3. The Auth-Key parameter must specify the MAX TNT unit's password as entered 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 Rad-Acct-Client subprofile on the MAX TNT must specify the same password as the Auth-Key parameter.
4. The Name parameter in the System profile must specify the MAX TNT unit's name as entered in the `/etc/raddb/clients` file. Verify that the IP address of the MAX TNT can be resolved from the name.
5. In the Answer-Defaults profile, make sure that Profiles-Required=Yes.
6. If you are using PAP, CHAP, or MS-CHAP authentication for incoming PPP, MP, and MP+ calls, you must set Recv-Auth-Mode in the PPP-Answer subprofile of the Answer-Defaults profile to the appropriate value.
7. If you want modem callers to dial into the terminal server, you must set Security-Mode=Full in the Terminal-Server profile.

Running the RADIUS daemon in debug mode

Run the RADIUS daemon in debug mode by entering one of the following commands:

- **`radiusd -x`** (for the flat ASCII `users` file)
- **`radiusd.dbm -x`** (for the DBM database)

Checking the log file

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 C-1 provides a partial list of error messages.

Table C-1. Log file error messages

Message	Explanation
CALC_DIGEST	The `clients` file contains an incorrect entry. Or, the name of the MAX TNT 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 message 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 Rad-Auth-Client subprofile of the External-Auth profile.
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 might have the incorrect IP address for the MAX TNT. Or, the RADIUS server might be unable to resolve the IP address from the name of the MAX TNT in the `clients` file. To resolve this error, specify the correct IP address of the MAX TNT in the `clients` file.

Determining whether all users are failing authentication

If all modem users except those on a particular platform can connect, contact Ascend technical support for assistance.

RADIUS accounting problems

This section describes the following types of problems:

- General accounting errors
- Duplicate or deleted records
- Backoff-queue error messages

General accounting errors

If RADIUS is not properly providing accounting information, proceed as follows:

1. Make sure that the RADIUS daemon is running with the `-A` argument specified.
2. Verify that the `/usr/adm/radacct` directory exists. This directory contains accounting information. If it does not exist, create it. Or, use the `-a` argument when starting the daemon, and specify a different directory in which to store accounting information.
3. In the External-Auth profile on the MAX TNT, make sure that Acct-Type=Acct-RADIUS.
4. Open the Rad-Auth-Client subprofile.
5. Make sure that the Acct-Server-*n* parameter specifies the IP address of the RADIUS host.
6. Verify that the Acct-Port indicates the UDP port number you specified for the accounting process of the daemon in `/etc/services`. If you used the `incr` keyword for the `-A` argument when starting the daemon, make sure that the parameter specifies the UDP port for authentication services plus 1.
7. Make sure that the Acct-Key specifies the RADIUS client password exactly as it appears in the RADIUS `clients` file.

Duplicate or deleted records

If the MAX TNT 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, it resends the packet. RADIUS reports the resent packet as a duplicate. The following message appears on the console:

`Dropping duplicate from MAX TNT, id=`*`num`*

The message can also appear if the MAX TNT 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. Delays in the link between the MAX TNT and the RADIUS server can cause the duplications. In addition, the delays can cause the MAX TNT to lose accounting records when its accounting buffer overflows.

The following devices can cause delays in the link between the MAX TNT 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 eventually runs out of memory. To prevent this situation, the unit deletes the accounting records and displays the following error message:

`Backoff Q full, discarding user` *`username`*

This error generally occurs for one of two reasons:

- You enabled RADIUS accounting on the MAX TNT, but not on the RADIUS server.
- You are using the Livingston server instead of the Ascend server.

Connect progress codes

The Ascend-Connect-Progress attribute specifies the state of the connection before it is disconnected. The MAX TNT includes Ascend-Connect-Progress in an Accounting-Request packet when the session has ended or has failed authentication (Acct-Status-Type=Stop).

For information about the values returned for the Ascend-Connect-Progress attribute, see “Ascend-Connect-Progress (196)” on page 3-18.

Disconnect cause codes

The Ascend-Disconnect-Cause attribute specifies the reason a connection is offline. The MAX TNT includes Ascend-Disconnect-Cause in an Accounting-Request packet when the session has ended or has failed authentication (Acct-Status-Type=Stop).

For information about the values returned for the Ascend-Disconnect-Cause attribute, see “Ascend-Disconnect-Cause (195)” on page 3-29.

Sample RADIUS Users File

D

This appendix contains an example of how you might set up a RADIUS users file. If you plan to use this example as a template, be sure to properly modify any site-specific settings before you use the file.

```
#  S A M P L E   R A D I U S   U S E R S   F I L E
#
#  This file contains security and configuration information
#  for each user. The first field is the user's name,
#  followed (on the same line) with the list of authentication
#  requirements for the user. These can include password, user name,
#  and an expiration date for the user's password. When an
#  authentication request is received from the unit, these values
#  are tested. A special user named "DEFAULT" can be created (and
#  should be placed at the end of the users file) to specify what to do
#  with users not contained in the users file. A special password of
#  "UNIX" can be specified to notify the authentication server to use
#  UNIX password (/etc/passwd) authentication for the user.
#
#  Line indented by means of the Tab character following the first
#  line indicate the configuration values to be passed back to
#  the unit to allow the initiation of a user session.
#  These can include things like the PPP configuration values.
#
#  Sample users file entries follow:

#  The following profile can only be used for PPP sessions.
#  It uses a local password.
#
testPassword = "test"
    User-Service = Framed-User,
    Framed-Protocol = MPP,
    Ascend-Assign-IP-Pool = 1,
    Framed-Routing = None,
    Ascend-Idle-Limit = 30
```

```
#  The following profile uses the UNIX password file so that
#  the password does not have to be stored locally.
#
ascend2Password = "UNIX"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.0.2.1,
    Framed-Netmask = 255.255.255.0

#  The following profile provides authentication by means of the
#  Enigma Logic SafeWord dynamic password library.
#
ascend3Password = "SAFEWORD"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.0.3.1,
    Framed-Netmask = 255.255.255.0

#  The following profile provides authentication, by means of the
#  Enigma Logic SafeWord dynamic password library, with token caching
#  for 90 minutes.
#
ascend4Password = "SAFEWORD", Ascend-Token-Expiry = 90
    Ascend-Receive-Secret = "shared secret",
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.0.3.1,
    Framed-Netmask = 255.255.255.0

#  The following profile provides authentication by means of the
#  Security Dynamics ACE dynamic password library, with token caching
#  for 540 minutes (9 hours) and an idle time of 80 minutes. "Idle"
#  means without a new call authentication, *not* without a call being
#  up. This example specifies that tokens should be cached all day and
#  allows a break as long as it doesn't exceed 80 minutes.
#
```

```
ascend5Password = "ACE", Ascend-Token-Expiry = 540, Ascend-Token-Idle
= 80
    Ascend-Receive-Secret = "shared secret",
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Address = 10.0.3.1,
    Framed-Netmask = 255.255.255.0

#   The following profile provides authentication by means of the
#   Security Dynamics ACE dynamic password library, with no challenge.
#   The dynamic password is entered in place of the usual "static"
#   password. The profile is useful only for modem dial-in calls.
#
ascend6Password = "ACE", Ascend-Token-Immediate = Tok-Imm-Yes
    User-Service = Login-User,
    Login-Service = Telnet,
    Login-Host = 10.0.4.1

#   The following profile provides authentication by means of the
#   Enigma Logic SafeWord dynamic password library, with no challenge.
#   The dynamic password is entered in place of the usual "static"
#   password. The profile is useful only for modem dial-in calls.
#
ascend7Password = "SAFEWORD", Ascend-Token-Immediate = Tok-Imm-Yes
    User-Service = Login-User,
    Login-Service = Telnet,
    Login-Host = 10.0.4.1

#
#
#   ANY ACE entry may be used to authenticate multiple users behind
#   a single remote router, such as a Pipeline. The following profile
#   entry uses the Pipeline unit’s name, and password = ACE, as usual.
#   However, when the user enters the password, he or she specifies
#   <password><.><realname> instead of just <password>. In this case,
#   <realname> will be presented to the ACE server, rather than the
#   Pipeline unit’s name. Token caching will still function normally.
#   All users will share the same profile, and all accounting will use
#   the Pipeline 50 name, not the real user name.
#
```

```
#  The following profile can only be used for PPP sessions. An
#  address will be assigned from address pool 1. A route to 10.0.0.1
#  is added with the user's address as the gateway.
#
ascendpPassword = "pipeline"
    User-Service = Framed-User,
    Framed-Protocol = PPP,
    Framed-Routing = None,
    Ascend-Assign-IP-Pool = 1,
    Ascend-Idle-Limit = 30,
    Framed-Route = "10.0.0.1 0.0.0.0 1"

#  The following profile causes the unit to start an auto-Telnet
#  to 10.0.4.1 upon login.
#
userPassword = "xyzzy"
    User-Service = Login-User,
    Login-Service = Telnet,
    Login-Host = 10.0.4.1

#  The following profile causes the password to expire on 99/01/30.
#  If the password is changed remotely, the new password will have
#  a duration of 180 days.
#
useraPassword = "ageing", Ascend-PW-Expiration = "Jan 1 1999"
    User-Service = Login-User,
    Login-Service = Telnet,
    Ascend-PW-Lifetime = 180

#  Use the following profile as a template for ARA user access.
#  NOTE: The password and Ascend-Send-Secret MUST be
#  identical
#
userxyz Password = "abcdef"
    Framed-Protocol = ARA,
    Ascend-Send-Secret = "abcdef"
```

```
#  The following profile causes the unit to start a raw TCP connection
#  to 10.0.5.1, port 23.
#
test1Password = "test1"
    Login-Service = TCP-Clear,
    Login-Host = 10.0.5.1,
    Login-TCP-Port = 23

#  The following profile causes the unit to start a raw TCP connection
#  to 10.0.6.1, port 7.
#
test2Password = "test2"
    Login-Service = TCP-Clear,
    Login-Host = 10.0.6.1,
    Login-TCP-Port = 7

#  The following profile causes the unit to start a Telnet connection
#  to 10.0.7.1, port 25.
#
test3Password = "test3"
    Login-Service = Telnet,
    Login-Host = 10.0.7.1,
    Login-TCP-Port = 25

#  The following profile specifies a unit on a subnet dialing in
#  across a T1/PRI link, using a maximum of 23 channels..
#
maxPassword = "max"
    Framed-Address = 10.0.8.1,
    Framed-Netmask = 255.255.255.0,
    Ascend-Metric = 1,
    Ascend-Maximum-Channels = 23,
    Ascend-Link-Compression = Link-Comp-None,
    Ascend-Idle-Limit = 30
```

```
#  The following profile specifies a Pipeline 50 performing IPX
#  Routing only.
#
ipxtest Password = "netware"
   Ascend-Route-IPX = Route-IPX-Yes,
   Ascend-Route-IP = Route-IP-No,
   Ascend-IPX-Peer-Mode = Peer-Mode-Router


#  P S E U D O-U S E R S
#
#  These 'users' exist to store information that the unit can query.
#  The profiles are not intended for real login users. The
#  password for pseudo-users is always "ascend". Each pseudo-user
#  profile includes a "User-Service" attribute of Dialout-Framed-User
#  so that it cannot be used for user authentication.
#
#  Following are the pseudo-users you can specify:
#
#  banner:Storage of the terminal-server menu mode,
#         login banner, and table of host addresses
#         with descriptive text for the login menu.
#
#  pools-xxx:Definitions of address pools used by the
#         unit named xxx. The unit can support
#         several address pools. Two can be defined
#         in the unit. Those two can be overridden
#         and more defined from RADIUS.
#
#  route-n:A series of pseudo-users fetched by the
#         unit to initialize its routing table.
#         The unit queries route-1, then route-2,
#         then route-3, and so on, until it receives an
#         authentication reject from RADIUS. Each entry
#         should be limited to about 25 routes.
#         (25 routes @ 50 char/route = 1250 characters.
#         Add RADIUS overhead and each entry will still fit
#         into one Ethernet packet.)
#
```

```
#  outdial users:The static routes specified in the route-n entries
#         can contain a name. The name is used to look up
#         a RADIUS pseudo-user to obtain out-dial information.
#         At this time separate entries are required for
#         both in-dial and out-dial users.
#         It is recommended (but not required) that user
#         X have an out-dial entry named X-out. See the
#         examples below.

#  B A N N E R   P S E U D O - U S E R
#
bannerPassword = "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 = " ",
   Reply-Message = "There can be up to 10 Ascend-Host-Info entries",
   Reply-Message = "in this profile. Each entry contains an IP
address",
   Reply-Message = "to Telnet to and up to 31 characters of text",
   Reply-Message = "describing the host. The text will be assigned",
   Reply-Message = "a number. When the number is selected a telnet",
   Reply-Message = "session to the ip address will be initiated.",
   Ascend-Host-Info = "1.2.3.4 a host name or phrase",
   Ascend-Host-Info = "1.2.3.5 another host",
   Ascend-Host-Info = "5.4.3.2 the last host"

#  A D D R E S S - P O O L S   P S E U D O - U S E R S
#
#  The user pools-xxx (where xxx is the name of the requesting
#  unit) returns the pools assigned to that unit.
#
#  The Ascend-IP-Pool-Definition attribute is used to define
#  an address pool. The format of the attribute is a string
#  containing:
#
#     x h.h.h.h n
```

```
#  where:
#
#     x  Pool number. A pool is selected in a user
#        profile by putting its pool number in an
#        Ascend-Assign-IP-Pool attribute.
#
#     h.h.h.hBase ip address. This is the first address in
#        the pool.
#
#     n  Maximum number of entries from the pool.
#
pools-xxxPassword = "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"

#  R O U T E - n   P S E U D O - U S E R S
#
#  The format of a route entry is a string containing
#
#     h.h.h.h/nn g.g.g.g m p name
#
#  where:
#
#     h.h.h.hIP address of destination host or network
#     /nn    Optional netmask indicator.
#     g.g.g.gIP address of the gateway
#     m      Metric (number of hops) for this route.
#     p      Optional Y or Yes if route is private
#     name   Optional route name (required if dialing out)
#
#  The presence of an optional field requires ALL previous fields
#  to be present. Routes are ignored if there is no place to store
#  them in the passed information structure.
#
```

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

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

#  O U T D I A L   P S E U D O - U S E R S
#
#  These profiles represent standard RADIUS
#  users, but contain extra attributes associated with outgoing
#  calls. Be sure that each is protected by adding the
#  User-Service attribute on the password line.
#

#

permconn-k-1 Password = "ascend" , User-Service = Dialout-Framed-User
    Framed-Protocol = FR,
    Framed-Address = 198.5.249.46,
    Framed-Netmask = 255.255.255.240,
    Framed-Routing = None,
    Ascend-Route-IP = Route-IP-Yes,
    Ascend-Metric = 7,
    Ascend-FR-DLCI = 109,
    Ascend-FR-Profile-Name = "fr1",
    Ascend-Idle-Limit = 130,
    Framed-MTU = 1524,
    Ascend-PRI-Number-Type = National-Number,
    Ascend-Force-56 = Force-56-No,
    Ascend-Data-Svc = Switched-56KR,
    Ascend-Call-Type = Nailed
```

```
permconn-k-2 Password = "ascend" , User-Service = Dialout-Framed-User
    Framed-Protocol = FR,
    Framed-Address = 198.5.249.164,
    Framed-Netmask = 255.255.255.240,
    Framed-Routing = None,
    Ascend-Route-IP = Route-IP-Yes,
    Ascend-Metric = 7,
    Ascend-FR-DLCI = 105,
    Ascend-FR-Profile-Name = "fr1",
    Ascend-Idle-Limit = 130,
    Framed-MTU = 1524,
    Ascend-PRI-Number-Type = National-Number,
    Ascend-Force-56 = Force-56-No,
    Ascend-Data-Svc = Switched-56KR,
    Ascend-Call-Type = Nailed

permconn-k-3 Password = "ascend" , User-Service = Dialout-Framed-User
    Framed-Protocol = FR,
    Framed-Address = 199.6.43.141,
    Framed-Netmask = 255.255.255.0,
    Framed-Routing = None,
    Ascend-Route-IP = Route-IP-Yes,
    Ascend-Metric = 7,
    Ascend-FR-DLCI = 114,
    Ascend-FR-Profile-Name = "fr1",
    Ascend-Idle-Limit = 130,
    Framed-MTU = 1524,
    Ascend-PRI-Number-Type = National-Number,
    Ascend-Force-56 = Force-56-No,
    Ascend-Data-Svc = Switched-56KR,
    Ascend-Call-Type = Nailed
```

```
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,
    Framed-Route = "10.5.0.0/24 10.0.100.1 1",
    Ascend-Idle-Limit = 30,
    Ascend-Send-Auth = Send-Auth-PAP,
    Ascend-Send-Secret = "passwrd1"

#   Filters (an Ascend extension to RADIUS)
#
#   Two string fields have been defined in the RADIUS dictionary,
#   Ascend-Data-Filter and Ascend-Call-Filter. The Ascend-Data-Filter
#   defines a data/routing filter. An Ascend-Call-Filter defines a
#   "place a call and/or keep a call active" filter.
#
#   Keywords are not case sensitive. In the following definitions
#   [ ... ] indicates an optional element.
#
#   IP Filters:
#
#   "ip dir action [ dstip n.n.n.n/nn ] [ srcip n.n.n.n/nn ]
#       [ proto [ dstport cmp value ] [ srcport cmp value ] [ est ] ]"
#
#   where:
#
#   ip:    The keyword ip. This keyword indicates an IP filter.
#
#   dir:   Filter direction, either IN or OUT.
#          IN filters packets coming into the Ascend box.
#          OUT filters packets going out of the Ascend box.
#
#   action:What to do with a packet that matches the filter,
#          either FORWARD or DROP.
#
```

```
#  dstip: The optional destination IP. If it is not present, the
#         filter will match any IP address. If a netmask
#         portion (/nn) of the address is present, the unit will
#         only compare the masked bits. The keyword "dstip"
#         must proceed the IP address.
#
#  srcip: The optional source IP. If it is not present, the
#         filter will match any IP address. If a netmask
#         portion (/nn) of the address is present, the unit will
#         only compare the masked bits. The keyword "srcip"
#         must proceed the IP address.
#
#
#  proto: The optional protocol. It may be specified as either
#         a name or a number. The supported names are
#         icmp(1), tcp(6), udp(17), ospf(89).
#
#  dstport:Only valid when proto is tcp(6) or udp(17). 'cmp'
#         can have the value '<', '=', '>', or '!='. The
#         value can be entered as a number or a name.
#         Supported names are ftp-data(20), ftp(21),
#         telnet(23), smpt(25), nameserver(42), domain(53),
#         tftp(69), gopher(70), finger(79), www(80),
#         kerberos(88), hostname(101), nntp(119), ntp(123),
#         exec(512), login(513), cmd(514), and talk(517).
#         The field matches any port when not present. The keyword
#         "dstport" must proceed 'cmp'.
#
#  srcport:Only valid when proto is tcp(6) or udp(17). 'cmp'
#         can have the value '<', '=', '>', or '!='. The
#         value can be entered as a number or a name.
#         Supported names are ftp-data(20), ftp(21),
#         telnet(23), smpt(25), nameserver(42), domain(53),
#         tftp(69), gopher(70), finger(79), www(80),
#         kerberos(88), hostname(101), nntp(119), ntp(123),
#         exec(512), login(513), cmd(514), and talk(517).
#         The field matches any port when not present. The keyword
#         "srcport" must proceed 'cmp'.
#
```

```
#  est:   The optional keyword EST. It is only valid when the proto
#         field is tcp(6).
#
#  GENERIC filters:
#
#
#  "generic dir action offset mask value [ more ]"
#
#  where:
#
#  generic:The keyword "generic". This keyword is used to indicate a
#              generic filter.
#
#  dir:   Filter direction, either IN or OUT.
#         IN filters packets coming into the Ascend box.
#         OUT filters packets going out of the Ascend box.
#
#  action:What to do with a packet that matches the filter.
#         (either FORWARD or DROP).
#
#  offset:A number that specifies an offset into a frame.
#
#  mask:  A hexadecimal mask of bits to compare. A one bit
#         in the mask indicates a bit to compare. Zero bits
#         are ignored. The length of the mask specifies the
#         length of the comparison. The mask may not exceed
#         6 bytes (12 hexadecimal digits).
#
#  value: The value to compare with the masked data at the offset
#         in the packet. Note: The length of the value must
#         be the same as the mask or the entry will be
#         ignored.
#
#  comparison:'==' or '!=', for Equal or NotEqual. No
#         comparison field means Equal.
#
```

```
#  more:  The optional keyword MORE. If present, the keyword
#         specifies that the next filter entry is to be applied to
#         the current packet. The <dir> and <action> of the
#         next entry must be the same as the <dir> and <action>
#         of the current entry or the MORE flag will be
#         ignored.
#
#  In the following example, the profile allows IP and ARP output,
#  but drop all other packets.
#
inu-out Password = "ascend", User-Service = Dialout-Framed-User
    User-Name = "inu",
    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"


#  C L I D   A U T H E N T I C A T I O N
#
#  CLID entries have a "name" set to the incoming phone number and
#  and a constant password of "Ascend-CLID". The real name should
#  be placed in the profile.
#
5551212Password = "Ascend-CLID", User-Service = Dialout-Framed-User
    User-Name = "real-user-name",
    Framed-Protocol = PPP,
    Framed-Address = 10.10.0.1,
    Framed-Address = 255.255.255.0
```

```
#  D E F A U L T S
#
#  Note: Only one of these may be used, and it must be
#  the last entry in the file.
#
#  The following entry allows a terminal-server user to log in using a
#  UNIX account name and password.
#
DEFAULTPassword = "UNIX"
   User-Service = Login-User,
   Login-Service = Telnet

#  The following entry allows a PPP user to log in using an account
#  name and SafeWord dynamic password.
#
#DEFAULTPassword = "SAFEWORD"
#  User-Service = Framed-User,
#  Framed-Protocol = PPP,
#  Framed-Address = 10.20.0.1,
#  Framed-Netmask = 255.255.255.0
```

Index

A

B

C

D

E

F

G

I

L

M

N

O

P

R

S

T

U

V

W