MAX TNT RADIUS Guide

Ascend Communications, Inc.
Part Number: 7820-0480-003
For Software Version 1.3A
September 26, 1997

Ascend Customer Service

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

How to contact Ascend Customer Service

If you need Technical Assistance, contact Ascend in one of the following ways:

Telephone in the United States	800-ASCEND-4 (800-272-3634)
Telephone outside the United States	510-769-8027 (800-697-4772)
UK	(+33) 492 96 5671
Germany/Austria/Switzerland	(+33) 492 96 5672
France	(+33) 492 96 5673
Benelux	(+33) 492 96 5674
Spain/Portugal	(+33) 492 96 5675
Italy	(+33) 492 96 5676
Scandinavia	(+33) 492 96 5677
Middle East and Africa	(+33) 492 96 5679
Email	support@ascend.com
Email (outside US)	EMEAsupport@ascend.com
Facsimile (FAX)	510-814-2312
Customer Support BBS by modem	510-814-2302

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

Ascend Communications
1701 Harbor Bay Parkway
Alameda, CA 94502

Need information about new features and products?

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

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

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

- For software upgrades, release notes, and addenda to this manual, visit our FTP site:

  `ftp.ascend.com`

Contents

Introduction

1

This introduction covers the following topics:

What is in this guide

This guide describes how to install and start up the RADIUS daemon, and provides detailed information about how to set up authentication, WAN connections, routing and bridging configurations, ATMP tunnels, and accounting records in RADIUS. It assumes that you have already installed the MAX TNT hardware, set up call routing, configured the Ethernet ports, and configured T1 PRI or E1 PRI lines. For details about carrying out these tasks, see the *MAX TNT Hardware Installation Guide* and the *MAX TNT Network Guide*.

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. The 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 multi-link PPP
- Connection cost management and accounting
- Modems
- Frame relay
- IP routing
- DNS
- OSPF routing (if applicable)
- Multicast (if applicable)
- Packet structure and formats (for defining filters)
- Network security

Related publications

Additional information is available in the other guides in the MAX TNT documentation set. If you need more background information than these guides provide, many external references are readily available on the Web or in technical bookstores. You'll find a partial list of such references below.

MAX TNT documentation set

The MAX TNT documentation set consists of the following manuals:

- *The Ascend 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). Describes how to configure RADIUS for authentication, network connectivity, and accounting.
- *MAX TNT Reference Guide*. An alphabetic reference to all MAX TNT profiles, parameters, and commands.

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 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 1638: *PPP Bridging Control Protocol (BCP)*
- RFC 1618: *PPP over ISDN*
- RFC 1332: *The PPP Internet Protocol Control Protocol (IPCP)*

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 2030: *Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI*
- 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.

Documentation conventions

This section shows the documentation conventions used in this guide.

Table 1-1. Documentation conventions

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

Table 1-1. Documentation conventions (continued)

Convention	Meaning
|	Separates command choices that are mutually exclusive.
>	Points to the next level in the path to a parameter. The parameter that follows the angle bracket is one of the options that appears when you select the parameter that precedes the angle bracket.
Key1-Key2	Represents a combination keystroke. To enter a combination keystroke, press the first key and hold it down while you press one or more other keys. Release all the keys at the same time. (For example, Ctrl-H means hold down the Control key and press the H key.)
Press Enter	Means press the Enter, or Return, key or its equivalent on your computer.
Note:	Introduces important additional information.

Getting Acquainted with RADIUS

2

This chapter introduces RADIUS authentication and accounting, and provides an overview of the files that the RADIUS server uses. The chapter consists of the following sections:

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 for an incoming call
- Routing and bridging 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, bridging, 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 bridge/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 (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 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 2-1., the RADIUS server performs both authentication and accounting.

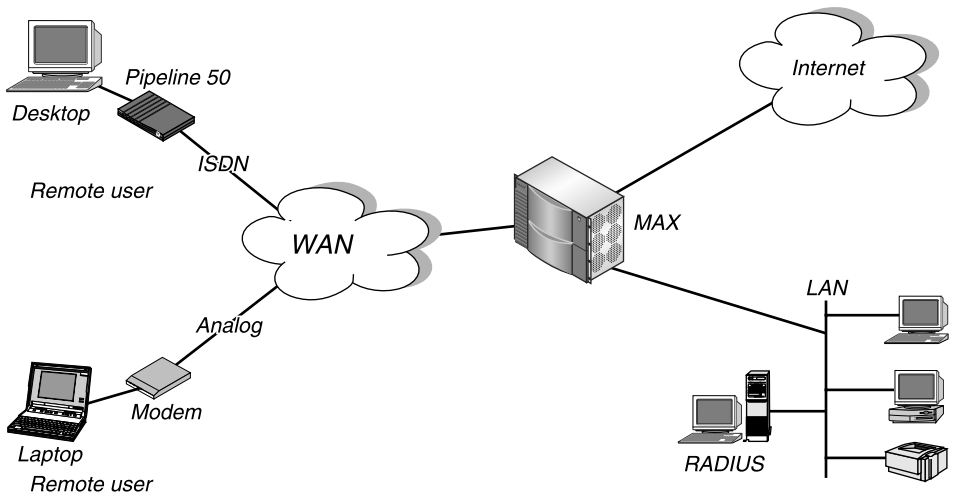


Figure 2-1. Simple RADIUS authentication and accounting

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

RADIUS authentication and accounting with a backup server

In Figure 2-2., 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.

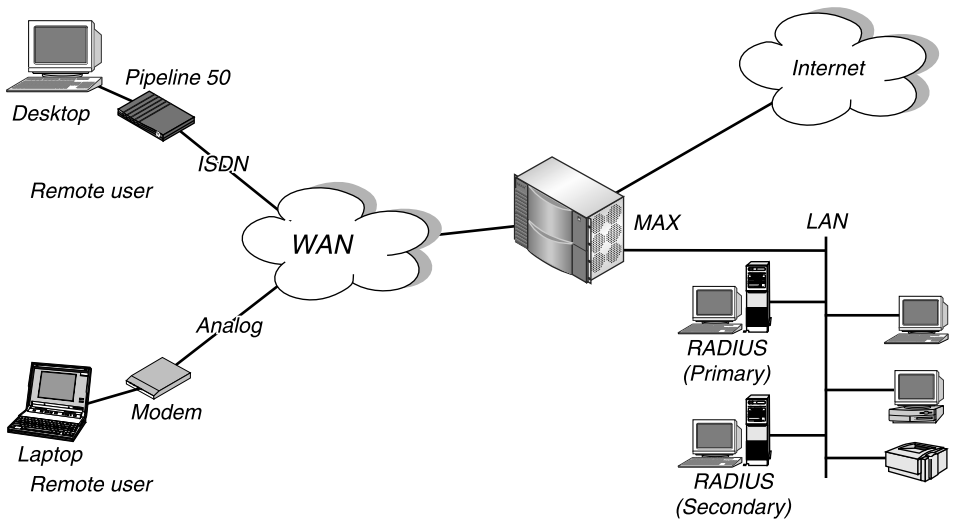


Figure 2-2. RADIUS authentication and accounting with a backup server

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 2-3. illustrates an environment that includes an Ascend Pipeline as the calling unit, an NAS (the MAX TNT), a RADIUS server, and an external authentication server.

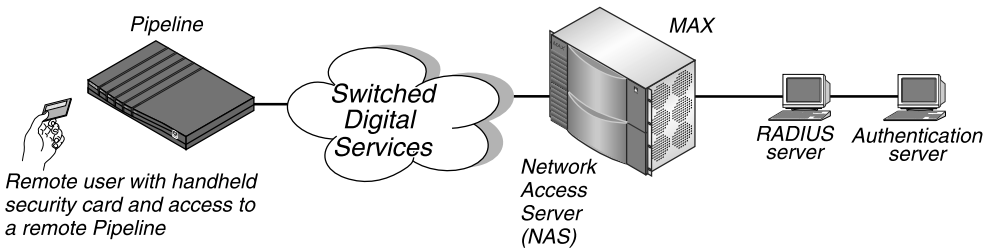


Figure 2-3. RADIUS with an external token-card server

For complete information about configuring RADIUS to work with token-card authentication servers, see "Setting up token-card authentication" on page 4-33.

Using RADIUS to sign up new customers

In Figure 2-4., the server 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.

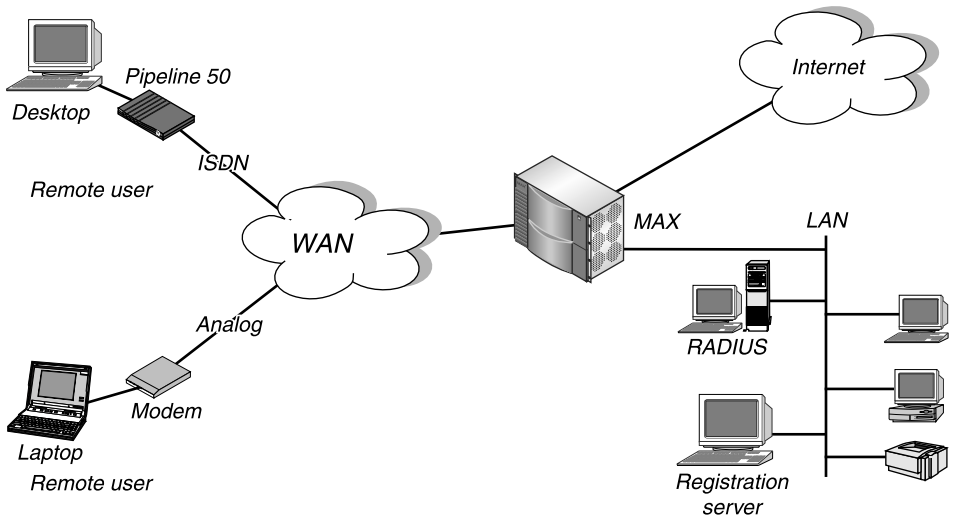


Figure 2-4. Using RADIUS to sign up new customers

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 2-1.

Table 2-1. 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 3-11.

Table 2-1. RADIUS files (continued)

File name	Default location	Description
`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 3-13.
`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 "Dictionary file" on page 2-7.
`clients`	`/etc/raddb`	File that identifies each client that can send requests to the RADIUS server. For overview information about the `clients` file, see "Clients file" on page 2-7. For details about setting up the `clients` file, see "Creating and configuring the clients file" on page 3-4.
`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 "Users file" on page 2-8. For details about setting up the `users` file, see Chapter 4, "Setting Up RADIUS Authentication" and all succeeding chapters in this guide.
`logfile`	`/etc/raddb`	File containing error messages. You must create this file yourself.
`detail`	`/usr/adm/`*`NAS-name`*`/radacct`	File containing accounting records.

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 2-2.

Table 2-2. Dictionary file format

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

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
```

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, bridging entries, and other types of data.

Note: Every attribute name and value is case sensitive. For more complete information on setting up the `users` file, see "Using the RADIUS interface" on page 2-11.

Overview of RADIUS packet formats

Each RADIUS packet consists of the fields listed in Table 2-3.

Table 2-3. RADIUS packet fields

Element	Description
Code (8 bits)	Specifies the packet type. For a list of packet types, see Table 2-4 on page 2-9.
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.
Authenticator (16 bytes)	Authenticates packets between the NAS and the authentication server. The NAS and the authentication server share a secret. The system uses this shared secret with the authenticator field to provide password encryption and packet authentication. The shared secret resides in the `clients` file on the authentication host. The MAX TNT checks all authentication and accounting packets to ensure that they come from known sources. The checking 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.

Table 2-3. RADIUS packet fields (continued)

Element	Description
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 2-4 lists the packet types that can appear in the code field.

Table 2-4. 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.
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-RequestS	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.

Table 2-4. Code field packet types (continued)

Number	Name	Description
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.
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.
31	Ascend-Terminate-Session	Response from the RADIUS server informing the MAX TNT that it should terminate the session and display the message sent in the packet.
32	Ascend-Password-Expired	Response from 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.

Table 2-4. Code field packet types (continued)

Number	Name	Description
41	Disconnect-Request-ACKed	Message the MAX TNT sends to the client if it found at least one session to disconnect.
42	Disconnect-Request-NAKed	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 bridging/routing session.
44	Change-Filter-Request-ACKed	Message the MAX TNT sends if it found at least one bridging/routing session for which filters could be changed.
45	Change-Filter-Request-NAKed	Message the MAX TNT sends if it could not find a bridging/routing session for which filters could be changed.

Using the RADIUS interface

To set up RADIUS, you must configure attributes in the `users` file. A `users` file can contain comment lines, user profiles, pseudo-user profiles, and blank lines. Table 2-5 lists each element.

Table 2-5. Users file elements

Element	Description
Comment line	Begins with the # character at column one, followed by text that extends to the end of the line. You can embed a comment line anywhere in a profile.
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.

Table 2-5. Users file elements (continued)

Element	Description
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 pre-defined 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
```

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

3

This chapter, which describes how to install and start the RADIUS daemon, consists of the following sections:

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.
- A TCP/IP connection between the RADIUS server and the MAX TNT.

Note: If you do use the Ascend RADIUS daemon, the MAX TNT is limited to 256 session IDs. If all session IDs are used up, the MAX TNT cannot answer a call. If you are using the Ascend RADIUS daemon, the MAX TNT is not limited to 256 session IDs, and you need not concern yourself with using up available session IDs.

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 Configuration 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 3-3.
- Configure the MAX TNT to use RADIUS, as described in “Configuring the MAX TNT to use the RADIUS server” on page 3-6.
- Start up the RADIUS daemon, as described in “Starting the RADIUS daemon” on page 3-11.

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 3-5.)
- 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 3-9.)

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 "Dictionary file" on page 2-7.

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 "Users file" on page 2-8. 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 "Configuring IP address pools shared by several MAX TNT units" on page 9-12. For information about configuring per-unit IP address pools, see "Configuring IP address pools for a single MAX TNT" on page 9-11.

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. Some 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 13, "Setting Up RADIUS Accounting.".

Performing the required configuration steps

When configuring the MAX TNT to use RADIUS, you must specify the type of authentication in use, the IP address of at least one RADIUS server, the UDP port number for the daemon, and the 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 3-8.

To specify settings required for RADIUS operation:

1. In the External-Auth profile, set the Auth-Type parameter to RADIUS or RADIUS-Logout. If you set Auth-Type=RADIUS-Logout, RADIUS keeps track of session logouts.
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:

- 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
- Enable the MAX TNT to recognize a token-card authentication server
- Enable the MAX TNT to use the APP Server utility

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

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 13-7.)

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 "Setting up CLID authentication" on page 4-20.)

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 If Auth-Type=RADIUS-Logout, 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 you do not require a RADIUS user profile to specify the User-Service (6) and Framed-Protocol (7) attributes in order for a user to access PPP, set Auth-Send67=No.

Specifying the duration of a RADIUS timeout

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.

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. 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 the MAX TNT to recognize a token-card server

If you plan to use an external server with token cards, you must configure the MAX TNT to recognize the server. Proceed as follows:

1. Set the Password Host parameter to the IP address of the token-card server on the remote network.
2. Set the Password Port parameter to the User Datagram Protocol (UDP) port number that the server indicated by Password Host is monitoring.
3. Set Password Server=Yes to specify that callers use token-card authentication rather than terminal-server authentication.

Configuring the MAX TNT to recognize the APP server utility

To allow users to supply token passwords from a PC or UNIX host on the local network, you must configure the MAX TNT to communicate with the APP Server utility on that host. To set up the MAX TNT to communicate with the APP Server utility:

1. Set APP Server=Yes to enable the MAX TNT to communicate password challenges to the host running the APP Server utility.
2. Set the APP Host parameter to the IP address of the host running the APP Server utility. If the host obtains its address at boot time from a BOOTP or DHCP server, or if it has no IP address, you can specify the IP broadcast address (255.255.255.255).
3. Set the APP Port parameter to the UDP port to use for communicating with the host running the APP Server.
4. If you modified the value of the APP Port parameter from its default of 7001, specify the new UDP port number in the APP Server utility (DOS), the WIN.INI file (Windows), or the `/etc/services` file (UNIX).

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 “Setting up disconnects” on page 5-31. For detailed information about specifying filter changes in RADIUS, see “Setting up filter changes” on page 12-11.)

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 make at least 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 clients and the RADIUS server. 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 a number between 1 and 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.

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 3-1 lists each argument.

Table 3-1. 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 you do not specify the -A argument.
-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.

Table 3-1. List of radiusd arguments (continued)

Argument	Description
-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 the following command:

```
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]`

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

Table 3-2 list each argument for the `builddbm` command.

Table 3-2. 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 3-11, 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.

Setting Up RADIUS Authentication

4

This chapter discusses how to configure the RADIUS server to authenticate MAX TNT clients. It consists of the following sections:

Before you begin

Before you begin configuring RADIUS authentication, you must set up the MAX TNT to require a profile for authentication. In addition, depending on the needs of your site, you can optionally configure the MAX TNT to:

- Check for a RADIUS profile before a local Connection profile.
- Enable Calling-Line ID (CLID) or called-number authentication.
- Support token-card authentication.

Requiring the MAX TNT to use a profile for authentication

To require a profile for authentication, set Profiles-Required=Yes in the Answer-Defaults profile at the MAX TNT configuration interface.

Configuring the MAX TNT to check for a RADIUS profile first

If you want the MAX TNT to check for a RADIUS profile before looking for a local Connection Profile, set Local-Profiles-First=No in the External-Auth profile at the MAX TNT configuration interface.

Enabling Calling-Line ID (CLID) or called-number authentication

If you plan to set up Calling-Line ID (CLID) or called-number authentication in RADIUS, you must make certain required settings at the MAX TNT configuration interface:

- When Signaling-Mode=E1-Chinese-Signaling, you must set Caller-ID=Get-Caller-ID in the Line-Interface subprofile of the E1 profile. For detailed information about other MAX TNT settings for CLID authentication, see “Configuring CLID authentication at the MAX TNT interface” on page 4-21.
- For detailed information about MAX TNT settings for called-number authentication, see “Configuring called-number authentication at the MAX TNT interface” on page 4-29.

Supporting token-card authentication

If you plan to use token-card authentication, you must:

- Set up the MAX TNT to use the token-card server. For detailed information, see “Configuring the MAX TNT to recognize a token-card server” on page 3-8.
- Set up the MAX TNT to use the APP Server utility. For detailed information, see “Configuring the MAX TNT to recognize the APP server utility” on page 3-8.

Overview of RADIUS authentication

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

By default, when you require a profile for authentication, the MAX TNT always checks for a Connection profile. If a Connection profile does not exist, the MAX TNT checks for a remote RADIUS, TACACS, or TACACS+ profile.

However, you can change this default by setting Local-Profiles-First=No in the External-Auth profile. When Local-Profiles-First=No, the MAX TNT first looks for a remote profile. If it cannot find one, the MAX TNT looks for a local Connection profile.

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

1 Before the MAX TNT answers a call, it determines whether or not the Answer-Defaults profile requires Calling-Line ID (CLID) authentication, called-number authentication, or both.

The CLID is the phone number of the calling device, which is not always provided by the WAN carrier. When the profile requires CLID authentication, the caller's phone number must match a phone number specified in a local Connection profile or RADIUS user profile.

The called-party number is the phone number the remote device called to connect to the MAX TNT, but without a trunk group or dialing prefix specification. This number is always available if specified in a profile. When the profile requires called-number authentication, the number called must match a called-party number in a local Connection profile or RADIUS user profile.

2 If the profile requires CLID authentication (CLID-Auth-Mode=CLID-Require in the Answer-Defaults profile), called-number authentication (CLID-Auth-Mode=DNIS-Require in the Answer-Defaults profile), or both (CLID-Auth-Mode=CLID-and-DNIS-Req in the Answer-Defaults profile), the MAX TNT first looks for a matching phone number in a local Connection profile.

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

3 If the profile does not require CLID or called-number authentication, or if the MAX TNT finds a matching phone number in a local Connection profile or RADIUS user profile, it answers the call.

4. The MAX TNT routes the call.

5 The MAX TNT checks its other Answer-Defaults profile settings.

6 If the Answer-Defaults profile specifies the type of link encapsulation the call uses, the MAX TNT continues checking Answer-Defaults parameters.

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

7 The MAX TNT checks the value of the Profiles-Required parameter in the Answer-Defaults profile.

If Profiles-Required=Yes, the MAX TNT must find a Connection profile, RADIUS user profile, TACACS profile, or TACACS+ profile to authenticate the call.

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

If Receive-Auth-Mode=PAP-PPP-Auth, CHAP-PPP-Auth, MS-CHAP-PPP-Auth, or Any-PPP-Auth, the MAX TNT requires a matching name and password as a condition of authentication.

9. For IP routing connections, the MAX TNT looks for a Connection profile that matches the client's IP address.

If it cannot find a Connection Profile, it looks for a RADIUS, TACACS, or TACACS+ profile. The MAX TNT then uses the name and password in the profile to authenticate the session. If the MAX TNT does not find a matching IP address (perhaps because the MAX TNT assigns addresses dynamically), it searches for a profile that matches the name and password that the dial-in client presents.

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

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

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

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

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

12 If name and password authentication is not required (Receive-Auth-Mode=No-PPP-Auth), the MAX TNT can use the IP address specified by the Connection profile to match IP-routed PPP calls.

13 If the Answer-Defaults profile does not require a profile (Profiles-Required=No), the MAX TNT uses the Answer-Defaults parameters to build the connection.

14. After building the session, the MAX TNT passes the data stream to the appropriate software module or host.

Overview of RADIUS authentication tasks

All RADIUS authentication tasks are optional, and depend upon your security needs. Most configurations use name and password authentication, as described in “Setting up name and password authentication” on page 4-5. If you require callers to supply a name and password, you must specify the authentication protocol to use for incoming calls. For detailed information, see “Specifying an access protocol for incoming calls” on page 4-15.

Other tasks include:

- Specifying whether multiple callers can use the same RADIUS user profile. (For detailed information, see “Specifying whether multiple callers can use a profile” on page 4-15.)
- Requesting an access protocol for calls that the MAX TNT dials. (For detailed information, see “Requesting an access protocol for outgoing calls” on page 4-17.)
- Setting up the MAX TNT to call back a dial-in user. (For detailed information, see “Setting up the MAX TNT for callback” on page 4-19.)
- Setting up authentication by Calling-Line ID. (For detailed information, see “Setting up CLID authentication” on page 4-20.)
- Setting up authentication by called number. (For detailed information, see “Setting up called-number authentication” on page 4-28.)
- Setting up authentication by means of an external token-card server. (For detailed information, see “Setting up token-card authentication” on page 4-33.)
- Setting up terminal-server authentication. (For detailed information, see “Setting up authentication for terminal-server calls” on page 4-41.)

Setting up name and password authentication

Name and password authentication is the simplest form of authentication. If you plan to use PAP, CHAP, or MS-CHAP authentication, you must specify a name and password in a RADIUS user profile. Carry out the following tasks:

- Specify the name of the remote user or device with the User-Name (1) attribute.
- Specify the password with the Password (2) attribute.

Depending on your needs, you also have the option of configuring:

- Password expiration
- The MAX TNT unit’s login name and password
- Pseudo-user profiles

Specifying a user name

The user name must be the first value on the first line of a RADIUS profile. Specify an alphanumeric string of up to 252 characters. You need not specify the `User-Name=` portion of the setting. Rather, you can simply specify the user name itself. The default value is null. Because the MAX TNT uses the first matching name for an incoming caller, you must not specify a duplicate user name in any RADIUS user profile.

Using the caller's name

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

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

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

Using the Default keyword

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

For example, the following first line of a profile enables a terminal-server user to log in with his or her UNIX account name or password:

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

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

Specifying a password

A user profile must contain an encrypted password to authenticate the caller. Specify a password by means of the Password attribute. The password must appear on the first line of the user profile, directly after the user name, and must be an alphanumeric string of up to 252 characters. The default value is null.

Table 4-1 lists the specifications you can make for the Password attribute.

Table 4-1. Password specifications

Type	Description
Static	A static password represents a string the user must enter to gain access to the MAX TNT. For example: **`Mark Password="pwd"`**
UNIX	By setting the Password attribute to **`"UNIX"`**, you can request validation from the `/etc/password` file on the UNIX host. Setting the password to **`"UNIX"`** provides authentication through the normal UNIX authentication procedure. For example: **`Mark Password="UNIX"`** **Note:** You cannot specify a UNIX password with Challenge Handshake Authentication Protocol (CHAP) authentication.

Table 4-1. Password specifications (continued)

Type	Description
SAFEWORD	By setting the Password attribute to **"SAFEWORD"**, you can request validation from an Enigma Logic SafeWord server. For example: **Mark Password="SAFEWORD"** For complete information on setting up token-card authentication, see "Setting up token-card authentication" on page 4-33.
ACE	By setting the Password attribute to **"ACE"**, you can request validation from a Security Dynamics ACE server. For example: **Mark Password="ACE"** For complete information on setting up token-card authentication, see "Setting up token-card authentication" on page 4-33.

Configuring password expiration

The Ascend RADIUS daemon supports password aging and expiration, and includes a method for enabling dial-in users to replace expired passwords. This section contains the following information on password expiration:

- Conditions for replacing expired passwords
- Setting the password expiration attributes
- Changing a non-expired password
- Changing an expired password

Conditions for replacing expired passwords

When the server is running the Ascend RADIUS daemon, and you have configured the daemon for expired passwords, a dial-in user can replace an expired password that meets all the following conditions:

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

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

  A user who dials in as an IP router, IP bridge, host-to-bridge, or bridge cannot replace an expired password.

Setting the password expiration attributes

The Ascend RADIUS daemon uses the attributes listed in Table 4-2 to support password aging and expiration.

Table 4-2. Password expiration attributes

Attribute	Specifies	Possible values
Ascend-PW-Expiration (21)	Expiration date for the user's password.	A date consisting of a month, day, and year specification. The default is no expiration date.
Ascend-PW-Lifetime (208)	Number of days that a password is valid.	Integer between 0 and 65535. The default is the value of Lifetime-In-Days from the Ascend dictionary.

To set up password expiration, you specify the Ascend-PW-Expiration attribute on the first line of the user profile. Then, you specify the Ascend-PW-Lifetime attribute on any line other than the first one.

Ascend-PW-Expiration

Ascend-PW-Expiration 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. Your specification might look like this one:

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

Ascend-PW-Lifetime

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

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

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

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

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

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

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

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

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

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

The password expires on January 15, 1997.

If Ascend-PW-Lifetime is absent, the value of Lifetime-In-Days determines the password duration. The Lifetime-In-Days value in the RADIUS dictionary is the default value for Ascend-PW-Lifetime. By default, Lifetime-In-Days is 0 (zero). This value means that passwords do not expire.

Note: If you run the Ascend RADIUS daemon with a flat ASCII file, RADIUS accepts a user's replacement for an expired password only if you start the daemon with the -p argument. For details, see "Running the daemon with a flat ASCII users file" on page 3-11. If you run the daemon in DBM mode, RADIUS accepts a user's replacement for an expired password if you specify the -p argument, but does not recognize the new password until you rebuild the `users` file database by running `builddbm` again. For information, see "Creating the DBM database" on page 3-13.

Changing a non-expired password

The MAX TNT supports a Password command that enables a RADIUS-authenticated terminal-server user to change his or her password. To change a password:

1. Enable password expiration in the user profile, following the instructions in "Configuring password expiration" on page 4-7.

   When you change a non-expired password, the MAX TNT uses the same mechanism that enables you to enter a new password when an older one has expired.

2. At the terminal-server prompt, enter the Password command:

   ```
   ascend% Password
   ```

   The following prompts appear:

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

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

4. At the `Enter new password` and `Re-type new password` prompts, enter the new password. The new password cannot be null, and must differ from the old password.

If the password change is successful, the following messages appears:

```
Password Updated
```

If the update fails for any reason, the following message appears:

```
Password NOT Changed
```

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

Changing an expired password

When a user attempts to establish a terminal-server connection with an expired password, the following events take place:

1. The MAX TNT informs the user that the authentication failed because the password has expired.
2. The MAX TNT prompts the user for a new password.

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

   If the new password is valid, the MAX TNT asks the user to re-enter it for confirmation. If the two entries do not match, the MAX TNT prompts again for a new password.
3. After receiving a valid confirmation of the new password, the MAX TNT contacts the RADIUS server for acceptance of the new password.

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

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

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

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

Configuring the MAX TNT unit's name and password for outgoing calls

When the MAX TNT places an outgoing call, it identifies itself by a login name and password. You have the option of overriding the system's default values by specifying a name and password in RADIUS. Table 4-3 lists the MAX TNT unit's login name and password attributes, as well as the other attributes necessary, as a minimum, for an outgoing call.

Table 4-3. MAX TNT unit's login name and password attributes

Attribute	Description	Possible values
Ascend-Authen-Alias (203)	Specifies the MAX TNT unit's login name.	Text string of up to 16 characters. The default is the value of the Name parameter in the System profile.
Ascend-Send-Passwd (232)	Specifies the password that the MAX TNT sends to the remote end of a connection on outgoing calls.	Text string containing up to 20 characters. The default value is null. If you do not specify a password in RADIUS, the MAX TNT uses the value of Send-Password in the local Connection profile.
Ascend-Send-Secret (214)	When used in place of the Ascend-Send-Passwd attribute, directs the system to encrypt the password when sending it between the RADIUS server and the MAX TNT on outgoing calls.	Text string containing up to 20 characters. The default value is null. If you do not specify a password in RADIUS, the MAX TNT uses the value of Send-Password in the local Connection profile.
Password (2)	Specifies the user's password.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Name (1)	Specifies the name of the remote user or device.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Service (6)	Specifies whether the link can use framed or unframed services.	Login-User (1) Framed-User (2) Dialout-Framed-User (5) By default, the MAX TNT does not restrict the services that a link can use.

To configure the MAX TNT unit's name and password for outgoing calls:

1. On the first line of the profile, set the User-Name attribute to the name of the device that will receive outgoing calls, appending **`-Out`** to the user name.
2. Set Password= "ascend".
3. Set User-Service=Dialout-Framed-User.
4. On the second line of the user profile, set the User-Name attribute to the name of the device that will receive outgoing calls.
5. Set the Ascend-Authen-Alias attribute to the MAX TNT unit's login name.
6. Set the Ascend-Send-Passwd or Ascend-Send-Secret attribute to the MAX TNT unit's password. (Use Ascend-Send-Passwd only if your version of the MAX TNT does not support Ascend-Send-Secret.)

   If the value you specify for Ascend-Send-Secret or Ascend-Send-Password does not match the value of the remote end's Ascend-Receive-Secret attribute (in a RADIUS user profile) or Recv-Password parameter (in a Connection profile), the remote system rejects the call.

Example of configuring the MAX TNT unit's login name and password

The following example uses the Ascend-Authen-Alias and Ascend-Send-Secret attributes 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
```

Configuring the name and password in 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, bridging entries, 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 4-4 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 on 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).
- ***ID*** is a unique string identifying a Frame Relay profile. You must assign IDs in sequence, starting with 1, with no missing numbers. If the numbers are not in sequence, the MAX TNT cannot retrieve the profiles correctly.
- ***num*** is a number in a sequential series, starting at 1, that identifies a routing or bridge entry.

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

Table 4-4. 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 “Setting up an outgoing PPP, MP, or MP+ connection” on page 5-9.
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 “Setting up the message text and a list of hosts” on page 6-10.
Frame Relay profile	**`frdlink-`*`name`*`-`*`ID`*` Password="ascend", User-Service=Dialout-Framed-User`** For complete information, see “Setting up the logical link to a Frame Relay switch” on page 7-3.
Frame Relay user profile	**`permconn-`*`name`*`-`*`ID`*` Password="ascend", User-Service=Dialout-Framed-User`** For complete information, see “Setting up Frame Relay user connections” on page 7-11.

Table 4-4. First-line configuration of pseudo-user profiles (continued)

Element configured	First-line specification
IP address pools	For a configuration specific to a single MAX TNT unit: **`pools-`*`name`* `Password="ascend", User-Service= Dialout-Framed-User`** For a configuration used by several MAX TNT units: **`global-pool-`*`name`* `Password="ascend", User-Service= Dialout-Framed-User`** To store the IP addresses of Ascend units that can use global IP pools, and the IP address of the host running `radipad`: **`radipa-hosts Password="ascend", User-Service= Dialout-Framed-User`** For complete information, see “Defining a pool of addresses for dynamic assignment” on page 9-9.
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 “Setting up static IP routes” on page 9-17.
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 “Setting up static IPX routes” on page 10-5.
Bridging entries	**`bridge-`*`name-num`* `Password="ascend", User-Service= Dialout-Framed-User`** For complete information, see “Setting up bridge entries” on page 11-7.

Specifying whether multiple callers can use a profile

By default, the MAX TNT requires that a RADIUS user profile apply only to a single caller. However, you can configure the MAX TNT to allow multiple callers to use the same RADIUS user profile. You can set up this feature on a system-wide or per-profile basis.

- To specify that all RADIUS user profiles can apply to more than a single dial-in user, set Shared-Prof=Yes in the IP-Global profile at the MAX TNT configuration interface.
- To specify that a particular RADIUS user profile can apply to more than a single dial-in user, set Shared-Prof=No in the IP-Global profile and Ascend-Shared-Profile-Enable=Shared-Profile-Yes in the RADIUS user profile.

Specifying an access protocol for incoming calls

The answering unit always determines the authentication method to use for the call. By default, the MAX TNT allows incoming calls without authentication. To indicate an authentication protocol for name and password authentication of PPP, MP, and MP+ calls, you must set the Receive-Auth-Mode parameter in the PPP-Answer subprofile of the Answer-Defaults profile. Specify one of the values listed in Table 4-5.

Table 4-5. Settings for the Receive-Auth-Mode parameter

Setting	Specifies
PAP-PPP-Auth	PAP, a PPP authentication protocol that provides a simple method for the MAX TNT to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment, and does not use encryption. The remote device must support PAP.
CHAP-PPP-Auth	CHAP, a PPP authentication protocol that is more secure than PAP. CHAP provides a way for the remote device to periodically verify the identity of the MAX TNT by means of a three-way handshake and encryption. Authentication takes place upon initial link establishment. A device can repeat the authentication process at any time after the connection is up. The remote device must support CHAP.
MS-CHAP-PPP-Auth	MS-CHAP, the Windows NT version of CHAP. This protocol uses DES and MD4 encryption. Using MS-CHAP, an Ascend unit can authenticate a Windows NT system, and a Windows NT system can authenticate an Ascend unit.
Any-PPP-Auth	PAP, CHAP, or MS-CHAP. The MAX TNT first tries to use MS-CHAP. If the remote end of the connection does not support it, the MAX TNT then attempts to use CHAP. If the remote end of the connection does not support CHAP, the MAX TNT uses PAP instead.

Consider the following:

- If the incoming PPP call does not include a source IP address, the MAX TNT requires PAP, CHAP, or MS-CHAP authentication.
- For modem, X.75, V.110, or V.120 calls, PAP, CHAP, and MS-CHAP authentication are not available.
- You cannot specify a UNIX password if you are using CHAP authentication.
- For PAP, CHAP, and MS-CHAP authentication, the calling unit and the MAX TNT share a different secret with the RADIUS server.
  - The calling unit's secret is called the remote secret. The MAX TNT does not know the remote secret's value.
  - The MAX TNT unit's secret is called the NAS secret (because the MAX TNT is an NAS). The calling unit does not know the NAS secret's value.

How PAP works

For PAP authentication, the following events take place:

1. The calling unit sends the unencrypted remote secret to the MAX TNT.
2. The MAX TNT uses the NAS secret to encrypt the remote secret.
3. The RADIUS server uses the NAS secret to decrypt the remote secret.
4. The RADIUS server validates the remote secret, or passes the clear copy of the remote secret to a UNIX or other password validation system.

How CHAP and MS-CHAP work

For CHAP and MS-CHAP authentication, the following events take place:

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

   The MAX TNT never has the remote secret.
4. The MAX TNT forwards the digest, along with the original challenge and PPP packet ID, to RADIUS.

   No encryption is necessary, because MD5 creates a one-way code that cannot be decoded.
5. The RADIUS server looks up the remote secret in a local database, and calculates an MD5 digest with the local version of the remote secret, along with the challenge and PPP packet ID received from the MAX TNT.
6. The RADIUS server compares the calculated MD5 digest with the digest it received from the MAX TNT.

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

Requesting an access protocol for outgoing calls

If you want to request an authentication protocol for an outgoing PPP or MP+ call, you must use the attributes described in Table 4-6. These attributes represent the minimum you must set to request an authentication protocol.

Table 4-6. Authentication protocol attributes

Attribute	Description	Possible values
Ascend-Send-Auth (231)	Specifies the authentication protocol that the MAX TNT requests when initiating a connection with PPP or MP+ encapsulation. The answering side of the connection determines which authentication protocol, if any, the connection uses.	Send-Auth-None (0) Send-Auth-PAP (1) Send-Auth-CHAP (2) Send-Auth-None is the default.
Ascend-Send-Passwd (232)	Specifies the password the MAX TNT sends to the remote end of a connection on outgoing calls.	Text string of up to 20 characters. The default value is null.
Ascend-Send-Secret (214)	When used in place of the Ascend-Send-Passwd attribute, directs the system to encrypt the password when sending it between the RADIUS server and the MAX TNT on outgoing calls.	Text string of up to 20 characters. The default value is null.
Framed-Protocol (7)	Specifies the type of protocol the link can use.	PPP (1) SLIP (2) MPP (256) EURAW (257) EUUI (258) FR (261) FR-CIR (263) By default, the MAX TNT does not restrict the type of protocol a link can use.
Password (2)	Specifies the user's password	Alphanumeric string containing up to 252 characters. The default value is null.
User-Name (1)	Specifies the name of the remote user or device.	Alphanumeric string containing up to 252 characters. The default value is null.
User-Service (6)	Specifies whether the link can use framed or unframed services.	Login-User (1) Framed-User (2) Dialout-Framed-User (5) By default, the MAX TNT does not restrict the services that a link can use.

To request an access protocol for outgoing calls:

1. On the first line of the profile, set the User-Name attribute to the name of the device that will receive outgoing calls, appending **`-Out`** to the user name.
2. Set Password= “ascend”.
3. Set User-Service=Dialout-Framed-User.
4. On the second line of the user profile, set the User-Name attribute to the name of the device that will receive outgoing calls.
5. On any succeeding line in the profile, set Framed-Protocol=PPP (for a PPP call), or MPP (for an MP+ call).
6. Set the Ascend-Send-Auth attribute to specify an authentication protocol for an outgoing PPP or MP+ call.

   The MAX TNT requests the authentication protocol you specify when it initiates a connection with PPP or MP+ encapsulation. The answering side of the connection determines which authentication protocol, if any, the connection uses.
7. If you request PAP or CHAP authentication, you must specify a password with Ascend-Send-Secret or Ascend-Send-Passwd.

Example of requesting CHAP for an outgoing call

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

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

Setting up the MAX TNT for callback

You have the option of setting up callback security on the MAX TNT. This type of security instructs the MAX TNT to hang up and call back when it receives an incoming call. You can require callback to ensure that the MAX TNT makes a connection with a known device. You can specify callback for switched lines only.

To set up the MAX TNT for callback, use the attributes listed in Table 4-7.

Table 4-7. Callback attributes

Attribute	Description	Possible values
Ascend-Callback (246)	Enables or disables callback.	Callback-No (0) Callback-Yes (1) Callback-No is the default.
Ascend-Dial-Number (227)	Specifies the phone number the MAX TNT dials to reach the bridge, router, or node at the remote end of the link.	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.
Ascend-Send-Passwd (232)	Specifies the password the MAX TNT sends to the remote end of a connection on outgoing calls.	Text string of up to 20 characters. The default value is null.
Ascend-Send-Secret (214)	When used in place of the Ascend-Send-Passwd attribute, directs the system to encrypt the password when sending it between the RADIUS server and the MAX TNT on outgoing calls.	Text string of up to 20 characters. The default value is null.

To configure the MAX TNT for callback:

1. Set Ascend-Callback=Callback-Yes.
2. Set Ascend-Dial-Number to the phone number of the remote device. (The MAX TNT can also use the CLID in order to reach the remote end of the connection, if the CLID is available.)
3. Set Ascend-Send-Secret or Ascend-Send-Passwd. (Use Ascend-Send-Passwd only if your version of the MAX TNT does not support Ascend-Send-Secret.)

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

1. The MAX TNT hangs up after receiving an incoming call that matches the one specified in the RADIUS user profile.
2. The MAX TNT uses the following values to call back the device at the remote end of the link:
   - Number specified by the Ascend-Dial-Number attribute or the CLID.
   - Password specified by Ascend-Send-Secret or Ascend-Send-Passwd.

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.

Example of configuring the MAX TNT for callback

Consider the following lines from a user profile:

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

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

Setting up CLID authentication

If you choose, you can require RADIUS to authenticate incoming calls by checking the calling party's phone number. The RADIUS server performs Calling-Line ID (CLID) authentication before enabling the MAX TNT to answer an incoming call. The CLID is the phone number of the calling device, which is not always provided by the WAN carrier. When the profile requires CLID authentication, the caller's phone number must match a phone number specified in a local Connection profile or RADIUS user profile. You can thereby ensure that the call comes from a known source.

This section describes how to set up a RADIUS user profile for CLID authentication. Before you begin your RADIUS configuration, you must set the CLID-Auth-Mode parameter at the MAX TNT configuration interface. If you choose, you can also set other optional parameters.

Then, when you configure RADIUS, you can choose from the following configurations:

- Authenticate all callers using name, password, and caller ID. (For details, see "CLID authentication using a name, password, and caller ID" on page 4-23.)
- Authenticate all callers using a caller ID only. (For details, see "CLID authentication using a caller ID only" on page 4-24.)
- Use an external authentication server, such as a token-card authentication server, to authenticate users after CLID authentication. (For details, see "External authentication after CLID authentication" on page 4-25.)
- Request PAP, CHAP, or MS-CHAP after CLID authentication. (For details, see "PAP, CHAP, or MS-CHAP after CLID authentication" on page 4-26.)

Configuring CLID authentication at the MAX TNT interface

Before you set up CLID authentication in RADIUS, you must set the CLID-Auth-Mode parameter in the Answer-Defaults profile. You also have the option of setting the CLID Timeout Busy and CLID Fail Busy parameters.

Setting the CLID-Auth-Mode parameter

You can set the CLID-Auth-Mode parameter using any of the settings described in Table 4-8.

Table 4-8. CLID-Auth-Mode settings for CLID authentication

Setting	Description
CLID-Prefer	If you want to authenticate callers by name, password, and caller ID, choose CLID-Prefer. CLID-Prefer specifies that whenever the CLID is available, the MAX TNT checks the calling party's phone number against the value of the Caller-Id attribute in a RADIUS user profile. If it finds a match, and the profile does not require any further authentication, the MAX TNT accepts the call. If the CLID is not available, or if the MAX TNT cannot find a match to the calling-party number, the MAX TNT uses the authentication method specified by the Answer-Defaults profile.
CLID-or-DNIS-Pref DNIS-or-CLID-Pref	If you want to authenticate callers by name, password, and either caller ID or the called-party number, choose one of these settings. When you set CLID-Auth-Mode=CLID-or-DNIS-Pref, the MAX TNT attempts CLID authentication first. When you set CLID-Auth-Mode=DNIS-or-CLID-Pref, the MAX TNT attempts called-number authentication first. In both cases, the MAX TNT also authenticates users by user name and password. (For information about called-number authentication, see "Setting up called-number authentication" on page 4-28.)
CLID-Require CLID-Fallback	If you want to authenticate callers by caller ID only, choose CLID-Require or CLID-Fallback. CLID-Require specifies that the calling party's phone number must match the value of the Caller-Id attribute before the MAX TNT can answer the call. If CLID is not available, the MAX TNT does not answer the call. CLID-Fallback handles the case of RADIUS server timeouts. If the RADIUS server query times out so that CLID authentication cannot be completed, the MAX TNT does not drop the call. Instead it looks for a resident Connection profile to use for standard PAP, CHAP, MS-CHAP, or terminal-server authentication. Therefore, if you set CLID-Auth-Mode=CLID-Fallback, you must also set up a Connection profile.

Table 4-8. CLID-Auth-Mode settings for CLID authentication (continued)

Setting	Description
CLID-and-DNIS-Req	If you want to authenticate callers by both caller ID and called-party number, but not by user name or password, choose CLID-and-DNIS-Req.
DNIS-or-CLID-Req	If you want to authenticate callers with a caller ID only or a called-party number only, but not both, choose DNIS-or-CLID-Req.

Setting disconnect parameters

When CLID authentication fails in an ISDN connection, the MAX TNT sends a Disconnect message. The Cause element in the Disconnect message can indicate why CLID authentication failed. You can set two parameters that affect Disconnect messages, as described in Table 4-9.

Table 4-9. Disconnect parameters

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

General guidelines for CLID authentication

Before you set up CLID authentication, consider the following:

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

CLID authentication using a name, password, and caller ID

To set up CLID authentication using name password, and caller ID, use the attributes listed in Table 4-10.

Table 4-10. Attributes for CLID authentication using name, password, and caller ID

Attribute	Specifies	Possible values
Caller-Id (31)	Calling-party number, indicating the phone number of the user that wants to connect to the MAX TNT.	Telephone number of up to 37 characters, limited to the following: **`1234567890()[]!z-*#|`** The default value is null. In this instance, specify Caller-Id on the first line of the user profile.
Password (2)	User's password.	Text string of up to 252 characters. The default value is null.
User-Name (1)	Name of the remote user or device.	Text string of up to 252 characters. The default value is null.

To require all callers to use name, password and caller ID for authentication, first set CLID-Auth-Mode=CLID-Prefer in the Answer-Defaults profile on the MAX TNT. Then, for the first line of all dial-in RADIUS user profiles, use the following format:

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

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

Although you can configure local Connection profiles for authentication using name, password, and caller ID, Ascend recommends that you perform this function in RADIUS.

Example of CLID authentication using a name, password, and caller ID

The following user profile sets up CLID authentication for Emma, using a name, password, and caller ID:

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

CLID authentication using a caller ID only

To set up CLID authentication using a caller ID only, use the attributes listed in Table 4-11.

Table 4-11. Attributes for CLID authentication using a caller ID only

Attribute	Description	Possible values
Ascend-Require-Auth (201)	Specifies whether the profile requires additional authentication after CLID authentication.	Not-Require-Auth (0) Require-Auth (1) In this instance, specify Not-Require-Auth (the default).
Password (2)	Specifies the user's password.	Text string of up to 252 characters. The default value is null. In this instance, the user name is the calling party's phone number.
User-Name (1)	Specifies the name of the remote user or device.	Text string of up to 252 characters. The default value is null. In this instance, **`"Ascend-CLID"`** is the password.

Note: 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.

Although you can configure local Connection profiles for authentication using a caller ID only, Ascend recommends that you perform this function in RADIUS. To require all callers to use a caller ID only for authentication:

1. If you have not done so already, set CLID-Auth-Mode=CLID-Require or CLID-Fallback in the Answer-Defaults profile on the MAX TNT. (If you also wish to require called-number authentication, you can set CLID-Auth-Mode=CLID-and-DNIS-Require for this step.)
2. In all dial-in RADIUS user profiles, set up the first line using the following format:

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

   where the ***`phonenum`*** argument is the calling party's phone number. The Password value specifies that RADIUS authenticates the caller by caller ID only.
3. On a subsequent line of all dial-in profiles, set the Ascend-Require-Auth attribute to Not-Require-Auth.

Example of CLID authentication using a caller ID only

The following user profile sets up CLID authentication using a caller ID only:

External authentication after CLID authentication

You can use an external authentication server, such as a token-card server, to authenticate callers after CLID authentication. All users must pass caller-ID authentication and external authentication. The configuration uses a two-tiered setup, with the attributes listed in Table 4-12.

Table 4-12. Attributes for external authentication after CLID authentication

Attribute	Description	Possible values
Ascend-Require-Auth (201)	Specifies whether the profile requires additional authentication after CLID authentication.	Not-Require-Auth (0) Require-Auth (1) Not-Require-Auth is the default. In this instance, specify Require-Auth in the first tier.
Password (2)	Specifies the user's password.	Text string of up to 252 characters. The default value is null. In the first tier, the user name is the calling party's phone number. In the second tier, the user name is Default.
User-Name (1)	Specifies the name of the remote user or device.	Text string of up to 252 characters. The default value is null. In this instance, the password is **`"Ascend-CLID"`** in the first tier.

To set up external authentication after CLID authentication:

1. If you have not done so already, set CLID-Auth-Mode=CLID-Require in the Answer-Defaults profile on the MAX TNT. (If you also wish to require called-number authentication, set CLID-Auth-Mode=CLID-and-DNIS-Require for this step.)
2. For the first profile of a two-tiered dial-in setup, specify only these two lines:

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

   where the ***`phonenum`*** argument is the calling party's phone number.
3. Configure the second-tier user profile with the following format for the first line:

   `Default Password="SAFEWORD"`
4. On the second and succeeding lines of the second-tier profile, specify the characteristics of the call.

Example of using a token-card server after CLID authentication

The following example makes use of two user profiles:

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

Default   Password="SAFEWORD"
          User-Service=Login-User,
          Login-Host=10.0.4.1,
          ...
```

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

PAP, CHAP, or MS-CHAP after CLID authentication

Following CLID authentication, you can indicate whether the MAX TNT should request Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), or MS-CHAP authentication for incoming calls on a PPP or MP+ connection. You specify PAP, CHAP, or MS-CHAP authentication using a two-tiered method with the attributes listed in Table 4-13.

Table 4-13. Attributes for PAP, CHAP, or MS-CHAP after CLID authentication

Attribute	Description	Possible values
Ascend-Require-Auth (201)	Specifies whether the profile requires additional authentication after CLID authentication.	Not-Require-Auth (0) Require-Auth (1) Not-Require-Auth is the default. In this instance, specify Require-Auth in the first-tier user profile (the one that sets up CLID authentication).
Caller-Id (31)	Specifies the calling-party number, indicating the phone number of the user that wants to connect to the MAX TNT.	Telephone number of up to 37 characters, limited to the following: **1234567890()[]!z-*#|** The default value is null. In the second-tier profile, specify the same value for Caller-Id as you specified for User-Name in the first-tier profile.

Table 4-13. Attributes for PAP, CHAP, or MS-CHAP after CLID authentication (continued)

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

To request PAP, CHAP, or MS-CHAP authentication after CLID authentication, you must set the Receive-Auth-Mode parameter in the PPP-Answer subprofile of the Answer-Defaults profile. Then, you must configure two RADIUS user profiles, as described in the following sections.

Configuring the first-tier profile

In RADIUS, set up a first-tier profile specifying CLID authentication, specifying only the attributes described in the following steps:

1. Set the User-Name attribute to the calling party's phone number.
2. Set the Password attribute to "Ascend-CLID".
3. Set the Ascend-Require-Auth attribute to Require-Auth.

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

Configuring the second-tier profile

You specify the characteristics of the call in the second-tier user profile. Proceed as follows:

1. In the first line, specify the User-Name and Password attributes.
2. On the same line as the User-Name and Password attribute, set the Caller-Id attribute to the phone number you specified for User-Name in the first-tier user profile.
3. On any succeeding lines, set the User-Service=Framed-User and Framed-Protocol=PPP.
4. Specify any additional attributes.

Example of using CHAP after CLID authentication

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

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

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

Setting up called-number authentication

If you choose, you can set up called-number authentication. This type of authentication works much like CLID authentication, except that the MAX TNT uses the called-party number to authenticate the connection. The remote end might use this form of authentication to make sure that the call goes to a known destination.

The called-party number is an information element of the Q.931 ISDN signalling protocol. It is the phone number the remote device calls to connect to the MAX TNT, but without a trunk group or dialing prefix specification. This number is always available if specified in a profile. When the profile requires called-number authentication, the number called must match a phone number in a local Connection profile or RADIUS user profile.

This section describes how to set up a RADIUS user profile for called-number authentication. Before you begin your RADIUS configuration, you must set the CLID-Auth-Mode parameter at the MAX TNT configuration interface. Then, when you configure RADIUS, you can choose from the following configurations:

- Authenticate all callers with a name, password, and the called-party number. (For details, see "Authentication using a name, password, and called-party number" on page 4-30.)
- Authenticate all callers with the called-party number only. (For details, see "Authentication using the called-party number only" on page 4-31.)
- Use an external authentication server, such as a token-card authentication server, to authenticate users after called-number authentication. (For details, see "External authentication after called-number authentication" on page 4-32.)

Configuring called-number authentication at the MAX TNT interface

Before you set up CLID authentication in RADIUS, you must set the CLID-Auth-Mode parameter in the Answer-Defaults profile. Use any of the settings described in Table 4-14.

Table 4-14. CLID-Auth-Mode settings for called-number authentication

Setting	Description
DNIS-Prefer	If you want to authenticate callers by name, password, and called-party number, choose DNIS-Prefer. DNIS-Prefer specifies that whenever the called-party number is available, the MAX TNT checks the called-party number against the value of the Client-Port-DNIS attribute in a RADIUS user profile. If it finds a match, and the profile does not require any further authentication, the MAX TNT accepts the call. If the called-party number is not available, or if the MAX TNT cannot find a match to the called-party number, the MAX TNT applies authentication by means of the Receive-Auth-Mode parameter in the PPP-Answer subprofile of the Answer-Defaults profile.
CLID-or-DNIS-Pref DNIS-or-CLID-Pref	If you want to authenticate callers by name, password, and either caller ID or the called-party number, choose one of these settings. When you choose CLID-or-DNIS-Pref, the MAX TNT attempts CLID authentication first. When you choose DNIS-or-CLID-Pref, the MAX TNT attempts called-number authentication first. In both cases, the MAX TNT also authenticates users by user name and password.

Table 4-14. CLID-Auth-Mode settings for called-number authentication (continued)

Setting	Description
DNIS-Require	If you want to authenticate callers by called-party number only, choose DNIS-Require. DNIS-Require indicates that the called-party number must match the value of the Client-Port-DNIS attribute before the MAX TNT can answer the call. If the called-party number is not available, the MAX TNT does not answer the call.
CLID-and-DNIS-Req	If you want to authenticate callers by both caller ID and called-party number, but not by user name or password, choose CLID-and-DNIS-Req.
DNIS-or-CLID-Req	If you want to authenticate callers by means of a caller ID only or a called-party number only, but not both, choose DNIS-or-CLID-Req.

Authentication using a name, password, and called-party number

To set up name, password, and called-number authentication, use the attributes listed in Table 4-15.

Table 4-15. Attributes for authentication using a name, password, and called-party number

Attribute	Specifies	Possible values
Client-Port-DNIS	Called-party number, indicating the phone number the user dialed to connect to the MAX TNT.	Telephone number of up to 18 characters, limited to the following: **`1234567890()[]!z-*#|`** The default value is null. In this instance, specify Client-Port-DNIS on the first line of the user profile.
Password (2)	User's password.	Text string of up to 252 characters. The default value is null.
User-Name (1)	Name of the remote user or device.	Text string of up to 252 characters. The default value is null.

To require all callers to use name, password and called-party number for authentication, first set CLID-Auth-Mode=DNIS-Pref in the Answer-Defaults profile on the MAX TNT. Then, for the first line of all dial-in RADIUS user profiles, use the following format:

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

- ***username*** is the user name.
- ***password*** is the user's password.
- ***phonenum*** is the called-party number.

Although you can configure local Connection profiles for authentication using name, password, and called-party number, Ascend recommends that you perform this function in RADIUS.

Example of authentication using a name, password, and called-party number

The following user profile sets up authentication, for Emma, using a name, password, and called-party number:

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

Authentication using the called-party number only

To set up authentication using the called-party number only, use the attributes listed in Table 4-16.

Table 4-16. Attributes for called-number authentication by called-party number only

Attribute	Description	Possible values
Ascend-Require-Auth (201)	Specifies whether the profile requires additional authentication after called-number authentication.	Not-Require-Auth (0) Require-Auth (1) In this instance, specify Not-Require-Auth (the default).
Password (2)	Specifies the user's password.	Text string of up to 252 characters. The default value is null. In this instance, **`"Ascend-DNIS"`** is the password.
User-Name (1)	Specifies the name of the remote user or device.	Text string of up to 252 characters. The default value is null. In this instance, the user name is the called-party number.

Although you can configure local Connection profiles for authentication using the called-party number only, Ascend recommends that you perform this function in RADIUS. To require all callers to use only the called-party number for authentication, proceed as follows:

1. If you have not done so already, set CLID-Auth-Mode=DNIS-Require or CLID-Auth-Mode=CLID-and-DNIS-Req in the Answer-Defaults profile on the MAX TNT.
2. In all dial-in RADIUS user profiles, set up the first line using the following format:

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

   where the ***`phonenum`*** argument is the called-party number. The Password value specifies that RADIUS authenticates the caller by called-party number only.

3. On a subsequent line of all dial-in profiles, set the Ascend-Require-Auth attribute to Not-Require-Auth.

Example of authentication using the called-party number only

The following user profile sets up authentication using the called-party number only:

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

External authentication after called-number authentication

You can use an external authentication server, such as a token-card server, to authenticate callers after called-number authentication. All users must pass called-number authentication and external authentication. The configuration uses a two-tiered setup, with the attributes listed in Table 4-17.

Table 4-17. Attributes for external authentication after called-number authentication

Attribute	Description	Possible values
Ascend-Require-Auth (201)	Specifies whether the profile requires additional authentication after called-number authentication.	Not-Require-Auth (0) Require-Auth (1) Not-Require-Auth is the default. In this instance, specify Require-Auth in the first tier.
Password (2)	Specifies the user's password.	Text string of up to 252 characters. The default value is null. In the first tier, the user name is the called-party number. In the second tier, the user name is Default.
User-Name (1)	Specifies the name of the remote user or device.	Text string of up to 252 characters. The default value is null. In this instance, the password is **"Ascend-DNIS"** in the first tier.

To set up external authentication after called-number authentication:

1. If you have not done so already, set CLID-Auth-Mode=DNIS-Require or CLID-Auth-Mode=CLID-And-DNIS-Require in the Answer-Defaults profile on the MAX TNT.
2. For the first profile of a two-tiered dial-in setup, specify only these two lines:

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

   where the ***phonenum*** argument is the called-party number.
3. Configure the second-tier user profile with the following format for the first line:

   Default Password="SAFEWORD"
4. On the second and succeeding lines of the second-tier profile, specify the characteristics of the call.

Example of using a token-card server after called-number authentication

The following example makes use of two user profiles:

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

Default   Password="SAFEWORD"
          User-Service=Login-User,
          Login-Host=10.0.4.1,
          ...
```

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

Setting up token-card authentication

This section begins with a discussion of how token-card authentication works. It then discusses each step for configuring token-card authentication at your site. The following list summarizes the configuration tasks. The first three tasks are required. The final task is optional, and depends upon the needs of your site.

1. Configure the MAX TNT to locate the authentication server. (For details, see “Configuring the MAX TNT to recognize a token-card server” on page 3-8.)
2. Configure the MAX TNT to use the APP Server utility on each workstation. (For details, see “Configuring the MAX TNT to recognize the APP server utility” on page 3-8.)
3. Choose PAP-TOKEN, CACHE-TOKEN, or PAP-TOKEN-CHAP authentication, and make the appropriate settings. (For details, see “Configuring PAP-TOKEN authentication” on page 4-35, “Configuring CACHE-TOKEN authentication” on page 4-37, and “Configuring PAP-TOKEN-CHAP authentication” on page 4-39.)
4. Configure ACE authentication for users behind a remote bridge/router. This step is optional. For detailed information, see “Configuring ACE authentication for remote bridge/router users” on page 4-40.

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

Introducing token-card authentication

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

Figure 4-1. illustrates an environment that includes an Ascend Pipeline as the calling unit, an NAS (the MAX TNT), a RADIUS server, and an external authentication server.

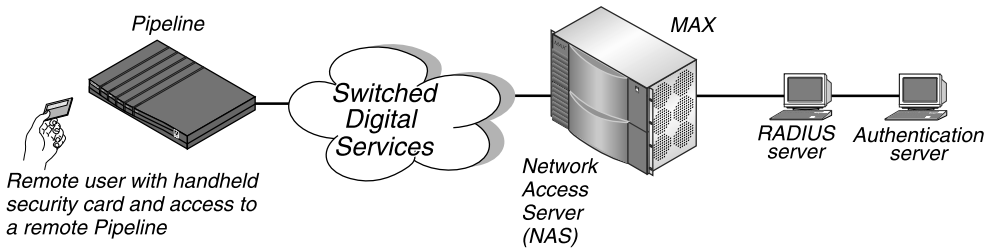


Figure 4-1. Using an external authentication server

When you use token-card authentication, the following events take place:

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

   This user is a client of the MAX TNT. The user can be in terminal-server mode or, alternatively, use the APP Server utility. Ascend Password Protocol (APP) is a UDP protocol from Ascend. When authentication is complete, the user can switch to PPP mode.
2. The MAX TNT determines that it must use a RADIUS user profile to authenticate the user.
3. The MAX TNT sends the user's connection request to the RADIUS server in an Access-Request packet.

   The MAX TNT is a client of the RADIUS server.
4. The RADIUS server forwards the connection request to the ACE or SafeWord client, which resides on the same system as RADIUS.
5. An ACE client forwards the information to the ACE/Server authentication server. A SafeWord client forwards the information to the SafeWord authentication server.

   In either case, the RADIUS server is a client of the authentication server.
6. The authentication server sends an Access-Challenge packet back through the RADIUS server and the MAX TNT to the user dialing in.
7. The user sees the challenge message and obtains the current password from his or her token card.

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

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

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

8. The user enters the current password obtained from the token card in response to the challenge message.
9. The password travels back through the NAS and the RADIUS server to the authentication server.
10. The authentication server sends a response to the RADIUS server, specifying whether the user has entered the proper user name and password.

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

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

Configuring PAP-TOKEN authentication

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

To set up PAP-TOKEN authentication, use the attributes listed in Table 4-18.

Table 4-18. PAP-TOKEN attributes

Attribute	Specifies	Possible values
Password (2)	User's password.	**`"SAFEWORD"`** or **`"ACE"`**; the default value is null.
User-Name (1)	Name of the remote user or device.	Text string of up to 252 characters. The default value is null.

To set up PAP-TOKEN authentication, set the User-Name attribute to the remote bridge/router's system name. Then, specify **"SAFEWORD"** or **"ACE"** for the Password attribute. By setting the Password attribute to **"SAFEWORD"**, you can request validation from an Enigma Logic SafeWord server. For example:

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

By setting the Password attribute to **"ACE"**, you can request validation from a Security Dynamics ACE server. For example:

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

Example of using PAP-TOKEN with Security Dynamics ACE/Server

This example shows how to set up RADIUS for use with the Security Dynamics ACE/Server. The remote end consists of a Pipeline 50 unit and a PC running Appserv. The local end consists of a MAX TNT 4000 and a UNIX device running RADIUS, ACE/Client, and ACE/Server. Figure 4-2. shows the WAN configuration.

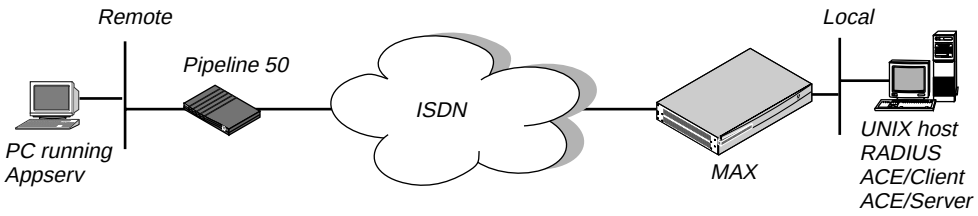


Figure 4-2. ACE/Server configuration

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

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

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

Configuring CACHE-TOKEN authentication

CACHE-TOKEN authentication uses a shared secret, and simplifies the authentication process by caching the user's token for the fixed length of time specified by the Ascend-Token-Expiry attribute. During the lifetime of the token, subsequent calls by the user require only CHAP authentication without the use of a hand-held token card. When the cached token expires, the ACE or SAFEWORD server authenticates CACHE-TOKEN access requests.

To set up CACHE-TOKEN authentication, use the attributes listed in Table 4-19. Except for the Ascend-Receive-Secret attribute, all attributes must appear on the first line of the user profile.

Table 4-19. CACHE-TOKEN attributes

Attribute	Description	Possible values
Ascend-Receive-Secret (215)	Specifies a value the RADIUS server uses to authenticate incoming calls from a user while his or her token is cached and alive. The cached token resides on the MAX TNT during the initial token-card authentication process.	Text string of up to 20 characters. The default value is null.
Ascend-Token-Expiry (204)	Sets the lifetime of a cached token, in minutes (that is, the lifetime of token-card authentication).	Integer between 0 and 65535, representing a number of minutes. The default value is 0 (zero), which specifies that token caching is not allowed. When you accept the default, the MAX TNT rejects subsequent calls
Ascend-Token-Idle (199)	Specifies the maximum length of time, in minutes, a cached token can remain alive between authentications if a call is idle.	Integer between 0 and 65535, representing a number of minutes. By default, the token remains alive until the value of Ascend-Token-Expiry is reached.
Ascend-Token-Immediate (200)	Establishes whether or not RADIUS sends the user's password to the token-card server.	Tok-Imm-No (0) Tok-Imm-Yes (1) Tok-Imm-No is the default.
Password (2)	Specifies the user's password.	**"SAFEWORD"** or **"ACE"**; the default value is null.
User-Name (1)	Specifies the name of the remote user or device.	Text string of up to 252 characters. The default value is null.

To set up CACHE-TOKEN authentication:

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

   If you specify **"ACE"**, the MAX TNT can authenticate multiple users behind the remote bridge/router. For details, see "Configuring ACE authentication for remote bridge/router users" on page 4-40. This feature is not available if you specify the **"SAFEWORD"** setting.
3. Set the Ascend-Token-Expiry attribute to the lifetime in minutes of a cached token.
4. If you want to specify the maximum length of time in minutes a cached token can remain alive between authentication, set the Ascend-Token-Idle attribute (optional).

   This attribute is useful for enforcing authentication when a connection comes up again after an idle period. If you do not specify this attribute, the cached token remains alive until the value of the Ascend-Token-Expiry attribute causes it to expire. Typically, the value of Ascend-Token-Idle is lower than the value of Ascend-Token-Expiry.
5. If the user profile contains the setting User-Service=Login-User, and the token-card server requires that a user enter a challenge, set Ascend-Token-Immediate=Tok-Imm-No.

   When you set Ascend-Token-Immediate=Tok-Imm-No, RADIUS ignores the user's password. If you specify, Tok-Imm-Yes, RADIUS sends the password to the security server for authentication.
6. Set the Ascend-Receive-Secret attribute to the same password as the Send-Password parameter in the Connection profile at the remote end.

   The RADIUS server uses this value to authenticate incoming calls from a user while his or her token is cached and alive. The cached token resides on the MAX TNT during the initial token-card authentication process.
7. When you start the RADIUS daemon, specify the -c argument to enable cache-token authentication.

Example of using CACHE-TOKEN with Enigma Logic server

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

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

Configuring PAP-TOKEN-CHAP authentication

PAP-TOKEN-CHAP authentication uses an encrypted CHAP password with which the answering unit authenticates second and subsequent channels of an MP+ call. The advantage of a PAP-TOKEN-CHAP call over a PAP-TOKEN call is that you need to verify only the initial connection by means of a hand-held token card. The MAX TNT uses CHAP to verify any additional channels.

To set up PAP-TOKEN-CHAP authentication, use the attributes listed in Table 4-20.

Table 4-20. PAP-TOKEN-CHAP attributes

Attribute	Specifies	Possible values
Ascend-Receive-Secret (215)	Value the RADIUS server uses to authenticate incoming calls from a user while his or her token is cached and alive. The cached token resides on the MAX TNT during the initial token-card authentication process.	Text string of up to 20 characters. The default value is null.
Password (2)	User's password.	**"SAFEWORD"** or **"ACE"**; the default value is null.
User-Name (1)	Name of the remote user or device.	Text string of up to 252 characters. The default value is null.

To set up PAP-TOKEN-CHAP authentication:

1. Set the User-Name attribute to the remote bridge/router's system name.
2. Specify **"SAFEWORD"** or **"ACE"** for the Password attribute.
3. Set Ascend-Receive-Secret to the value of the Aux-Send-Password parameter specified in the remote end's Connection profile.

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

   In PAP-TOKEN-CHAP authentication, the user has to provide token-card verification for the initial connection only. CHAP verifies any additional channels. That is, whenever the MAX TNT adds channels to a PPP or MP+ call with PAP-TOKEN-CHAP, the calling unit sends the encrypted value of Aux-Send-Password, and the answering unit checks this password against Ascend-Receive-Secret. The answering unit receives Ascend-Receive-Secret from the RADIUS server when the first channel of the call connects.

Example of using PAP-TOKEN-CHAP with Enigma Logic server

The following example shows the settings necessary for a user called Emma to use an Enigma Logic server. After authentication, the user can open an MP+ (or PPP) session. The user receives IP address 200.0.5.1 and subnet mask 255.255.255.0. Because this profile includes the attribute Ascend-Receive-Secret, the MAX TNT can authenticate additional channels through CHAP without having to go to the SAFEWORD server for authentication.

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

Configuring ACE authentication for remote bridge/router users

You can specify that the RADIUS server use an ACE entry to authenticate multiple users behind a single remote bridge/router (such as an Ascend Pipeline unit). To set up this type of configuration, use the attributes listed in Table 4-21.

Table 4-21. ACE authentication attributes for remote users

Attribute	Specifies	Possible values
Password (2)	User's password.	Text string of up to 252 characters. The default value is null.
User-Name (1)	Name of the remote user or device.	Text string of up to 252 characters. The default value is null.

First, set the User-Name attribute to the remote router's system name. Then, specify **"ACE"** for the Password attribute.

The user must enter the token in this format:

password.*realname*

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

Setting up authentication for terminal-server calls

This section describes how to set up authentication for the following configurations:

- Terminal-server calls with PAP, CHAP, or MS-CHAP
- Asynchronous PPP calls using terminal-server authentication
- Digital dial-in using terminal-server authentication

Configuring terminal-server calls with PAP, CHAP, or MS-CHAP

Table 4-22 lists the types of equipment that allow a customer to communicate with PPP and PAP, CHAP, or MS-CHAP authentication.

Table 4-22. Terminal-server devices for using PAP, CHAP, or MS-CHAP

Device	Special considerations
Analog modems with no expect-send script	The customer's PPP software must support PAP, CHAP, or MS-CHAP. The software must start negotiating PPP once it registers that the modems have connected.
ISDN TAs using asynchronous-to-synchronous conversion	The connection between the client and the TA is asynchronous, and the ISDN connection between the TA and the MAX TNT is synchronous. You must ensure that the customer's TA is configured for asynchronous-to-synchronous conversion. You do not need V.120 support for clients using ISDN TAs with PAP, CHAP, or MS-CHAP authentication.
True ISDN routers, such as the Pipeline 50	None

The following events take place:

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

For detailed information about setting up PAP, CHAP, or MS-CHAP authentication, see "Specifying an access protocol for incoming calls" on page 4-15.

Configuring async PPP calls with terminal-server authentication

If a customer is dialing in over an analog line using asynchronous PPP and will undergo terminal-server authentication, proceed as follows:

1. If the user will make use of the terminal-server interface and then use PPP, set User-Service=Login-User.
2. If the user will bypass the terminal-server interface and use PPP, set User-Service=Framed-User.
3. If User-Service=Login-User, set PPP=Yes in the PPP-Mode-Configuration subprofile of the Terminal-Server profile.
4. If User-Service=Login-User, your customer's PPP software must have an expect-send script, at the end of which the user starts sending PPP packets.

For analog dial-in using asynchronous PPP and terminal-server authentication, the following events take place:

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

Configuring digital dial-in with terminal-server authentication

If a customer is dialing in using an ISDN TA (terminal adapter) and will undergo terminal-server authentication, proceed as follows:

1. If the user will make use of the terminal-server interface and then use PPP, set User-Service=Login-User.
2. If the user will bypass the terminal-server interface and use PPP, set User-Service=Framed-User.
3. If User-Service=Login-User, set PPP=Yes in the PPP-Mode-Configuration subprofile of the Terminal-Server profile.
4. In the Answer-Defaults profile, set V.120=Yes.
5. Make sure that your customer's TA is configured for V.120 encapsulation.You can set most TAs in automatic mode so the TA looks for a PPP packet from the host. If the TA finds a PPP packet, it starts PPP negotiations. If it does not find one, it tries V.120 authentication. Once the call connects, the TA uses asynch/PPP for the duration of the call.

For digital dial-in, the following events take place:

1. The client calls using an ISDN TA, and the MAX TNT answers the call.
2. The MAX TNT waits for PPP packets, while the client software expects the terminal-server login prompt.
3. The MAX TNT times out on PPP, and sends the login prompt.
4. The client software sees the login prompt, enters a user name, and waits, expecting the password prompt.
5. The MAX TNT sends the password prompt, and the client sends a password.
6. The MAX TNT authenticates the user name and password against a RADIUS profile or local Connection profile.
7. If User-Service=Framed-User in the RADIUS user profile, the MAX TNT does not present the `ascend%` prompt, but sends PPP packets.
8. If User-Service=Login-User in the RADIUS user profile, the MAX TNT presents the `ascend%` prompt, and then sends PPP packets.
9. The client software and the MAX TNT communicate using PPP over an asynchronous line— asynchronous from the workstation to the TA, and asynchronous over V.120 from the TA to the MAX TNT.

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

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

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

Setting Up PPP, MP, and MP+ Connections

5

This chapter describes how to configure a RADIUS user profile for PPP, MP, and MP+ connections. The chapter is divided into the following sections:

Before you begin

Before configuring the RADIUS user profile for a PPP, MP, or MP+ connection, perform the following tasks at the MAX TNT configuration interface:

- Specify system-wide settings.
- Enable the appropriate encapsulation method(s).
- Specify an authentication protocol.
- Set up the MAX TNT to accept client requests.

The sections that follow briefly describe each task. For complete information, see the *MAX TNT Network Configuration Guide*.

Specifying system-wide settings

To specify system-wide settings:

1 In the System profile, indicate the MAX TNT unit's name with the Name parameter. You can specify up to 24 characters. The default value is null.

2 If you want the MAX TNT to add channels to an MP+ call in multiples, rather than one at a time, set the System Profile's Parallel-Dialing parameter to a number greater than 1. The Parallel-Dialing parameter determines how many calls the unit can dial out concurrently.

3 Decide whether the MAX TNT should use the Answer-Defaults profile as the default when answering a call. If so, set Use-Answer-For-All-Defaults=Yes in the Answer-Defaults profile. If you accept the default setting of No, the MAX TNT uses the factory defaults.

Enabling the encapsulation method

When setting up your connection, select the appropriate encapsulation method(s) in a subprofile of the Answer-Defaults profile. Proceed as follows:

1 To enable the MAX TNT to answer a single-channel PPP call, set PPP-Enabled=Yes in the PPP-Answer subprofile.

2 To enable the MAX TNT to answer an MP call, set Enabled=Yes in the MP-Answer subprofile.

3 To enable the MAX TNT to answer a multichannel MP+ call, set Enabled=Yes in the MPP-Answer subprofile.

Specifying an authentication protocol

If you choose, you can specify an authentication protocol for name and password authentication of PPP, MP, and MP+ calls. In the Answer-Defaults profile's PPP-Answer subprofile, set the Receive-Auth-Mode parameter to PAP-PPP-Auth, CHAP-PPP-Auth, MS-CHAP-PPP-Auth, or Any-PPP-Auth. (For descriptions of these settings, see Table 4-5 on page 4-15.)

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

Setting up the MAX TNT to accept client requests

If you plan to configure RADIUS to accept disconnect requests, you must specify settings in the Rad-Auth-Server subprofile of the External-Auth profile. For information about how to carry out this task, see “Configuring the MAX TNT for RADIUS client requests” on page 3-9.

Overview of PPP, MP, and MP+

This section provides a brief introduction to PPP, MP, and MP+ connections. For complete information, see the *MAX TNT Network Configuration Guide*.

What is PPP?

Point-to-Point Protocol (PPP) enables dial-in connections from an analog modem or ISDN device that uses a single channel, and supports single-channel dialout connections. Figure 5-1. shows the MAX TNT with a PPP connection to a remote user running Windows 95 with the TCP/IP stack and PPP dialup software.

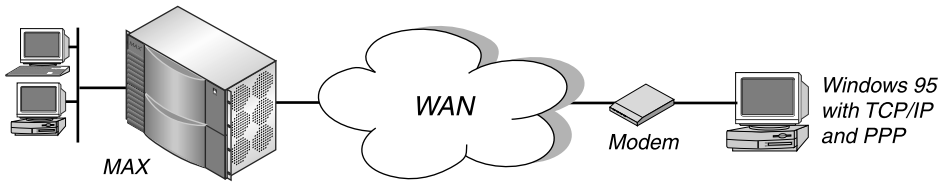


Figure 5-1. A PPP connection

If the caller uses an analog modem, as in Figure 5-1., the connection can use PPP and PAP, CHAP, or MS-CHAP authentication, but the MAX TNT handles the call as a terminal-server connection. The MAX TNT routes the call to a digital modem, which passes the call to the terminal-server software. When the terminal server recognizes PPP encapsulation in the call, it passes the call to the router software.

If the caller is an ISDN device, the connection can use terminal server, PAP, CHAP, or MS-CHAP authentication.

What is MP?

MP uses the encapsulation defined in RFC 1990, and enables the MAX TNT to interact with MP-compliant equipment from other vendors. MP supports multichannel links, but not Dynamic Bandwidth Allocation (DBA). The base channel count determines the number of calls to place, and the number of channels does not change.

In addition, MP requires that all channels in the connection share the same phone number. That is, the channels on the answering side of the connection must be in a hunt group. Both sides of the link must support MP encapsulation.

What is MP+?

MP+ uses PPP encapsulation with Ascend extensions, and enables the MAX TNT to connect to another Ascend unit with multiple channels. MP+ supports Dynamic Bandwidth Allocation (DBA), enabling the MAX TNT to increase bandwidth as necessary and to drop bandwidth when the connection no longer requires it. The criteria for adding or dropping a link are determined by Ascend extensions and are supported only by Ascend equipment.

An MP+ connection can combine up to 30 channels into a single high-speed connection.

Figure 5-2. shows the MAX TNT connected to a remote Pipeline 25 with an MP+ connection.

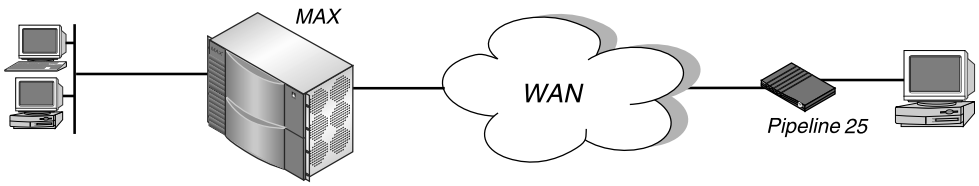


Figure 5-2. An MP+ connection

Other types of units might support MP but not MP+. So, if you configure an MP+ connection in RADIUS between the MAX TNT and a non-Ascend unit, the MAX TNT first requests the MP+ protocol. If the remote device refuses MP+, the MAX TNT uses MP instead. If the answering device refuses both MP+ and MP, the MAX TNT sets up a PPP call on a single channel.

Overview of PPP, MP, and MP+ configuration tasks

When you configure a PPP, MP, or MP+ connection, you must:

- Configure a basic dial-in connection. (For complete information, see “Setting up a dial-in PPP, MP, or MP+ connection” on page 5-5.)
- Configure a basic outgoing connection. (For complete information, see “Setting up an outgoing PPP, MP, or MP+ connection” on page 5-9.)

Depending on the nature of your dial-in connection, you might also need to carry out the following additional tasks:

- Configure a Nailed/MPP connection. (For information, see “Setting up a Nailed/MPP connection” on page 5-16.)
- Configure a nailed-up connection. (For information, see “Setting up a nailed-up connection” on page 5-18.)
- Manage bandwidth for the connection. (For information, see “Managing bandwidth” on page 5-21.)
- Limit the devices and services the caller can use. (For information, see “Limiting access to devices and services” on page 5-28.)
- Limit the ports, lines, and channels the caller can use. (For information, see “Restricting access to ports, lines, and channels” on page 5-30.)
- Configure disconnects for certain users and sessions. (For information, see “Setting up disconnects” on page 5-31.)

Setting up a dial-in PPP, MP, or MP+ connection

When you configure a dial-in PPP, MP, or MP+ connection, you must carry out the following tasks:

- Set the User-Name, Password, and User-Service attributes.
- Set the Framed-Protocol attribute.

For complete information about performing the required tasks, see "Configuring required attributes for a PPP, MP, or MP+ connection" on page 5-7.

Depending on your configuration, you also have the option of specifying:

- IP address of the MAX TNT
- Async control character map
- Maximum packet size
- Compression settings

For complete information about performing the optional tasks, see "Configuring optional attributes for a PPP, MP, or MP+ connection" on page 5-7.

Overview of PPP, MP, and MP+ attributes

To configure a PPP, MP, or MP+ connection in RADIUS, use the attributes listed in Table 5-1.

Table 5-1. PPP, MP, and MP+ attributes

Attribute	Description	Possible values
Ascend-Link-Compression (233)	Turns data compression on or off.	Link-Comp-None (0) turns off data compression. Link-Comp-Stac (1) turns on data compression. The MAX TNT applies the STACKER LZS compression/decompression algorithm. Link-Comp-None is the default.
Ascend-PPP-Address (253)	Specifies the IP address of the MAX TNT as reported to the calling unit during PPP IPCP negotiations.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0.
Ascend-PPP-Async-Map (212)	Provides the async control character map for the session.	Four-byte bitmap to one or more control characters. The default is the standard async control character.

Table 5-1. PPP, MP, and MP+ attributes (continued)

Attribute	Description	Possible values
Ascend-PPP-VJ-1172 (211)	Instructs the MAX TNT to use the 0037h value for the VJ compression type. 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.	You can specify PPP-VJ-1172 to indicate 0037h. If you do not specify this value, RADIUS uses the default—VJ compression type 002dh.
Ascend-PPP-VJ-Slot-Comp (210)	Specifies whether the MAX TNT uses slot compression when sending VJ-compressed packets.	VJ-Slot-Comp-No (0) VJ-Slot-Comp-Yes (1) VJ-Slot-Comp-Yes is the default.
Framed-Address (8)	Specifies the IP address of the remote user or calling device.	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.
Framed-Compression (13)	Turns on TCP/IP header compression. This setting applies only to packets in TCP applications, such as Telnet, and turns on header compression for both sides of the link.	You can specify Van-Jacobson-TCP-IP to turn on TCP/IP header compression. If you do not specify this value, RADIUS uses the default of no header compression.
Framed-MTU (12)	Specifies the maximum number of bytes the MAX TNT can receive in a single packet on a link.	Integer between 1 and 1524. The default value is 1524.
Framed-Netmask (9)	Specifies the subnet mask associated with the IP address of a station or router at the remote end of the link.	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.
Framed-Protocol (7)	Specifies the type of protocol the link can use.	PPP (1) SLIP (2) MPP (256) EURAW (257) EUUI (258) FR (261) FR-CIR (263) By default, the MAX TNT does not restrict the type of protocol a link can use.
Password (2)	Specifies the user's password.	Alphanumeric string of up to 252 characters. The default value is null.

Table 5-1. PPP, MP, and MP+ attributes (continued)

Attribute	Description	Possible values
User-Name (1)	Specifies the name of the remote user or device.	Alphanumeric string of up to 252 characters. The default value is null.
User-Service (6)	Specifies whether the link can use framed or unframed services.	Login-User (1) Framed-User (2) Dialout-Framed-User (5) By default, the MAX TNT does not restrict the services that a link can use.

Configuring required attributes for a PPP, MP, or MP+ connection

To configure a dial-in PPP, MP, or MP+ connection in a RADIUS user profile, you must set:

- User-Name, Password, and User-Service attributes.
- Framed-Protocol attribute.
- Framed-Address attribute (and Framed-Netmask if a subnet mask is in use)

Setting the User-Name, Password, and User-Service attributes

On the first line of the RADIUS user profile:

1 For User-Name, specify the name of the dial-in user or device.

2 For Password, specify the dial-in caller's password.

3 Set User-Service=Framed-User.

Setting the Framed-Protocol attribute

To specify that the caller must use PPP, MP, or MP+, set Framed-Protocol=PPP on any line other than the first. A user requesting access can dial in with MP+, MP, or PPP framing. Or, the user can dial in unframed, and then change to PPP framing. If the user dials in with any other type of framing, the MAX TNT rejects the call.

Setting the Framed-Address attribute

On any line other than the first, set the Framed-Address attribute to the IP address of the caller. If a subnet mask is in use, specify it by setting the Framed-Netmask attribute as well.

Configuring optional attributes for a PPP, MP, or MP+ connection

When configuring a dial-in PPP, MP, or MP+ connection, you have the option of specifying:

- IP address of the MAX TNT
- Async control character map
- Maximum packet size
- Compression settings

Specifying the MAX TNT unit's IP address

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

If you specify a valid IP address, IPCP negotiates with that IP address. If you set the value of this attribute to 255.255.255.255, IPCP negotiates with the address 0.0.0.0. Note that you can assign Ascend-PPP-Address a value different from the MAX TNT unit's true IP address, as long as the user requesting access is aware of the discrepancy.

If you accept the default value of 0.0.0.0, IPCP negotiates using the value of the IP-Address and Netmask values in the IP-Interface profile.

Specifying the async control character map

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

The value you specify is 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 one of the 32 ASCII control characters. The bits are ordered with the lowest bit of the lowest byte being 0 (zero). For example, bit 19 corresponds to Control-S (DC3) or ASCII 19. The control characters pass through the link as data. Only applications running over the link use the data.

Specifying the maximum packet size

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

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

Specifying compression settings

To specify compression settings, proceed as follows:

1 To turn on data compression, set Ascend-Link-Compression=Link-Comp-Stac. Both sides of the link must turn on data compression for this setting to have any effect.

2 To turn on TCP/IP header compression, set Framed-Compression=Van-Jacobson-TCP-IP. Turning on header compression is most effective in reducing overhead when the data portion of the packet is small.

When you specify this setting, 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.

3 If Framed-Compression=Van-Jacobson-TCP-IP, you can instruct the MAX TNT not to use slot compression by setting Ascend-PPP-VJ-Slot Comp=VJ-Slot-Comp-No. When you specify this setting, each VJ-compressed packet has a slot ID.

4 To instruct the MAX TNT to use the 0037h value for the VJ compression type, set Ascend-PPP-VJ-1172=PPP-VJ-1172.

Example of configuring a connection that uses PPP, MP, or MP+

The following sample user profile showing a PPP connection that uses link compression, TCP/IP header compression, and IP routing for an incoming call from the user Emma.

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

Setting up an outgoing PPP, MP, or MP+ connection

To configure outgoing calls in a RADIUS user profile, you must specify:

- User name, password, and user service
- Telephone number the MAX TNT dials
- IP address and subnet mask (if dynamic IP addressing is not in use)

Depending on your configuration, you also have the option of specifying:

- Encapsulation method
- Data service
- Billing number
- Remote-device callback
- Type of T1 PRI service
- Type of phone number for T1 PRI calls
- U.S. Interexchange Carrier (IEC) for long distance T1 PRI calls

Overview of outgoing-call attributes

To configure outgoing calls in RADIUS, use the attributes listed in Table 5-2.

Table 5-2. Outgoing call attributes

Attribute	Description	Possible values
Ascend-Billing-Number (249)	Specifies a billing number for charges you incur on the line. If you do not enter a billing number, the telephone company assigns charges to the telephone number associated with the line.	Up to ten characters, limited to the following: **`1234567890()[]!z-*# |`** The default value is null.
Ascend-Call-By-Call (250)	Specifies the T1 PRI service that the MAX TNT uses when placing a PPP call.	Integer corresponding to services provided by AT&T, MCI, and Sprint. By default, the MAX TNT uses ACCUNET Switched Digital Services from AT&T (6).
Ascend-Data-Svc (247)	Specifies the type of data service the link uses for outgoing calls.	For a complete list of possible values, see “Ascend-Data-Svc (247)” on page 14-23. When you set Ascend-Data-Svc=Switched-Modem, a user cannot connect to the MAX TNT with ISDN and is restricted to analog access. Setting Ascend-Data-Svc=Switched-64K enables to the user to connect to any and all data services. Switched-56K is the default.
Ascend-Dial-Number (227)	Specifies the phone number the MAX TNT dials to reach the bridge, router, or node at the remote end of the link.	Up to 21 characters, limited to the following: **`1234567890()[]!z-*#|`** The default value is null.
Ascend-Expect-Callback (149)	Specifies whether the outgoing caller should expect the remote end to call back.	Expect-Callback-No (0) Expect-Callback-Yes (1) Expect-Callback-No is the default.
Ascend-PRI-Number-Type (226)	Specifies the type of phone number the MAX TNT dials.	Unknown-Number (0) Intl-Number (1) National-Number (2) Local-Number (4) Abbrev-Number (5) National-Number is the default.
Ascend-Transit-Number (251)	Specifies the U.S Interexchange Carrier (IEC) you use for long distance calls over a T1 PRI line.	Integer corresponding to an IEC. The default value is null.

Table 5-2. Outgoing call attributes (continued)

Attribute	Description	Possible values
Framed-Address (8)	Specifies the IP address of the called device.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0. An answering user profile with this setting matches all IP addresses.
Framed-Netmask (9)	Specifies the subnet mask in use for the called device.	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.
Framed-Protocol (7)	Specifies the type of protocol the link can use.	PPP (1) MPP (256) EURAW (257) EUUI (258) FR (261) FR-CIR (263) When User-Service=Dialout-Framed-User, the Framed-Protocol attribute specifies the type of framing allowed on the outgoing call. By default, the MAX TNT does not restrict the type of protocol a link can use.
Password (2)	Specifies the user's password.	Alphanumeric string of up to 252 characters. The default value is null.
User-Name (1)	Specifies the name of the remote user or device.	Alphanumeric string of up to 252 characters. The default value is null.
User-Service (6)	Specifies whether the link can use framed or unframed services.	Login-User (1) Framed-User (2) Dialout-Framed-User (5) By default, the MAX TNT does not restrict the services that a link can use.

Configuring required outgoing call attributes

To set up an outgoing call in a RADIUS user profile, you must specify a user name and password, a user service, and the telephone number the MAX TNT dials. If dynamic IP addressing is not in use, you must also specify an IP address and subnet mask.

Specifying a name, password, and user service for outgoing calls

On the first line of the user profile, proceed as follows:

- Set the User-Name attribute to the name of the remote device that will receive outgoing calls, appending **`-Out`** to the user name.
- Set Password= "ascend".
- Set User-Service=Dialout-Framed-User. This setting ensures that no one can use the profile for authentication of an incoming call.

Then, on the second line of the profile, set the User-Name attribute to the name of the remote device that will receive outgoing calls.

For example, you might enter the first two lines in the profile for the remote device Homer as follows:

```
Homer-Out Password="ascend", User-Service=Dialout-Framed-User
     User-Name="Homer",
```

Specifying the phone number the MAX TNT dials

To indicate the phone number the MAX TNT dials to reach the bridge, router, or node at the remote end of the link, set the Ascend-Dial-Number attribute. The MAX TNT sends only the numeric characters to place a call.

If Use-Trunk-Groups=Yes in the System profile, the first digits in the Ascend-Dial-Number attribute have the meanings listed in Table 5-3.

Table 5-3. Ascend-Dial-Number digits

First digit	Significance
4 through 9	The MAX TNT places the call over the trunk group listed in the Trunk-Group parameter.
3	The MAX TNT places the call to a destination listed in a Call-Route profile. In this case, the second and third digits indicate the number of the Call-Route profile.
2	The MAX TNT places the call between host ports on the same MAX TNT, or between Terminal Equipment (TEs) on a local ISDN BRI line. In a port-to-port call, the second digit indicates the slot of a Dual/Host or Host/6 card. In a TE-to-TE call, the second digit indicates the slot of a Host/BRI module. If you enter 0 (zero) for the second digit, the call connects to any available AIM port and ignores the third digit. If you enter a non-zero value for the second digit, the third digit selects the AIM port or a local ISDN BRI port. If you enter 0 (zero) for the third digit, the call connects to any available AIM port or local ISDN BRI line in the module selected by the second digit.

Specifying an IP address and subnet mask

Specify the called device's IP address with the Framed-Address attribute. If a subnet is in use, you must also specify a value for the Framed-Netmask attribute.

If you specify an IP address, you must also enable IP routing for the profile by setting Ascend-Route-IP=Route-IP-Yes. (For more information, see "Enabling IP routing" on page 9-6.)

Configuring optional outgoing call attributes

When you configure an outgoing call, you can specify the encapsulation method and data service the call should use, and a billing number for the line. You can also determine whether the MAX TNT waits for the remote unit to call back. In addition, if you are using a T1 PRI line, you can specify the type of phone number, T1 PRI service, and long-distance service the call uses.

Specifying an encapsulation method for an outgoing call

To specify the encapsulation method in use for the call, set the Framed-Protocol attribute. For PPP calls, set Framed-Protocol=PPP. For MP+ calls, set Framed-Protocol=MPP.

Specifying a data service

To specify the data service the link uses for outgoing calls, set the Ascend-Data-Svc attribute. For a complete list of the values you can specify, see “Ascend-Data-Svc (247)” on page 14-23.

Specifying a billing number

To indicate a billing number for charges you incur on the line, set the Ascend-Billing-Number attribute. If you do not enter a billing number, the telephone company assigns charges to the telephone number associated with the line. Your carrier determines the billing number, and uses it to sort your bill. If you have several departments, and each department has its own billing number, your carrier can separate and tally each department’s usage.

The MAX TNT uses the Ascend-Billing-Number value differently depending on the type of line you use:

- 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 on an ISDN BRI line applies only to installations in Australia.
- For a T1 PRI line, the MAX TNT uses the Ascend-Billing-Number attribute, rather than the phone number ID, to identify itself to the answering party.

Specifying whether the caller should expect a call back

To specify whether the caller expects the remote device to call back, set the Ascend-Expect-Callback attribute.

When the remote device is set to call back (Ascend-Callback=Callback-Yes in a RADIUS user profile or Callback=Yes in a Connection profile) and CLID authentication is not required, the remote device answers the call, verifies a name and password against a user profile, hangs up, and dials back to the caller.

If the remote end is set up for callback *and* requires CLID-only authentication (CLID-Auth-Mode=CLID-Require), the remote device never answers the call. The caller therefore avoids billing charges. However, a problem can occur. To the caller, it appears as though the call never got through at all. This is a special problem for Ping and Telnet, because those processes continuously try to open a connection, and they reject any callback.

When you set Ascend-Expect-Callback=Expect-Callback-Yes, calls that dial out and do not connect (for any reason) appear in a list of destinations to which no further calls can be placed for 90 seconds. The delay gives the remote device an opportunity to complete the callback. You can specify one of the following values:

- Expect-Callback-No (0) indicates that the caller does not wait for a callback after placing a call that does not connect.
- Expect-Callback-Yes (1) indicates that the caller waits 90 seconds after placing a call that does not connect before attempting to place another call to the same number.

Specifying the T1 PRI service

To specify the T1 PRI service that the MAX TNT uses, set the Ascend-Call-By-Call attribute. Specify a number corresponding to the type of service the MAX TNT uses. Table 5-4 lists the services available for each service provider.

Table 5-4. 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

Specifying the type of number the MAX TNT dials (T1 PRI only)

To specify the type of phone number the MAX TNT dials, set the Ascend-PRI-Number-Type attribute to one of the settings listed in Table 5-5.

Table 5-5. Ascend-PRI-Number-Type settings

Setting	Description
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.

Specifying the long-distance carrier (T1 PRI only)

To specify the U.S. Interexchange Carrier (IEC) you use for long distance calls over a T1 PRI line, set the Ascend-Transit-Number attribute. Specify the same digits you use to prefix a phone number you dial over an ISDN BRI line, T1 access line, or voice interface:

- 288 selects AT&T.
- 222 selects MCI.
- 333 selects Sprint.

The default value is null. If you accept the default, the MAX TNT uses any available IEC for long-distance calls.

Example of configuring an outgoing call

The following example shows a user profile for dialing calls from the MAX TNT. The following profile enables IP traffic to initiate a call to a number in the United States:

```
Homer-Out Password="ascend", User-Service=Dialout-Framed-User
     User-Name="Homer",
     Ascend-Dial-Number=31,
     Framed-Protocol=PPP,
     Framed-Address=10.0.100.1,
     Framed-Netmask=255.255.255.0,
     Ascend-Metric=2,
     Framed-Routing=None,
     Ascend-Idle-Limit=30,
     Ascend-PRI-Number-Type=National-Number,
     Ascend-Send-Auth=Send-Auth-PAP,
     Ascend-Send-Secret="password1"
```

Setting up a Nailed/MPP connection

A Nailed/MPP connection is a nailed-up connection that can add switched channels to increase bandwidth or to provide a backup if nailed-up channels are down. The maximum number of channels for the Nailed/MPP connection is the value of the Ascend-Maximum-Channels attribute or the number of nailed channels in the specified group, whichever is greater.

The base channels of a Nailed/MPP connection are nailed-up. If a nailed-up channel is temporarily down, the MAX TNT polls continuously trying to re-establish that connection. If the MAX TNT receives an outbound packet while the nailed-up connection is still down, 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 adds or subtracts switched channels according to the Dynamic Bandwidth Allocation (DBA) settings you make in the Connection profile or RADIUS user profile. If the two sides of a connection disagree on the number of channels necessary for a connection, the side requesting the greater number prevails. Both sides make calculations on the required number of channels on the basis of the traffic each end receives.

Overview of Nailed/MPP attributes

To configure a Nailed/MPP connection in RADIUS, you must set the attributes for a regular MP+ connection, and then configure the additional RADIUS attributes listed in Table 5-6.

Table 5-6. Nailed/MPP attributes

Attribute	Description	Possible values
Ascend-Call-Type (177)	Specifies the type of nailed-up connection in use.	Nailed (1) Nailed/Mpp (2) Perm/Switched (3) Nailed is the default.
Ascend-FT1-Caller (175)	Specifies whether the MAX TNT initiates or waits for the remote end to initiate an FT1-AIM or an FT1-B&O call.	FT1-No (0) specifies that the MAX TNT waits for the remote end to initiate the call. FT1-Yes (1) specifies that the MAX TNT dials to bring online any switched circuits that are part of the call. The remote end must have the setting FT1-Caller=No (in a Connection profile) or Ascend-FT1-Caller=FT1-No (in a RADIUS user profile). FT1-No is the default.
Ascend-Group (178)	Points to the nailed-up channels the WAN link uses.	Single integer, or comma-separated list of integers, between 1 and 60. The default value is 1. You can specify a list of integers assigning multiple nailed-up groups to the profile only if Ascend-Call-Type=Nailed/Mpp. The list cannot include spaces.

Configuring attributes for a Nailed/MPP connection

To configure a Nailed/MPP connection in a RADIUS user profile:

1. Configure a regular MP+ connection in RADIUS, as described in “Setting up a dial-in PPP, MP, or MP+ connection” on page 5-5.
2. Set Ascend-Call-Type=Nailed/Mpp.
3. Set Ascend-FT1-Caller=FT1-Yes.
4. Set the Ascend-Group attribute to specify the nailed-up channels the profile can use.

   If a Nailed/MPP connection is down and the nailed channels are also down, the connection does not re-establish itself until the nailed channels come back up or one end dials the switched channels. (When the calling unit receives a packet whose destination is the unit at the remote end of the Nailed/MPP connection, the unit automatically dials the switched channels.)
5. Set the Answer-Originate and FT1-Caller parameters for answering only in the remote end’s Connection profile.

Note: If you modify the RADIUS user profile for a Nailed/MPP connection, most changes become active only after the call goes down and then back up. However, if you add a group number with the Ascend-Group attribute and save your changes, the MAX TNT adds the channels to the connection without bringing it down.

Example of configuring a Nailed/MPP connection

In the following example, a Nailed/MPP connection uses the channels in groups 1, 3, 5, and 7:

```
permconn-Dial-1 Password="ascend", User-Service=Dialout-Framed-User
       User-Name="Tom",
       Framed-Protocol=PPP,
       Framed-Address=50.1.1.1,
       Framed-Netmask=255.0.0.0,
       Ascend-Route-IP=Route-IP-Yes,
       Ascend-Metric=7,
       Framed-Routing=None,
       Ascend-Idle-Limit=0,
       Ascend-Bridge=Bridge-No,
       Ascend-Call-Type=Nailed/Mpp,
       Ascend-Group="1,3,5,7",
       Ascend-FT1-Caller=FT1-Yes
```

Setting up a nailed-up connection

A nailed-up connection is a permanent link that is always up as long as the physical connection persists. If the unit or central switch resets, or if the link goes down, the MAX TNT attempts to restore the link at ten-second intervals. If the MAX TNT or the remote unit is powered off, the link comes back up when the device boots up again. On an ISDN line, a nailed-up connection uses one or more of the line's channels. A serial WAN link is not divided into channels and is always 100% nailed up.

Overview of nailed-up connection attributes

To configure a nailed-up connection in RADIUS, use the attributes listed in Table 5-7.

Table 5-7. Nailed-up attributes

Attribute	Description	Possible values
Ascend-Backup (176)	Specifies the backup profile for a nailed-up link whose physical connection fails.	Text string (profile name). The default value is null.
Ascend-Call-Type (177)	Specifies the type of nailed-up connection in use.	Nailed (1) specifies a link that consists entirely of nailed-up channels. Nailed/Mpp (2) specifies a link that consists of both nailed-up and switched channels. Perm/Switched (3) specifies a permanent switched connection—an outbound call that the MAX TNT attempts to keep up at all times. Nailed is the default.
Ascend-FT1-Caller (175)	Specifies whether the MAX TNT initiates or waits for the remote end to initiate an FT1-AIM or an FT1-B&O call.	FT1-No (0) specifies that the MAX TNT waits for the remote end to initiate the call. FT1-Yes (1) specifies that the MAX TNT dials to bring online any switched circuits that are part of the call. The remote end must have the setting FT1-Caller=No (in a Connection profile) or Ascend-FT1-Caller=FT1-No (in a RADIUS user profile). FT1-No is the default.

Table 5-7. Nailed-up attributes (continued)

Attribute	Description	Possible values
Ascend-Group (178)	Points to the nailed-up channels the WAN link uses.	Single integer, or comma-separated list of integers, between 1 and 60. The default value is 1. You can specify a list of integers assigning multiple nailed-up groups to the profile only if Ascend-Call-Type=Nailed/Mpp. The list cannot include spaces.
Framed-Protocol (7)	Specifies the type of protocol the link can use.	PPP (1) SLIP (2) MPP (256) EURAW (257) EUUI (258) FR (261) FR-CIR (263) By default, the MAX TNT does not restrict the type of protocol a link can use.
Password (2)	Specifies the user's password.	Alphanumeric string of up to 252 characters. The default value is null.
User-Name (1)	Specifies the name of the remote user or device.	Alphanumeric string of up to 252 characters. The default value is null.
User-Service (6)	Specifies whether the link can use framed or unframed services.	Login-User (1) Framed-User (2) Dialout-Framed-User (5) By default, the MAX TNT does not restrict the services that a link can use.

Configuring attributes for a nailed-up connection

To configure a nailed-up connection in a RADIUS user profile:

1. On the first line of the RADIUS user profile, specify the User-Name, Password, and User-Service attributes in the following format:

   name **Password="ascend", User-Service=Dialout-Framed-User**

   where the ***name*** argument is a descriptive name that specifies the nailed-up profile.
2. On the second line of the user profile, specify the User-Name attribute to indicate the name of the user that can make the nailed-up connection.
3. Set Framed-Protocol=PPP.
4. Set the Ascend-Call-Type attribute to Nailed or Nailed/Mpp.
5. If the remote end is configured to wait for the MAX TNT to initiate FT1 calls, set Ascend-FT1-Caller=FT1-Yes in the RADIUS user profile for the local MAX TNT. If the remote end is configured to initiate FT1 calls, set Ascend-FT1-Caller=FT1-No in the user profile for the local MAX TNT.
6. Set the Ascend-Group attribute to specify the nailed-up channels the profile can use.

Example of configuring a nailed-up connection

The following user profile defines a nailed-up link that uses the channels in group 1:

```
permconn-Dial-1 Password="ascend", User-Service=Dialout-Framed-User
       User-Name="Tom",
       Framed-Protocol=PPP,
       Framed-Address=50.1.1.1,
       Framed-Netmask=255.0.0.0,
       Ascend-Route-IP=Route-IP-Yes,
       Ascend-Metric=7,
       Framed-Routing=None,
       Ascend-Idle-Limit=0,
       Ascend-Bridge=Bridge-No,
       Ascend-Call-Type=Nailed,
       Ascend-Group="1",
       Ascend-FT1-Caller=FT1-Yes
```

Modifying or deleting nailed-up profiles

To modify or delete nailed-up profiles:

1. Change or delete the profile on the RADIUS server.
2. Choose the Upd Rem Cfg command from the Sys Diag menu.

   The Ascend unit closes all the sessions related to all nailed-up profiles, deletes all the profiles from the system, and restarts the process of retrieving profiles from RADIUS.

Managing bandwidth

You can manage bandwidth in the following ways:

- Use Dynamic Bandwidth Allocation (DBA).

  DBA is a way to automatically add or subtract channels on demand. When traffic levels expand, the MAX TNT adds switched channels to the call. When traffic levels subside, the MAX TNT removes the channels and frees up the bandwidth for reallocation. For information about setting up DBA, see "Configuring DBA in RADIUS" on page 5-25.
- Specify a time limit for a session and the MAX TNT unit's response to an idle connection. For information about carrying out this task, see "Configuring a time limit and idle connection attributes" on page 5-26.

How Dynamic Bandwidth Allocation (DBA) works

The MAX TNT uses the time period specified by the Ascend-Seconds-Of-History attribute as the basis for calculating average line utilization (ALU), and uses the algorithm specified by the Ascend-History-Weigh-Type attribute for calculating ALU.

The MAX TNT then compares ALU to the percentage specified by the Ascend-Target-Util attribute. When ALU exceeds the threshold defined by Ascend-Target-Util for a time 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. When ALU falls below the threshold defined by Ascend-Target-Util for a 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.

The MAX TNT compares the calculated ALU to the percentage specified in the Ascend-Target-Util attribute. It uses the following logic to determine when to add channels:

If ALU > Ascend-Target-Util for > Ascend-Add-Seconds seconds, add Ascend-Inc-Channel-Count channels.

The MAX TNT uses the following logic to determine when to subtract channels:

If ALU < Ascend-Target-Util for > Ascend-Remove-Seconds seconds, subtract Ascend-Dec-Channel-Count channels.

How RADIUS authenticates multiple channels

When the system adds additional channels, the MAX TNT must authenticate each one. You can secure each circuit with one of the methods described in the following sections.

Static passwords

Before the MAX TNT dials a new circuit, it prompts the user to enter a static, reusable password as specified in the RADIUS user profile. To prevent intruders from capturing the password as it travels across the WAN, you can specify that the MAX TNT use the Challenge Handshake Authentication Protocol (CHAP). This protocol uses encryption to protect the password and verify the identity of the caller.

(For information about specifying a static password, see “Specifying a password” on page 4-6. For information about requiring CHAP authentication, see “Specifying an access protocol for incoming calls” on page 4-15.)

Tokens

Using PAP-TOKEN authentication, RADIUS can require a user to specify a one-time-only password, generated by a token-card server, for each additional channel. This password is called a *token*. (For information, see “Configuring PAP-TOKEN authentication” on page 4-35.)

Combination of static passwords and tokens

In RADIUS, you can indicate that the user need only specify a token for the initial channel, and that CHAP must authenticate all other channels. Whenever the MAX TNT uses PAP-TOKEN-CHAP authentication and adds channels to a PPP or MP+ call, the calling unit sends the encrypted value of Aux-Send-Password (found in the Connection profile used to dial the call). The answering unit checks this password against the value of Ascend-Receive-Secret in the RADIUS user profile. The answering unit receives Ascend-Receive-Secret from the RADIUS server when the first channel of the call connects.

(For details, see “Configuring PAP-TOKEN-CHAP authentication” on page 4-39.)

Cached passwords

You can configure RADIUS to reuse a password dynamically generated during session initiation. In this case, both the user and the MAX TNT cache the password. Then, when the MAX TNT needs to add bandwidth, the user provides the CHAP-encrypted password automatically, and the MAX TNT uses an internal key to authenticate the additional channels. You can specify a timeout value for the cached password, or configure RADIUS to maintain the password throughout the session.

(For detailed information about setting up RADIUS for cached passwords, see“Configuring CACHE-TOKEN authentication” on page 4-37.)

Overview of DBA attributes

To configure DBA in RADIUS, use the attributes listed in Table 5-8.

Table 5-8. DBA attributes

Attribute	Description	Possible values
Ascend-Add-Seconds (240)	Specifies the number of seconds that average line utilization (ALU) for transmitted data must exceed the threshold indicated by the Ascend-Target-Util attribute before the MAX TNT begins adding bandwidth to a session.	Integer between 1 and 300. The default value is 5.
Ascend-Base-Channel-Count (172)	Specifies the initial number of channels the MAX TNT sets up when originating calls for a PPP, MP, or MP+ 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.
Ascend-DBA-Monitor (171)	Specifies how the MAX TNT monitors traffic on an MP+ call.	DBA-Transmit (0) specifies that the MAX TNT adds or subtracts bandwidth on the basis of the amount of data it transmits. 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, and DBA functionality is disabled. DBA-Transmit is the default.
Ascend-Dec-Channel-Count (237)	Specifies the number of channels the MAX TNT removes when bandwidth changes during a call.	Integer between 1 and 32. The default value is 1.

Table 5-8. DBA attributes (continued)

Attribute	Description	Possible values
Ascend-History-Weigh-Type (239)	Specifies which Dynamic Bandwidth Allocation (DBA) algorithm to use for calculating average line utilization (ALU) of transmitted data.	History-Constant (0) gives equal weight to all samples taken during the time period specified by the Ascend-Seconds-Of History attribute. History-Linear (1) gives more weight to recent samples of bandwidth usage than to older samples taken during the 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 period specified by the Ascend-Seconds-Of-History attribute. The weighting grows at a quadratic rate. History-Quadratic is the default.
Ascend-Inc-Channel-Count (236)	Specifies the number of channels the MAX TNT adds when bandwidth changes during a call.	Integer between 1 and 32. The default value is 1.
Ascend-Maximum-Channels (235)	Specifies the maximum number of channels allowed on an MP+ call.	Integer between 1 and the maximum number of channels your system supports. The default value is 1.
Ascend-Minimum-Channels (173)	Specifies the minimum number of channels an MP+ call maintains.	The default value is 1.
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.	Integer between 1 and 300. The default value is 10.
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.	Integer between 1 and 300. The default value is 15.
Ascend-Target-Util (234)	Specifies the percentage of bandwidth utilization at which the MAX TNT adds or subtracts bandwidth dynamically.	Integer between 0 and 100. The default value is 70.

Configuring DBA in RADIUS

To configure DBA for a RADIUS user profile, first configure an MP+ connection, as described in "Setting up a dial-in PPP, MP, or MP+ connection" on page 5-5. Then, follow the steps described below. (For guidelines on how to set up DBA for optimum performance, see "Guidelines for optimum use of DBA" on page 5-25.)

1. Set the Ascend-Target-Util attribute to the percentage of bandwidth use at which the MAX TNT should add or subtract bandwidth.
2. Set the Ascend-History-Weigh-Type attribute to the algorithm the MAX TNT should use for calculating ALU.
3. Set the Ascend-Seconds-of-History attribute to the number of seconds the MAX TNT should use as a sample for calculating ALU.
4. Set the Ascend-Add-Seconds attribute to the number of seconds that ALU must exceed the Ascend-Target-Util threshold before the MAX TNT begins adding bandwidth to a session.
5. Set the Ascend-Remote-Seconds attribute to the number of seconds that ALU must fall below the Ascend-Target-Util threshold before the MAX TNT begins removing bandwidth from a session.
6. Set the Ascend-Base-Channel-Count attribute to specify the initial number of channels the MAX TNT sets up when originating calls for the link.
7. Set the Ascend-Maximum-Channels attribute to specify the maximum number of channels allowed on a call.
8. Set the Ascend-Minimum-Channels attribute to specify the minimum number of channels the call maintains.
9. Set the Ascend-Inc-Channel-Count attribute to specify the number of channels to add to a call when increasing bandwidth.
10. Set the Ascend-Dec-Channel-Count attribute to specify the number of channels to remove from a call when decreasing bandwidth.
11. Set the Ascend-DBA-Monitor attribute to specify how the MAX TNT monitors traffic on an MP+ call.

Guidelines for optimum use of DBA

For optimum MP+ performance, both sides of a connection must set the base channel count, minimum channel count, and maximum channel count to the same number. In addition, the values for the Ascend-Seconds-Of-History, Ascend-Add-Seconds, and Ascend-Remove-Seconds attributes should smooth out spikes in bandwidth utilization that last for a shorter time than it takes to add capacity. Over T1 lines, the MAX TNT can add bandwidth in less than ten seconds. Over ISDN lines, the MAX TNT can add bandwidth in less than five seconds.

After the MAX TNT adds bandwidth, you typically incur a minimum usage charge. Thereafter, billing is time sensitive. The Ascend-Remove-Seconds value should be at least equal to the minimum duration charge plus one or two billing time increments. Typically, billing is done to the next multiple of six seconds, with a minimum charge for the first 30 seconds.

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 relative to the value of Ascend-Seconds-Of-History, the system becomes less responsive to quick spikes. The easiest way to determine the proper values for all these attributes is to observe usage patterns. If the system is not responsive enough, the value of Ascend-Seconds-Of-History is too high.

Avoid adding or subtracting channels too quickly (less than 10-20 seconds apart). Adding or subtracting channels very quickly leads to many short duration calls, each of which incur the carrier's minimum charge. In addition, adding or subtracting channels too quickly can affect link efficiency, because the devices on either end have to retransmit data when the link speed changes.

When selecting a target utilization value, monitor how the application behaves when using different bandwidths and different loads. For example, an application might be able to use 88% of a 64-Kbps link, but only 70% of a 256-Kbps link.

Example of configuring DBA

The following RADIUS user profile contains all the RADIUS attributes necessary for configuring DBA:

```
John  Password="4yr66", User-Service=Framed-User
      Framed-Protocol=PPP,
      Framed-Address=200.0.5.1,
      Framed-Netmask=255.255.255.0,
      Ascend-Target-Util=80,
      Ascend-History-Weigh-Type=History-Constant,
      Ascend-Seconds-Of-History=90,
      Ascend-Add-Seconds=30,
      Ascend-Remove-Seconds=30,
      Ascend-Maximum-Channels=10,
      Ascend-Inc-Channel-Count=2,
      Ascend-Dec-Channel-Count=2,
      Ascend-DBA-Monitor=DBA-Transmit-Recv,
      ...
```

Configuring a time limit and idle connection attributes

To configure a time limit and idle connection values, use the attributes listed in Table 5-9.

Table 5-9. Time limit and idle connection attributes

Attribute	Specifies	Possible values
Ascend-Idle-Limit (244)	Number of seconds the MAX TNT waits before clearing a call when a session is inactive.	Integer between 0 and 65535. If you specify 0 (zero), the MAX TNT always clears a call when a session is inactive. The default value is 120. 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.
Ascend-Maximum-Call-Duration (125)	Maximum number of minutes an incoming call can remain connected.	Integer between 0 and 1440. The default value is 0 (zero). If you accept the default, the MAX TNT does not set a limit on the duration of an incoming call.

Table 5-9. Time limit and idle connection attributes (continued)

Attribute	Specifies	Possible values
Ascend-Maximum-Time (194)	Maximum length of time in seconds that any session is allowed. Once a session reaches the time limit, its connection is taken offline.	Integer between 0 and 4,294,967,295. The default value is 0 (zero). When you accept the default, the MAX TNT does not enforce a time limit.
Ascend-MPP-Idle-Percent (254)	Percentage of bandwidth utilization below which the MAX TNT clears a single-channel MP+ call.	Integer between 0 and 99. The default value is 0 (zero), which causes the MAX TNT to ignore bandwidth utilization when determining whether to clear a call.
Ascend-Preempt-Limit (245)	Number of idle seconds the MAX TNT waits before using one of the channels of an idle link for a new call.	Integer between 0 and 65535. The MAX TNT never preempts a call if you enter 0 (zero). The default value is 60.

To specify the time limit for a session and the action the MAX TNT should take when a connection is idle, follow the steps described below. (For guidelines on how to set up idle connection attributes for optimum performance, see "Guidelines for optimum use of idle connection attributes" on page 5-28.)

1. Configure an MP+ connection, as described in "Setting up a dial-in PPP, MP, or MP+ connection" on page 5-5.
2. Set the Ascend-Maximum-Call-Duration attribute to specify the number of minutes an incoming call can remain connected. The MAX TNT checks the connection once per minute, so the actual time the call is connected is slightly longer than the time you set.
3. Set the Ascend-Maximum-Time attribute to specify the maximum length of time in seconds that any session is allowed. Once a session reaches the time limit, its connection is taken offline.
4. Set the Ascend-Idle-Limit attribute to indicate the number of seconds the MAX TNT waits before clearing a call when a session is inactive.
5. Set the Ascend-MPP-Idle-Percent attribute to specify a percentage of bandwidth utilization below which the MAX TNT clears a single-channel MP+ call. (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.)
6. Set the Ascend-Preempt-Limit attribute to indicate the number of idle seconds the MAX TNT waits before using one of the channels of an idle link for a new call.

Guidelines for optimum use of idle connection attributes

When you set the Ascend-MPP-Idle-Percent attribute, bandwidth utilization must fall below this percentage *on both sides of the connection* before the MAX TNT clears the call. If the device at the remote end of the link has 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.

Limiting access to devices and services

To limit the devices and services a PPP, MP, or MP+ link can use, you must specify a value for each of the attributes listed in Table 5-10. If you do not specify a value, the MAX TNT does not restrict the devices and services available to the caller.

Table 5-10. Limiting devices and services

Attribute	Description	Possible values
Ascend-Force-56 (248)	Specifies whether the MAX TNT uses only the 56-Kbps portion of a channel.	Force-56-No (0) specifies that the call uses the entire 64 kbps (when available). Use this setting if you are placing calls only within North America. Force-56-Yes (1) specifies that the call uses only the 56-kbps portion of a channel. Use this setting when you place calls to European or Pacific Rim countries from within North America and the complete path does not distinguish between the Switched-56 and Switched-64 data services. Force-56-No is the default.
Client-Port-DNIS (30)	Specifies the called-party number, indicating the phone number the user dialed to connect to the MAX TNT.	Telephone number of up to 18 characters, limited to the following: **`1234567890()[]!z-*#|`** The default value is null.
NAS-Port-Type (61)	Specifies the type of service in use for the established session.	NAS_Port_Type_Sync indicates a synchronous ISDN connection. NAS_Port_Type_Async indicates a call the MAX TNT routes to a digital modem. NAS_Port_Type_Async is the default.

Table 5-10. Limiting devices and services (continued)

Attribute	Description	Possible values
User-Service (6)	Specifies whether the link can use framed or unframed services.	Login-User (1) specifies that the caller can use an asynchronous Telnet connection to log into the terminal server. The MAX TNT rejects incoming framed calls. Framed-User (2) specifies that incoming calls must use a framed protocol. Otherwise, the MAX TNT rejects them. Asynchronous Telnet sessions are unframed and therefore not allowed when you specify this value. Dialout-Framed-User (5) specifies that the user profile applies to outgoing calls only. By default, the MAX TNT does not restrict the services that a link can use. **Note:** If User-Service=Framed-User or is unspecified, a user requesting access can dial in with the framing specified by Framed-Protocol. But the user can also dial in unframed, and then change to the Framed-Protocol framing.

To limit access to devices and services for a PPP, MP, or MP+ connection, follow the steps described below. The steps assume you have already set the User-Name and Password attributes, and any other appropriate PPP, MP, or MP+ attributes.

1 Set the User-Service=Framed-User attribute on the first line of the profile.

If RADIUS authenticates an incoming call with the User-Name and Password attributes, and the type of call matches the value of the User-Service attribute, the MAX TNT applies the attributes specified in the user profile. If the type of call does not match the value of the User-Service attribute, the MAX TNT rejects the call.

2 To specify the phone number of the device the caller can access, set the Client-Port-DNIS attribute.

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

4 To specify whether the MAX TNT uses only the 56-kbps portion of a channel, even when all 64 kbps appear to be available, set the Ascend-Force-56 attribute.

Example of restricting service access

The dial-in user in the following example can use PPP protocols (PPP, MP+, or MP), and has no access to the terminal server:

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

Restricting access to ports, lines, and channels

If you want to restrict the ports, lines, and channels that a user can access on a PPP, MP, or MP+ call, set the NAS-Port attribute to the network port on which the MAX TNT received the call.

On the first line of the user profile, specify the User-Name, Password, and NAS-Port attributes. For NAS-Port, use 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.

You must specify a decimal value for each number. This value must translate to a bit-encoded number that specifies each shelf, slot, line, and channel. The default value for the RADIUS daemon appears in the `/etc/services` file.

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.

Example of restricting access to ports, lines, and channels

To restrict an ISDN user to channel 2 on line 2 for slot 2 and shelf 1, use the NAS-Port setting specified in the first line of the following user profile:

```
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 value NAS-Port=1057 translates to the bit-encoded number 0000010000100001. This number indicates the following NAS port:

shelf=00 (shelf 1)

slot=0001 (shelf 2)

line=00001 (line 2)

channel=00001 (channel 2)

Setting up disconnects

If you write a special RADIUS client program to disconnect a link, the MAX TNT can accept RADIUS requests from clients to disconnect a link for a particular session, user, or IP address. The following sections describe how to configure a disconnect request.

Overview of disconnect-request attributes

A RADIUS Disconnect-Request packet (code 40) contains the attributes necessary for making a disconnect request. Table 5-11 lists these attributes.

Table 5-11. Disconnect-request attributes

Attribute	Description	Possible values
Acct-Session-Id (44)	Identifies a bridging, routing, or terminal server session.	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.
Ascend-Session-Svr-Key (151)	Enables the MAX TNT to match a user session with a client request.	Text string of up to 16 characters. The default value is null.
Framed-Address (8)	Specifies the IP address of the user. The MAX TNT disconnects all routing or bridging sessions associated with the specified address. If you specify User-Name as well, the MAX TNT disconnects only routing/bridging sessions associated with both attributes.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The MAX TNT ignores the default address of 0.0.0.0.
User-Name (1)	Specifies the user's name. The MAX TNT disconnects all routing or bridging sessions associated with the user name. If you specify Framed-Address as well, the MAX TNT disconnects only routing/bridging sessions associated with both attributes.	Text string of up to 252 characters. The default value is null. The string need not be null terminated.

The MAX TNT sends the session key and session ID in all RADIUS access requests. You can also obtain the session key, session ID, and user name through RADIUS accounting or from the accounting MIB (for systems that support SNMP accounting). If the MAX TNT assigns the IP address from a pool, RADIUS accounting or the accounting MIB can provide the address as well.

The Auth-Session-Key and Auth-Attribute-Type parameters in the External-Auth profile's Rad-Auth-Server subprofile determine the attributes the MAX TNT uses when handling the disconnect request. For complete information about setting these parameters, see "Specifying session key parameters" on page 3-11.

Configuring attributes for disconnect requests

To set up a RADIUS user profile that requests a disconnect, follow the steps described below. Only the first step is required. All others are optional, and depend upon the needs of your site. None of the attributes may appear more than once. That is, you may not specify two different user names with a single request.

1. Specify the values for the User-Name and Password attributes. These attributes must identify a user at the IP address indicated by the Auth-Client or Auth-Netmask parameters in the External-Auth profile's Rad-Auth-Server subprofile.
2. To identify the session by IP address, set the Framed-Address attribute.
3. To identify the session by its ID number, set the Acct-Session-Id attribute. The number you specify must match the session reference number used in SNMP accounting or RADIUS accounting.
4. To identify the session by a session key, set the Ascend-Session-Svr-Key attribute.

How the MAX TNT handles disconnect requests

The MAX TNT silently discards a Disconnect-Request packet if one of the following conditions is true:

- The packet is badly formatted.
- The client is not on the list of clients allowed to send RADIUS requests to the server.
- The authenticator field is incorrect.
- The packet contains invalid attribute values.

If RADIUS finds at least one session is can disconnect, the response code is 41 (Disconnect-Request-ACK). Otherwise, the code is 42 (Disconnect-Request-NAK). RADIUS does not return any attributes in the response.

Example of configuring disconnects

If two users with the name Steve are logged into the MAX TNT, a request specifying the name Steve disconnects both. A request specifying the session reference number of the first user disconnects only that user.

If there is a four-channel MP session for user Steve at IP address 11.0.0.1, a request specifying IP address 11.0.0.1 and/or the name Steve disconnects all four channels. A request specifying the session reference number associated with one of the four channels disconnects all channels in the MP session. If the request specifies Steve and an address of 11.0.0.2, the MAX TNT returns a NAK because there is no session Steve with that address.

If there is also a terminal-server session for Steve in addition to the four-channel MP session, a request specifying Steve disconnects both. A request specifying Steve and 11.0.0.1 disconnects only the MP session. Likewise, a request specifying 11.0.0.1 disconnects only the MP session.

Setting Up Terminal-Server Connections

6

This chapter, which describes how to configure terminal-server connections, is divided into the following sections:

Before you begin

Before configuring a terminal-server connection in a RADIUS user profile, carry out the following tasks at the MAX TNT configuration interface:

- Specify system-wide settings.
- Enable the appropriate encapsulation methods.
- Specify Terminal-Server profile settings.

The sections that follow briefly describe each task. For complete information, see the *MAX TNT Network Configuration Guide*.

Specifying system-wide settings for a terminal-server connection

To specify system-wide settings for a terminal-server connection, proceed as follows:

1 In the System profile, indicate the MAX TNT unit's name with the Name parameter. You can specify up to 24 characters. The default value is null.

2 Decide whether the MAX TNT should use the Answer-Defaults profile as the default when answering a call. If so, set Use-Answer-For-All-Defaults=Yes in the Answer-Defaults profile. If you accept the default setting of No, the MAX TNT uses the factory defaults.

3 If you are setting up a TCP link between two MAX TNT units, set CLID-Auth-Mode=DNIS-Require in the Answer-Default profile for the MAX TNT at the central switch.

Enabling the encapsulation method for a terminal-server connection

When setting up your connection, select the appropriate encapsulation method(s) in a subprofile of the Answer-Defaults profile. Proceed as follows:

1 If you give the terminal-server operator raw TCP access, makes sure that Enabled=Yes in the TCP-Clear-Answer subprofile.

2 To allow V.120 calls, set V.120=Yes.

3 To allow X.75 calls, set EU-RAW=Yes and EU-UI=Yes.

Specifying Terminal-Server profile settings

To make settings affecting the terminal-server interface, open the Terminal-Server profile. All the settings discussed in this section are optional, and depend upon the needs of your site. Proceed as follows:

1 To specify the type of security that the MAX TNT uses for a remote terminal-server session, set the Security-Mode parameter.

2 To enable users to establish Telnet sessions from the terminal-server interface, set Telnet=Yes in the Terminal-Mode-Configuration > Telnet-Options subprofile.

3 If you want the RADIUS server to remotely configure a login banner and a list of Telnet hosts, set Remote-Configuration=Yes in the Menu-Mode-Options subprofile.

4 To specify whether the operator uses the command-line interface or the menu-driven interface, set the Start-With-Menus parameter, the Toggle-Screen parameter, or both in the Menu-Mode-Options subprofile.

5 To enable users to access PPP from inside the terminal-server interface, set PPP=Yes in the PPP-Mode-Configuration subprofile.

6 To specify that you want to control the use of the MAX TNT unit's digital modems for outgoing calls, set Imm. Modem Auth=User.

Overview of terminal-server connections

A terminal-server connection is a host-to-host link initiated by an analog modem or ISDN modem (such as a V.120 terminal adapter). When the MAX TNT receives a call that uses raw TCP, X.75, V.34, V.42, V.110, or V.120 encapsulation, it removes the encapsulation and then determines whether the call is further encapsulated in PPP.

The terminal server waits briefly to receive a PPP packet. If it times out waiting for PPP, it sends its Login prompt. When it receives a name and password, it authenticates the user with a Connection Profile or RADIUS user profile. If authentication is successful, the MAX TNT routes the call to a digital modem and then forwards it to the terminal server.

A terminal-server call that contains PPP encapsulation is known as an asynchronous PPP call. If the terminal server receives a PPP packet, it does not send the Login prompt. Instead, it responds with a PPP packet. LCP negotiations begin, including PAP, CHAP, or MS-CHAP authentication. If authentication is successful, the MAX TNT forwards the call to the router software, and establishes a regular PPP session. Except for the initial processing, the MAX TNT handles an asynchronous PPP call as any regular PPP call.

Figure 6-1. shows an incoming modem call. A PC running SoftComm initiates the connection. (SoftComm is a program that causes the user's modem to dial into the MAX TNT.) The MAX TNT directs the call to its digital modem, and then forwards the calls to its terminal-server software. In Figure 6-1., the MAX TNT immediately directs the call to a Telnet host.

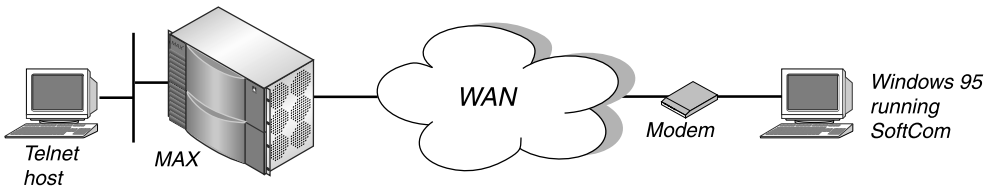


Figure 6-1. A terminal-server connection

When the MAX TNT directs the call to the terminal server, the user sees one of the terminal-server interfaces (command line or menu), or bypasses the terminal-server interface and initiates an immediate Telnet, TCP, or Rlogin connection to a host on the local network.

Note: Most sites restrict dial-in access to the terminal-server interface of the MAX TNT, because a user who has logged into the MAX TNT is able to access status and routing information, and might be able to modify routes.

Overview of terminal-server configuration tasks

All terminal-server tasks are optional. The attributes you configure depend upon the specific needs of your site. You can set RADIUS attributes in a user profile to perform the following tasks:

- Configure Telnet, TCP, and Rlogin connections. (For information, see "Enabling Telnet, TCP, and Rlogin connections" on page 6-4.)
- Set the terminal-server idle timer. (For information, see "Setting the terminal-server idle timer" on page 6-6.)
- Configure menu items and an input prompt. (For information, see "Setting up a custom menu and an input prompt" on page 6-7.)
- Configure message text and a list of hosts to which users can Telnet. (For information, see "Setting up the message text and a list of hosts" on page 6-10.)
- Restrict the use of the MAX TNT unit's digital modems for outgoing calls on a per-user basis. (For information, see "Controlling access to digital modems" on page 6-12.)
- Set up a TCP connection between MAX TNT units. (For information, see "Setting up a TCP link between two MAX TNT units" on page 6-13.)

Enabling Telnet, TCP, and Rlogin connections

The terminal-server software manages dial-in Telnet, TCP, and BSD-style Rlogin connections. You can set them up as regular terminal-server connections, or you can direct them to an IP host immediately so that the dial-in user never sees the terminal-server interface. Telnet, TCP, and Rlogin connections are TCP/IP based.

When you enable Telnet, TCP, and Rlogin connections, you specify the attributes listed in Table 6-1.

Table 6-1. Telnet, TCP, and Rlogin attributes

Attribute	Description	Possible values
Login-Host (14)	Specifies the host to which the user automatically connects when you set User-Service=Login-User and specify a value for the Login-Service attribute.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0. This setting specifies that the user does not automatically connect to a particular host. If you specify Login-Service=Telnet or Login-Service=TCP-Clear, and you do not specify a value for the Login-Host attribute, the MAX TNT unit's response depends on the value of the Auth-TS-Secure parameter in the Rad-Auth-Client subprofile of the External-Auth profile. If Auth-TS-Secure=Yes (the default), the MAX TNT drops the call. If Auth-TS-Secure=No, the MAX TNT allows the caller access to the terminal-server interface. For detailed information about the Auth-TS-Secure parameter, see the *MAX TNT Reference Guide*.

Table 6-1. Telnet, TCP, and Rlogin attributes (continued)

Attribute	Description	Possible values
Login-Service (15)	Specifies the type of terminal-service connection to an IP host that occurs immediately after authentication.	Telnet (0) specifies that the user immediately enters a Telnet session with the host specified by the Login-Host attribute. Rlogin (1) specifies that the user immediately enters an Rlogin session with the host specified by the Login-Host attribute. TCP-Clear (2) specifies a TCP/IP connection with no Telnet protocol. This setting establishes a TCP session, between the MAX TNT and the host specified by Login-Host, over which 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.
Login-TCP-Port (16)	Specifies the port number to which a TCP session connects.	Integer between 1 and 65535. The default value is 23.
Password (2)	Specifies the user's password.	Alphanumeric string of up to 252 characters. The default value is null.
User-Name (1)	Specifies the name of the remote user or device.	Alphanumeric string of up to 252 characters. The default value is null.
User-Service (6)	Specifies whether the link can use framed or unframed services.	Login-User (1) Framed-User (2) Dialout-Framed-User (5) If User-Service=Login-User, the caller cannot use a framed protocol. By default, the MAX TNT does not restrict the services that a link can use.

To enable Telnet, TCP, and Rlogin connections in a RADIUS user profile, proceed as follows:

1 Set User-Service=Login-User on the first line of the user profile, along with the User-Name and Password attributes.

After the terminal server has authenticated an incoming caller, the operator can use an asynchronous Telnet connection to log into the terminal server, and can start Telnet or raw TCP sessions to an IP host on the local network. The MAX TNT rejects incoming framed calls and the caller cannot use any framed protocol.

2 To specify the type of service that user immediately has access to upon login (without ever seeing the terminal-server interface), set the Login-Service attribute.

3 To specify the host to which the user automatically connects, set the Login-Host attribute to an IP address in dotted decimal notation. (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 you specify an IP address, the Login-User never sees the MAX TNT interface, but connects immediately to the specified host via a Telnet, Rlogin, or TCP-Clear connection.

4 If you set Login-Service=TCP-Clear, set the Login-TCP-Port attribute to specify the port number to which a TCP session connects

Example of configuring an Rlogin connection

In the following example, an Rlogin session starts automatically for anyone entering the user name Greg and the password xyzzy:

```
# This profile causes an auto-rlogin to 10.0.200.4 upon login.
Greg    Password="xyzzy"
        User-Service=Login-User,
        Login-Service=Rlogin,
        Login-Host=10.0.200.4,
        ...
```

Setting the terminal-server idle timer

The two terminal-server idle timer settings in a user profile determine the circumstances under which the MAX TNT disconnects a session. You cannot make terminal-server idle-timer settings for a Frame Relay or raw TCP connection.

When you set the terminal-server idle timer, use the attributes listed in Table 6-2.

Table 6-2. Idle-timer attributes

Attribute	Description	Possible values
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.	Integer between 0 and 65535.The default value is 120. A setting of 0 (zero) means that the line can be idle indefinitely.
Ascend-TS-Idle-Mode (170)	Specifies whether the MAX 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-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-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. TS-Idle-Input is the default.

Setting up a custom menu and an input prompt

You can configure the user profile to give the operator a custom menu of items from which to choose, along with an input prompt. The server uses the custom menu to present the user with a subset of terminal-server commands. The user does not have access to the regular menu or to the terminal-server command line.

When you configure a custom menu and input prompt, use the attributes listed in Table 6-3.

Table 6-3. Custom menu and input prompt parameters

Attribute	Description	Possible values
Ascend-Menu-Item (206)	Defines a single menu item that appears in lieu of the terminal-server prompt. You can specify up to 20 Ascend-Menu-Item attributes per profile to give the user a custom menu of items from which to choose. The menu items are displayed in the order in which they appear in the RADIUS profile.	***command*;*text*[;*match*]** where ***command*** is the string sent to the terminal server when the user selects the menu item ***text*** is the text that displays to the user. ***match*** is the pattern the user must type to select the item. By default, the MAX TNT uses the standard terminal-server menu.
Ascend-Menu-Selector (205)	Specifies a string as a prompt for user input in the terminal-server menu interface.	Text string of up to 31 characters. The default is `Enter Selection (1-`*num*`, q)` where *num* is the number of items on the menu.

Specifying the Ascend-Menu-Item attribute

In a RADIUS user profile, you can set one or more Ascend-Menu-Item attributes. Each Ascend-Menu-Item attribute defines a single menu item that appears in lieu of the terminal-server prompt. You can specify up to 20 Ascend-Menu-Item attributes per profile. RADIUS ignores additional entries. The menu items are displayed in the order in which they appear in the RADIUS profile.

Enter your specifications in the following format:

`Ascend-Menu Item="`*`command`*`;`*`text`*`[;`*`match`*`]"`

Table 6-4 lists each argument. If any entry consists of an option containing more that the maximum number of characters allowed, the RADIUS server discards the entry.

Table 6-4. Ascend-Menu-Item arguments

Argument	Description
command	Specifies the string sent to the terminal server when the user selects the menu item. The ***command*** specification must be in a format that the Ascend terminal server understands. It can contain up to 80 characters.
text	Specifies the text that displays to the user. The maximum length for ***text*** is 31 characters.
match	Specifies the pattern the user must type to select the item. The maximum length for ***match*** is 10 characters. 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***.

Specifying the Ascend-Menu-Selector attribute

To specify a string as a prompt for user input in the terminal-server menu interface, set the Ascend-Menu-Selector attribute. By default, when you create a custom menu with the Ascend-Menu-Item attribute, the terminal server displays 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. If you define this attribute, its value overrides the default.

Enter your specification using the following format:

`Ascend-Menu-Selector="`*`string`*`"`

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

Example of configuring custom terminal-server menus

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 unit",
   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 unit
2. Ping server          4. Display ARP Table.
               Option:
```

Now, suppose you also enter specifications for the ***match*** option, as in the following profile:

```
Emma Password="m2dan", User-Service=Login-User
   Ascend-Menu-Item="show ip stats;ip=Display ip stats;ip",
   Ascend-Menu-Item="ping 1.2.3.4;p=Ping server;p",
   Ascend-Menu-Item="telnet 10.2.4.5;t=Telnet to Ken's unit;t",
   Ascend-Menu-Item="show arp;dsp=Display arp table;dsp ",
   Ascend-Menu-Selector="              Option:",
   ...
```

The terminal server displays the following text:

```
ip=Display ip stats          p=Ping server
t=Telnet to Ken's unit       dsp=Display arp table
               Option:
```

Note that you cannot combine numeric menu selections with pattern matching. The first Ascend-Menu-Item attribute determines whether the screen displays numbered selections or patterns. The following example shows what you should *not* do:

```
Emma Password="m2dan", User-Service=Login-User
   Ascend-Menu-Item="show ip stats;ip=Display ip stats",
   Ascend-Menu-Item="ping 1.2.3.4;p=Ping server;p",
   Ascend-Menu-Item="telnet 10.2.4.5;t=Telnet to Ken's unit;t",
   Ascend-Menu-Item="show arp;dsp=Display arp table;dsp ",
   Ascend-Menu-Selector="              Option:",
   ...
```

If you mix numbered selections and pattern matching, the terminal-server screen displays the following text:

```
1. ip=Display ip stats              3. t=Telnet to Ken's unit
2. p=Ping server                    4. dsp=Display arp table
               Option:
```

Setting up the message text and a list of hosts

For terminal-server operators using the standard menu-driven interface, you can specify message text and a list of available Telnet hosts. The message text can contain instructions or other helpful information. The list of hosts consists of each host's IP address and description.

When you set up the message text and list of hosts, you must carry out the following tasks:

- Create the first line of a pseudo-user profile
- Specify the message text
- Specify the list of hosts

Use the attributes listed in Table 6-5.

Table 6-5. Message-text and host-list attributes

Attribute	Description	Possible values
Ascend-Host-Info (252)	Specifies the IP address and name of up to 10 hosts to which the user can establish a Telnet session. (The terminal-server menu-driven interface lists the addresses.)	***IP_address;text*** where ***IP_address*** specifies the IP address of each host, and ***text*** describes each host. The default address is 0.0.0.0/0 and the default description is null.
Password (2)	Specifies the user's password.	Alphanumeric string of up to 252 characters. The default value is null.
Reply-Message (18)	Specifies text that appears to the terminal-server operator using the menu-driven interface. You can specify up to 16 entries per user profile.	Text string of up to 80 characters. The default value is null.
User-Name (1)	Specifies the name of the remote user or device.	Alphanumeric string of up to 252 characters. The default value is null.
User-Service (6)	Specifies whether the link can use framed or unframed services.	Login-User (1) Framed-User (2) Dialout-Framed-User (5) By default, the MAX TNT does not restrict the services that a link can use.

Creating the first line of a pseudo-user profile for the message and list

You create a pseudo-user profile to store information that the MAX TNT can query. In this case, information consists of message text and a list of hosts. You can configure pseudo-users for both global and MAX TNT-specific configuration of the message text and list. The terminal server loads the unit-specific information in addition to the global information.

For a unit-specific configuration, specify the first line of a pseudo-user profile in the following format:

`initial-banner-`*`name`* `Password="ascend", User-Service=Dialout-Framed-User`

where ***`name`*** is the system name of the Ascend unit (the name specified by the Name parameter in the System profile).

For a global configuration, specify the first line of a pseudo-user profile in the following format:

`initial-banner Password="ascend", User-Service=Dialout-Framed-User`

Specifying the message text

To specify message text, set one or more Reply-Message attributes. The maximum number of Reply-Message attributes per profile is 16. Use the following format:

`Reply-Message="`*`string`*`"`

where ***`string`*** is the text of the reply message. Enter up to 80 characters.

Specifying the list of hosts

To specify a list of hosts to which a user can establish a Telnet session, set the Ascend-Host-Info attribute. You can specify up to 10 Ascend-Host-Info entries. Enter your attribute settings in 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.

If you specify a value for the Ascend-Host-Info attribute, you must also make the following settings in the Menu-Mode-Options subprofile of the Terminal-Server profile:

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

Example of configuring message text and a list of hosts

Suppose you have a MAX TNT named Cal that you configure to use a RADIUS server. When Cal boots up, it looks into the RADIUS database for a pseudo-user profile named initial-banner-Cal. If it does not find this pseudo-user profile, it looks for a pseudo-user profile named initial-banner. If it does not find this pseudo-user profile, it uses the value of the Banner parameter in the Terminal-Mode-Configuration subprofile of the Terminal-Server profile.

Whenever a user logs into the MAX TNT unit's terminal server, the screen displays the appropriate message text and list of hosts. Here is an example for a MAX TNT named Cal:

```
initial-banner-Cal Password="ascend", User-Service=Dialout-Framed-User
    Reply-Message="Up to 16 lines of up to 80 characters each",
    Reply-Message="will be accepted. "
    Reply-Message="Additional lines will be ignored.",
    Reply-Message="",
    Ascend-Host-Info="1.2.3.4 Berkeley",
    Ascend-Host-Info="1.2.3.5 Alameda",
    Ascend-Host-Info="1.2.36 San Francisco",
    ...
```

Controlling access to digital modems

The immediate modem feature enables a user to Telnet to a MAX TNT in order to access the MAX TNT unit's modems. The user can place outgoing calls without going through the MAX TNT terminal-server interface. The MAXDial software offers the same outgoing call ability, but through a GUI interface.

Specifying the Ascend-Dialout-Allowed attribute

You can control access to the modems on a per-user basis by setting the Ascend-Dialout-Allowed attribute in a RADIUS user profile. This attribute 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. You can specify one of the following settings:

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

Dialout-Not-Allowed is the default.

Understanding accounting for immediate-modem dialout

When you configure the MAX TNT to use RADIUS accounting, RADIUS generates the appropriate session Start and Stop records for the immediate modem dialout sessions. In the Stop record, the attribute Ascend-Connect-Progress identifies a modem dialout session. The User-Name attribute contains the user name if Imm. Modem Auth=User. If Imm. Modem Auth=Global or None, the User-Name attribute is null. The Acct-Input-Octets attribute specifies the number of bytes the MAX TNT receives from the modem. The Acct-Output-Octets attribute specifies the number of bytes the MAX TNT writes to the modem.

Call accounting does not record outgoing modem calls you make through the terminal-server interface. It applies only to immediate modem calls.

Example of controlling access to digital modems

The following profile enables the user Fred to dial out by means of the MAX TNT unit's digital modems:

```
Fred Password="scr41"
     User-Service=Framed-User,
     Framed-Protocol=PPP,
     Framed-Address=10.0.1.1,
     Framed-Netmask=255.255.255.0,
     Ascend-Metric=2,
     Framed-Routing=None,
     Ascend-Idle-Limit=30,
     Ascend-Dialout-Allowed=Dialout-Allowed
```

Setting up a TCP link between two MAX TNT units

The MAX TNT enables ISPs to receive TCP connections instead of switched calls. A MAX TNT unit at a central switch creates a TCP connection to port 150 on a second MAX TNT at an ISP. The MAX TNT at the ISP treats the connection like a modem connection, routing the call to the terminal-server interface or handling it as an asynchronous PPP session. The user appears to have a connection to the second MAX TNT.

This type of setup bypasses the Public Switched Telephone Network (PSTN). It also has the advantage of concentrating phone calls. For example, if the central switch receives two asynchronous calls, each of which uses 32K of bandwidth, the MAX TNT can handle both calls on one T1 PRI channel.

Figure 6-2. shows a TCP connection between MAX TNT units.

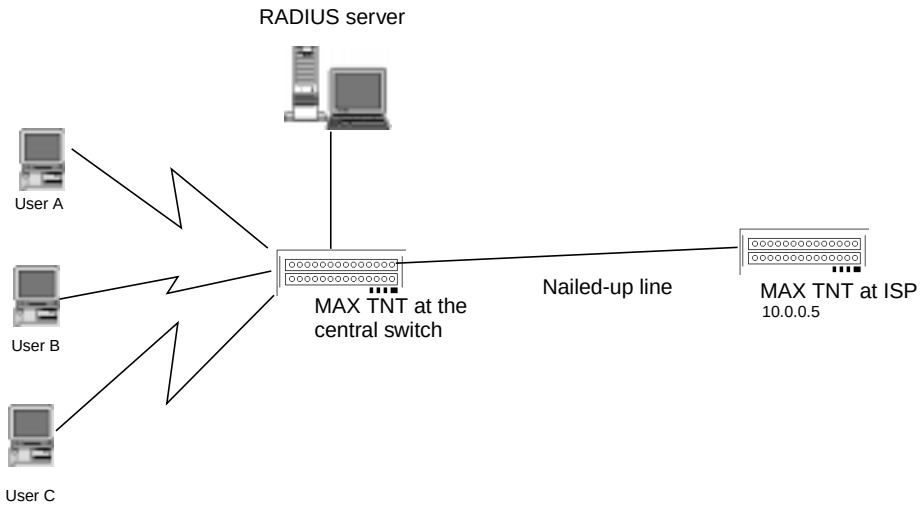


Figure 6-2. A TCP connection between MAX TNT units

Overview of TCP connection attributes

To set up a TCP connection between two MAX TNT units, use the attributes in Table 6-6.

Table 6-6. TCP connection attributes

Attribute	Description	Possible values
Login-Host (14)	Specifies the host to which the user automatically connects when you set User-Service=Login-User and specify a value for the Login-Service attribute.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0. This setting specifies that the user does not automatically connect to a particular host.
Login-Service (15)	Specifies the type of terminal-service connection to an IP host that occurs immediately after authentication.	Telnet (0) specifies that the user immediately enters a Telnet session with the host specified by the Login-Host attribute. Rlogin (1) specifies that the user immediately enters an Rlogin session with the host specified by the Login-Host attribute. TCP-Clear (2) specifies a TCP/IP connection with no Telnet protocol. This setting establishes a TCP session, between the MAX TNT and the host specified by Login-Host, over which 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.
Login-TCP-Port (16)	Specifies the port number to which a TCP session connects.	Integer between 1 and 65535. The default value is 23.
Password (2)	Specifies the user's password.	Alphanumeric string of up to 252 characters. The default value is null.
User-Name (1)	Specifies the name of the remote user or device.	Alphanumeric string of up to 252 characters. The default value is null.
User-Service (6)	Specifies whether the link can use framed or unframed services.	Login-User (1) Framed-User (2) Dialout-Framed-User (5) By default, the MAX TNT does not restrict the services that a link can use.

Configuring the MAX TNT for a TCP connection at the central switch

To configure the MAX TNT at the central switch:

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

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

   where ***phonenum*** represents the called-party number.
2. Set User-Service=Login-User.
3. Set Login-Service=TCP-Clear.
4. Set Login-Host to the IP address of the MAX TNT at the ISP.
5. Set Login-TCP-Port=50.

Configuring the MAX TNT for a TCP connection at the ISP

To configure the MAX TNT at the ISP:

1. Set User-Service=Login-User on the first line of the user profile, along with the User-Name and Password attributes.

   Once the terminal server has authenticated an incoming caller, the operator can use an asynchronous Telnet connection to log into the terminal server, and can start Telnet or raw TCP sessions to an IP host on the local network. The MAX TNT rejects incoming framed calls and the caller cannot use any framed protocol.
2. To specify the type of service that user immediately has access to upon login (without ever seeing the terminal-server interface), set the Login-Service attribute.
3. To specify the host to which the user automatically connects, set the Login-Host attribute to an IP address in dotted decimal notation. (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 you specify an IP address, the Login-User never sees the MAX TNT interface, but connects immediately to the specified host via a Telnet, Rlogin, or TCP-Clear connection.
4. If you set Login-Service=TCP-Clear, set the Login-TCP-Port attribute to specify the port number to which a TCP session connects

Example of configuring a TCP connection between two MAX TNT units

Suppose the MAX TNT at the central switch has the following RADIUS user profile:

```
555-1212 Password="Ascend-DNIS"
         User-Service=Login-User,
         Login-Service=TCP-Clear,
         Login-Host=10.0.0.5,
         Login-TCP-Port=150
```

When the MAX TNT receives a connection from a device at 555-1212, it opens a TCP connection to the specified IP address. The MAX TNT at the ISP receives an incoming TCP connection on port 150 and treats that connection like a modem connection. The second MAX TNT uses the profile that follows to route the call to the terminal-server interface:

```
Jonah  Password="test1"
       User-Service=Login-User,
       Login-Service=TCP-Clear,
       Login-Host=10.0.0.6,
       Login-TCP-Port=9
```

An extended terminal-server example

In this example, a network administrator needs to set up a terminal-server menu giving each user the choice of logging into a BBS or starting PPP, SLIP, or CSLIP. RADIUS is running on a UNIX server. The RADIUS server uses the Default profile to determine the kind of access it grants to users who do not appear in the `users` file.

Note: You can configure only one Default profile in the `users` file. Make sure that the Default profile is last in the file. RADIUS ignores any profiles that follow the Default profile.

The first line of the user profile enables a terminal-server user to log in with his or her UNIX account name or password. The Reply-Message attribute provides introductory message text. The Ascend-Menu-Selector and Ascend-Menu-Item attributes provide each line of menu text.

```
Default Password="UNIX"
   Ascend-Idle-Limit=1800,
   Framed-Routing=None,
   Framed-Compression=Van-Jacobsen-TCP-IP,
   Ascend-Link-Compression=Link-Comp-None,
   Ascend-PPP-VJ-1172=PPP-VJ-1172,
   Ascend-Assign-IP-Pool=1,
   Ascend-Route-IP=Route-IP-Yes,
   Ascend-Route-IPX=Route-IPX-No,
   Ascend-Bridge=Bridge-No,
   Ascend-Handle-IPX=Handle-IPX-None,
   Ascend-Callback=Callback-No,
   Reply-Message="Welcome to ABCNet's Terminal Server."
   Ascend-Menu-Selector="Press q to Quit>>",
   Ascend-Menu-Item="rlogin bbs.net;BBS",
   Ascend-Menu-Item="ppp;Start PPP",
   Ascend-Menu-Item="slip;Start SLIP",
   Ascend-Menu-Item="cslip;Start CSLIP"
```

The following text appears on the terminal-server screen:

```
Welcome to ABCNet's Terminal Server
1. BBS           3. Start SLIP
2. Start PPP     4. Start CSLIP
Press q to Quit>>
```

Notice that pressing the first option causes the MAX TNT to establish an Rlogin session with the BBS at bbs.net.

Instead of using the Default profile, you can configure individual profiles to restrict users from certain services. For example, if you want the user Emma to immediately establish an Rlogin session with bbs.net upon authentication, you might use the following user profile:

```
Emma Password="UNIX"
   User-Service=Login-User,
   Login-Host=bbs.net,
   Login-Service=Rlogin
```

To let new users sign up, you might use a profile like the following:

```
Guest Password="UNIX"
   User-Service=Login-User,
   Login-Host=unix.bbs.net,
   Login-Service=Rlogin
```

When a user dials in as Guest, he or she immediately logs into the UNIX machine. The UNIX machine has a shell `/usr/local/bin/guest` like the following:

```
#!/bin/sh
echo Welcome to BBS.NET.
signup
```

The signup line refers to an interactive shell script you can write in order to gather introductory information, set up a temporary account for verification, and perform any other relevant tasks.

Setting Up Frame Relay Connections

7

This chapter covers the following topics:

Before you begin

Before setting up Frame Relay in RADIUS, you must configure a nailed-up T1 PRI link as the physical interface to the Frame Relay switch. Then, make the following settings in the Answer-Defaults profile:

- Set Profiles-Required=Yes.
- Enable Frame Relay and PPP encapsulation.

For complete information, see the *MAX TNT Network Configuration Guide.*

Using the MAX TNT as a Frame Relay concentrator

In a Frame Relay backbone, every access line must connect directly to a Frame Relay switch. In the past, most connections to the Frame Relay network were relatively high speed, such as full T1 and E1 links. With recent changes in Frame Relay pricing, many sites now want to concentrate many low-speed, dial-in connections into one high-speed, nailed-up connection to a Frame Relay switch. When you configure the MAX TNT as a Frame Relay concentrator, it accepts incoming dial-in connections as usual and forwards them to a Frame Relay switch (as shown in Figure 7-1).

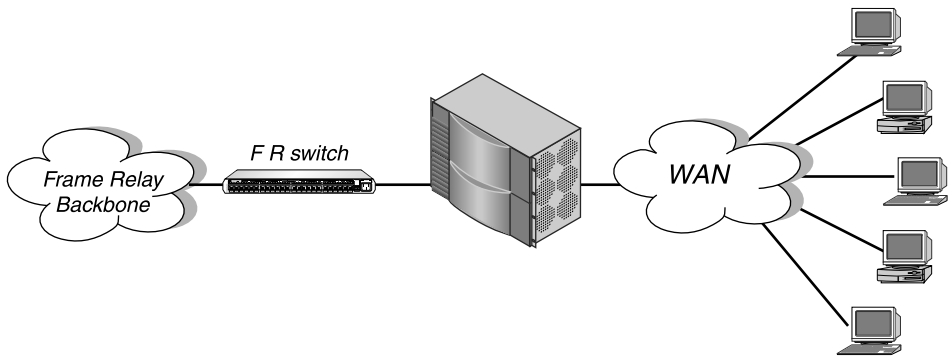


Figure 7-1. The MAX TNT operating as a Frame Relay concentrator

For the MAX TNT to operate as a Frame Relay concentrator, it must appear as a Frame Relay switch to both MAX TNT users and other Frame Relay switches (such as those from Cascade or Stratacom).

Overview of Frame Relay configuration tasks

To set up the MAX TNT as a Frame Relay concentrator, you must carry out the following tasks:

- Set up a logical link between the MAX TNT and the Frame Relay switch. A RADIUS Frame Relay profile defines each logical link. For details, see “Setting up the logical link to a Frame Relay switch” on page 7-3.
- Create one or more Frame Relay user connections that use the logical link. For details, see “Setting up Frame Relay user connections” on page 7-11.

Setting up the logical link to a Frame Relay switch

You must define the link between the MAX TNT and a Frame Relay switch in a RADIUS Frame Relay profile. The MAX TNT accesses the profile at system startup.

This section begins with a description of the types of logical links you can configure. Then, an overview section describes all the attributes you can set for a Frame Relay profile. The remaining sections describe the required and optional steps for configuring the profile, along with detailed examples.

Types of logical links between the MAX TNT and a Frame Relay switch

The MAX TNT supports the following types of interfaces to the Frame Relay network:

- User-to-Network Interface–Data-Circuit-Terminating-Equipment (UNI-DCE)
- User-to-Network Interface–Data Terminal Equipment (UNI-DTE)

The sections that follow describe each type of interface.

UNI-DCE interfaces

UNI is the interface between an end user and a network endpoint (a router or a switch) on the Frame Relay network. In this configuration, illustrated in Figure 7-2, the MAX TNT operates as a Frame Relay router communicating with a DTE device. To the DTE device, the MAX TNT appears as a Frame Relay network endpoint.

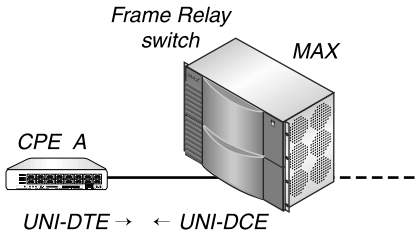


Figure 7-2. UNI-DCE interface

When you set up a MAX TNT in this configuration, it can perform DCE link management functions. The MAX TNT expects to get regular requests for the status of the link. If the MAX TNT does not receive these requests within the expected interval, it considers the link inactive. The MAX TNT responds to these requests with the status of the link identified by the Data Link Connection Indicator (DLCI).

A RADIUS user profile specifies a DLCI for each user connection. A DLCI is a number between 16 and 991 that the Frame Relay administrator assigns. A DLCI is not an address, but a local label that identifies a logical link between a device and a Frame Relay switch. The switch uses the DLCI to route frames through the network. The DLCI can change as frames pass through multiple switches.

(For an example of setting up a RADIUS Frame Relay profile for a UNI-DCE interface, see “Specifying a UNI-DCE interface” on page 7-10.)

UNI-DTE interfaces

In a UNI-DTE connection, the MAX TNT is a DTE communicating with a Frame Relay switch (Figure 7-3). The MAX TNT acts as a Frame Relay feeder and can perform DTE functions for link management.

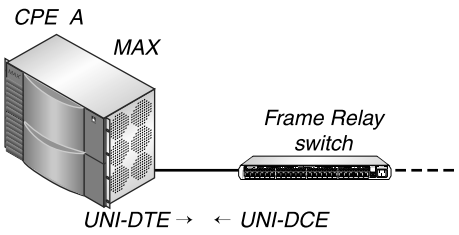


Figure 7-3. UNI-DTE interface

When it performs DTE link management, the MAX TNT regularly requests updates on the status of the link. If the Frame Relay unit at the other end of the link does not respond to the requests, or if the response indicates a DLCI failure, the MAX TNT considers the link inactive.

In addition, the MAX TNT can query the device at the other end of the link about the status of the DLCIs in the connection. If any of the DLCIs becomes unusable and the DLCI's RADIUS user profile specifies a backup connection, the MAX TNT dials the connection.

(For an example of setting up a RADIUS Frame Relay profile for a UNI-DTE interface, see "Specifying a UNI-DTE interface" on page 7-10. For information about setting up a backup connection, see "Setting up a backup profile for a Frame Relay link" on page 7-19.)

Overview of Frame Relay profile attributes

To configure a Frame Relay profile in RADIUS, you create a pseudo-user profile specifying the attributes listed in Table 7-1.

Table 7-1. Frame Relay profile attributes

Attribute	Description	Possible values
Ascend-Call-Type (177)	Specifies the type of nailed-up connection in use.	Nailed (1) Nailed/Mpp (2) Perm/Switched (3) Nailed is the default.
Ascend-Data-Svc (247)	Specifies the type of data service the link uses for outgoing calls.	For a complete list of possible settings, see "Ascend-Data-Svc (247)" on page 14-23. Switched-56K is the default.
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.	Integer between 1 and 10. The default value is 3.

Table 7-1. Frame Relay profile attributes (continued)

Attribute	Description	Possible values
Ascend-FR-DCE-N393 (164)	Specifies the maximum value for the DCE-monitored event count.	Integer between 1 and 10. The default value is 4.
Ascend-FR-DTE-N392 (163)	Specifies the number of errors, occurring during Ascend-FR-DTE-N393-monitored events, that cause the network side to declare the user side's procedures inactive.	Integer between 1 and 10. The default value is 3.
Ascend-FR-DTE-N393 (165)	Specifies a maximum value for the DTE-monitored event count.	Integer between 1 and 10. The default value is 4.
Ascend-FR-Link-Mgt (160)	Specifies the type of Frame Relay link management in use for the profile.	Ascend-FR-No-Link-Mgt (0) Ascend-FR-T1-617D (1) Ascend-FR-Q-933A (2) Ascend-FR-No-Link-Mgt is the default.
Ascend-FR-LinkUp (157)	Specifies whether a link comes up automatically.	Ascend-LinkUp-Default (0) Ascend-LinkUp-AlwaysUp (1) Ascend-LinkUp-Default is the default.
Ascend-FR-N391 (161)	Specifies the interval at which the MAX TNT requests a Full Status Report.	Integer between 1 and 255. The default is 6.
Ascend-FR-Nailed-Grp (158)	Associates a group of nailed-up channels with the Frame Relay profile.	Integer between 1 and the maximum number of nailed-up channels your MAX TNT allows. The default value is 1.
Ascend-FR-T391 (166)	Sets the Link Integrity Verification polling timer.	An integer between 5 and 30. The default value is 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 specified number of seconds.	An integer between 5 and 30. The default value is 15.
Ascend-FR-Type (159)	Specifies the type of Frame Relay connection.	Ascend-FR-DTE (0) Ascend-FR-DCE (1) Ascend-FR-DTE is the default.
Framed-MTU (12)	Specifies the maximum number of bytes the MAX TNT can receive in a single packet.	Integer between 128 and 1600. The default value is 1524.

Table 7-1. Frame Relay profile attributes (continued)

Attribute	Description	Possible values
Password (2)	Specifies the password.	Alphanumeric string of up to 252 characters. The default value is null.
User-Name (1)	Specifies the name of the RADIUS Frame Relay profile.	Alphanumeric string of up to 252 characters. The default value is null.
User-Service (6)	Specifies whether the link can use framed or unframed services.	Login-User (1) Framed-User (2) Dialout-Framed-User (5) By default, the MAX TNT does not restrict the services that a link can use.

Configuring the required attributes for a Frame Relay profile

When you configure a Frame Relay profile, you must specify:

- User-Name, Password, and User-Service attributes
- Nailed-up attributes
- Type of Frame Relay link

Specifying the User-Name, Password, and User-Service attributes

Specify the first line of a pseudo-user profile with the following format:

`frdlink-`*`name`*`-`*`ID`* `Password="ascend", User-Service=Dialout-Framed-User`

where the ***`name`*** argument is the system name of the Ascend unit (the name specified by the Name parameter in the System profile), and ***`ID`*** is a unique string identifying the Frame Relay profile.You must assign IDs in sequence, starting with 1, with no missing numbers. If the numbers are not in sequence, the MAX TNT cannot retrieve them correctly.

On the second line, specify the User-Name attribute to indicate the name of the Frame Relay profile. User connections link up with the Frame Relay profile by indicating the profile name. The name must be unique and cannot exceed 15 characters.

Specifying nailed-up attributes

Set Ascend-Call-Type=Nailed to specify that the link consists entirely of nailed-up channels. Then, set Ascend-FR-Nailed-Grp to specify the group number of the nailed-up channels.

Specifying the type of Frame Relay link

To specify the type of Frame Relay link in use for the profile, set the Ascend-FR-Type attribute.You can specify one of the values listed in Table 7-2.

Table 7-2. Ascend-FR-Type settings

Setting	Specifies
Ascend-FR-DTE (0)	UNI-DTE interface (the default). When you use this value, the MAX TNT acts as a DTE that can connect to a Frame Relay switch.
Ascend-FR-DCE (1)	UNI-DCE interface. When you use this value, the MAX TNT acts as a DCE that can connect to a Frame Relay DTE unit (that is, to the user's CPE).

Configuring optional attributes for a Frame Relay profile

When you set up a Frame Relay profile, you have the option of specifying:

- Automatic link activation
- Link-management protocol in use
- DCE attributes related to the event count and polling cycle
- DTE attributes related to the event count, polling cycle, and status report interval
- Maximum packet size
- Data service

Specifying automatic link activation

To specify whether the link comes up automatically, set the Ascend-FR-LinkUp attribute. You can specify one of the values listed in Table 7-3.

Table 7-3. Ascend-FR-LinkUp settings

Setting	Description
Ascend-LinkUp-Default (0)	Specifies that the link does not come up unless a DLCI brings it up, and that the link shuts down after the last DLCI becomes inactive. This value is the default.
Ascend-LinkUp-AlwaysUp (1)	Specifies that the link comes up automatically and stays up even when the last DLCI becomes inactive

Specifying the link-management protocol

To specify the link-management protocol the MAX TNT should use during communication with the Frame Relay switch, set the Ascend-FR-Link-Mgt attribute. You can specify one of the settings listed in Table 7-4.

Table 7-4. Ascend-FR-Link-Mgt settings

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

Specifying DCE attributes

If Ascend-FR-Type=Ascend-FR-DCE, you can set the attributes listed in Table 7-5.

Table 7-5. DCE attributes

Attribute	Description
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. You can enter an integer between 1 and 10. The default value is 3.
Ascend-FR-DCE-N393 (164)	Specifies the maximum value for the DCE-monitored event count. You can enter an integer between 1 and 10. The default value is 4.
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 specified number of seconds. You can enter an integer between 5 and 30. The default value is 15.

Specifying DTE attributes

If Ascend-FR-Type=Ascend-FR-DTE, you can set the attributes listed in Table 7-6.

Table 7-6. DTE attributes

Attribute	Description
Ascend-FR-N391 (161)	Specifies the interval at which the MAX TNT requests a Full Status Report. You can enter an integer between 1 and 255. The default value is 6.
Ascend-FR-DTE-N392 (163)	Specifies the number of errors, occurring during Ascend-FR-DTE-N393-monitored events, that cause the network side to declare the user side's procedures inactive. You can enter an integer between 1 and 10. The default value is 3.
Ascend-FR-DTE-N393 (165)	Specifies a maximum value for the DTE-monitored event count. You can enter an integer between 1 and 10. The default value is 4.
Ascend-FR-T391 (166)	Sets the Link Integrity Verification polling timer. You can enter an integer between 5 and 30. The default value is 10.

Specifying the maximum packet size

Set the Framed-MTU attribute to the maximum number of bytes the MAX TNT can receive in a single packet. You can enter an integer between 128 and 1600. The default value is 1524.

Specifying the data service

To specify the data service the link can use, set the Ascend-Data-Svc attribute. For a complete list of settings, see "Ascend-Data-Svc (247)" on page 14-23.

Sample RADIUS Frame Relay profile configurations

This section shows a sample RADIUS Frame Relay profile configuration for each type of Frame Relay interface—UNI-DCE and UNI-DTE.

Specifying a UNI-DCE interface

In the following example, the MAX TNT acts as a Frame Relay switch with a UNI-DCE interface to CPE A. Figure 7-4 shows the network connection.

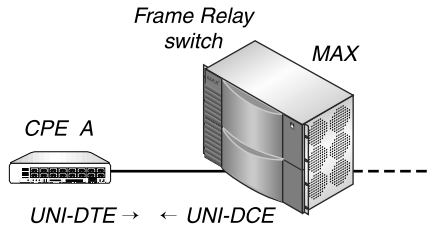


Figure 7-4. UNI-DCE interface to an endpoint (DTE)

To set up a Frame Relay profile called FR Prof 1 with a UNI-DCE interface, enter the following specifications:

```
frdlink-MAXTNT-1 Password="ascend", User-Service=Dialout-Framed-User
     User-Name="FR Prof 1",
     Ascend-FR-Type=Ascend-FR-DCE,
     Ascend-FR-Nailed-Grp=1,
     Ascend-Data-Svc=Nailed-64K,
     Ascend-FR-LinkUp=Ascend-LinkUp-AlwaysUp,
     Ascend-FR-Link-Mgt=Ascend-FR-T1-617D
```

Specifying a UNI-DTE interface

In the following example, the MAX TNT has a nailed connection to a Frame Relay switch. The Frame Relay switch has a UNI-DCE interface, and the MAX TNT has a UNI-DTE interface to that switch. Figure 7-5 shows the connection.

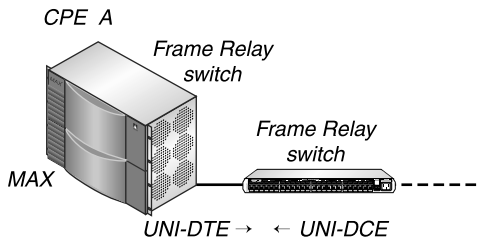


Figure 7-5. UNI-DTE interface to a Frame Relay switch

To set up a Frame Relay profile called FR Prof 2 with a UNI-DTE interface, enter the following specifications:

```
frdlink-MAXTNT-2 Password="ascend", User-Service=Dialout-Framed-User
     User-Name="FR Prof 2",
     Ascend-FR-Type=Ascend-FR-DTE,
     Ascend-FR-Nailed-Grp=1,
     Ascend-Data-Svc=Nailed-64K,
     Ascend-FR-Link-Mgt=Ascend-FR-T1-617D,
     Ascend-FR-N391=20
```

Setting up Frame Relay user connections

You must configure a Frame Relay connection for each user that will access a Frame Relay link.

This section begins by describing the three types of Frame Relay user connections the MAX TNT supports: gateway, circuit, and redirect. Then, an overview section describes all the attributes you must set up for a Frame Relay user connection.

The sections following the attribute overview describe the tasks you must carry out regardless of the type of user connection you wish to configure. The remaining sections then describe the configuration steps necessary for each specific type, and provide sample profiles.

Types of Frame Relay user connections

This section describes the types of Frame Relay user connections you can configure.

Gateway connections

A gateway connection is a bridging or routing link. The MAX TNT receives an incoming PPP call, examines the destination IP address, and brings up the appropriate RADIUS profile to the destination. If the RADIUS user profile specifies Frame Relay encapsulation, a Frame Relay profile, and a DLCI, the MAX TNT encapsulates the packets in Frame Relay (RFC 1490) and forwards the data stream out to the Frame Relay switch. The Frame Relay switch uses the DLCI to route the frames.

Figure 7-6 illustrates a gateway connection.

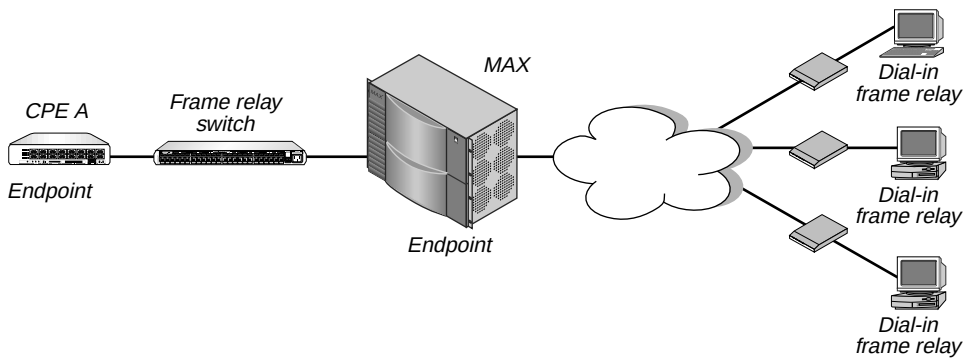


Figure 7-6. Gateway connections

(For information about setting up a RADIUS user profile for a gateway connection, see “Configuring a Frame Relay gateway connection” on page 7-14.)

Circuit connections

A circuit is a connection that follows a specified path through the Frame Relay switch, as shown in Figure 7-7.

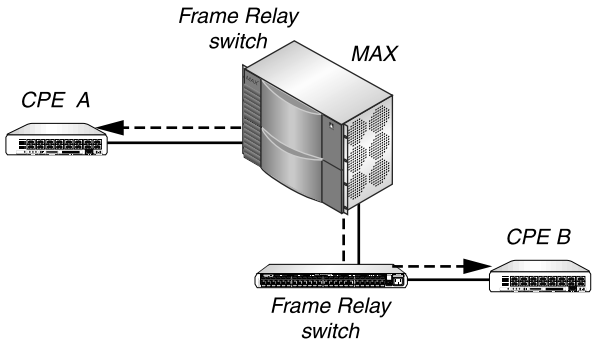


Figure 7-7. Circuit connections

By linking two DLCI endpoints, the MAX TNT creates a Permanent Virtual Circuit (PVC). The two DLCI endpoints act as a tunnel. Data that the MAX TNT receives on one DLCI bypasses the Ascend router and goes out on the other DLCI.

Each endpoint is specified in a RADIUS user profile (or Connection profile). The two DLCIs can use the same Frame Relay profile or different ones. The connection requires two and only two DLCI numbers. The MAX TNT drops data if the circuit has only one DLCI, and uses only two DLCIs if more are configured. The MAX TNT switches data coming in one DLCI to the other DLCI. If any one of the DLCIs in a PVC becomes inactive because of disconnect or failure, the PVC using that DLCI becomes inactive. A physical line can carry multiple DLCIs, and the failure of the line causes the failure of all DLCIs it carries.

For information about setting up a RADIUS user profile for a circuit connection, see “Configuring a Frame Relay circuit connection” on page 7-15.

Redirect connections (rarely used)

When the MAX TNT receives an incoming PPP call for a redirect connection, it ignores the destination IP address in the packet from the dial-in client. Instead, it uses the specified DLCI to route the packet. In effect, the MAX TNT does not route packets from the client in the usual sense. It simply passes them on to the Frame Relay network, and assumes that another device will route the packets on the basis of the destination IP address.

A Frame Relay redirect connection is not a full-duplex tunnel between the PPP dial-in and the switch. The MAX TNT router handles the IP packets coming back from the Frame Relay switch, so the packets must contain the PPP caller’s IP address for proper routing back across the WAN.

This type of connection is not commonly used. (For information about setting up a redirect connection in a RADIUS user profile, see “Configuring a Frame Relay redirect connection” on page 7-15.)

Overview of Frame Relay connection attributes

To configure the Frame Relay user connection in RADIUS, you create a pseudo-user profile by specifying the attributes listed in Table 7-7.

Table 7-7. RADIUS user profile attributes for a Frame Relay connection

Attribute	Description	Possible values
Ascend-FR-Circuit-Name (156)	Specifies the PVC for which this profile is an endpoint.	Text string of up to 15 characters. The default value is null.
Ascend-FR-Direct (219)	Specifies whether the Ascend unit creates a redirect connection to the Frame Relay switch.	FR-Direct-No (0) FR-Direct-Yes (1) FR-Direct-No is the default.
Ascend-FR-Direct-DLCI (221)	Specifies the Data Link Connection Indicator (DLCI) for a redirect connection.	Integer between 16 and 991. The default value is 16.
Ascend-FR-Direct-Profile (220)	Specifies the name of the Frame Relay profile that carries the redirect connection to the Frame Relay switch.	Text string of up to 15 alphanumeric characters. The default value is null.
Ascend-FR-DLCI (179)	Specifies the Data Link Connection Indicator (DLCI) for a gateway or circuit connection.	Integer between 16 and 991. The default value is 16.
Ascend-FR-Profile-Name (180)	Specifies the name of the Frame Relay profile to use in building a gateway or circuit connection.	Text string of up to 15 alphanumeric characters. The default value is null.
Framed-Protocol (7)	Specifies the type of protocol the link can use.	PPP (1) SLIP (2) MPP (256) EURAW (257) EUUI (258) FR (261) FR-CIR (263) By default, the MAX TNT does not restrict the type of protocol a link can use.
Password (2)	Specifies the user's password.	Alphanumeric string of up to 252 characters. The default value is null.
User-Name (1)	Specifies the name of the remote user or device.	Alphanumeric string of up to 252 characters. The default value is null.

Table 7-7. RADIUS user profile attributes for a Frame Relay connection (continued)

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

Configuring any type of Frame Relay user connection

Regardless of the type of Frame Relay user connection you plan to configure, you must carry out the tasks described in this section. Then, to complete the tasks for the specific type of Frame Relay connection you wish to set up, you must refer to the section that describes that type of configuration.

For any type of Frame Relay user connection, create the first line of the pseudo-user profile as follows:

`permconn-`*`name`*`-`*`ID`* `Password="ascend", User-Service=Dialout-Framed-User`

where the ***`name`*** argument is the system name of the Ascend unit (the name specified by the Name parameter in the System profile), and ***`ID`*** is a unique string identifying the user profile. You must assign IDs in sequence, starting with 1, with no missing numbers. If the numbers are not in sequence, the MAX TNT cannot retrieve them correctly.

On the second line of the user profile, set the User-Name attribute to the name of the user that can make the Frame Relay connection.

Configuring a Frame Relay gateway connection

To configure a Frame Relay gateway connection in a RADIUS user profile, follow the steps described below. All steps are required.

1. Perform the tasks described in “Configuring any type of Frame Relay user connection” on page 7-14.
2. Set Ascend-FR-Direct=FR-Direct-No.
3. Set Ascend-FR-Profile-Name to the value of the User-Name attribute that appears on the second line of the Frame Relay profile. This setting indicates the name of the Frame Relay profile the MAX TNT uses when building the connection.
4. Set the Ascend-FR-DLCI attribute to the DLCI value assigned by your Frame Relay network administrator. Each user profile that specifies a gateway connection is a separate logical link and must have a separate DLCI.
5. Set Framed-Protocol=FR.
6. Set Ascend-IP-Route=Route-IP-Yes.
7. Set the Framed-Route attribute to the IP address of the remote router.

Configuring a Frame Relay circuit connection

To set up a Frame Relay circuit connection in a RADIUS user profile, follow the steps described below. All steps are required.

1. Perform the tasks described in "Configuring any type of Frame Relay user connection" on page 7-14.
2. Set Ascend-FR-Profile-Name to the value of the User-Name attribute that appears on the second line of the Frame Relay profile. This setting indicates the name of the Frame Relay profile the MAX TNT uses when building the connection.
3. Set the Ascend-FR-DLCI attribute to the DLCI value assigned by your Frame Relay network administrator. Each user profile that specifies a gateway connection is a separate logical link and must have a separate DLCI.
4. Set Framed-Protocol=FR-CIR.
5. Set Ascend-FR-Circuit-Name to a text string identifying the PVC. Because the MAX TNT connects pairs of links with matching Ascend-FR-Circuit-Name attributes, you must specify the exact same value for Ascend-FR-Circuit-Name in each profile.
6. Configure the routing or bridging setup in the MAX TNT for the WAN connection.

   (For details, see Chapter 9, "Setting Up IP Routing for WAN Links," Chapter 10, "Setting Up IPX Routing for WAN Links," and Chapter 11, "Setting Up Bridging for WAN Links," in this guide, and the relevant chapters of the *MAX TNT Network Configuration Guide.)*

Configuring a Frame Relay redirect connection

To configure a Frame Relay redirect connection in a RADIUS user profile, follow the steps described below. All steps are required.

1. Perform the tasks described in "Configuring any type of Frame Relay user connection" on page 7-14.
2. Set Ascend-FR-Direct=FR-Direct-Yes.
3. Set Ascend-FR-Direct-Profile to the value of the User-Name attribute that appears on the second line of the Frame Relay profile. This setting indicates the name of the Frame Relay profile the MAX TNT uses when building the connection.
4. Set the Ascend-FR-Direct-DLCI attribute to indicate the DLCI that identifies the user profile to the Frame Relay switch. Many redirect connections can use the same DLCI.
5. Set Framed-Protocol=PPP.
6. Configure the incoming PPP or MP+ connection as described in "Setting up a dial-in PPP, MP, or MP+ connection" on page 5-5.
7. Configure the routing or bridging setup in the MAX TNT for the WAN connection.

   (For details, see Chapter 9, "Setting Up IP Routing for WAN Links," Chapter 10, "Setting Up IPX Routing for WAN Links," and Chapter 11, "Setting Up Bridging for WAN Links," in this guide, and the relevant chapters of the *MAX TNT Network Configuration Guide.)*

Sample RADIUS Frame Relay user profile configurations

This section shows a Frame Relay user profile for each type of user connection—gateway, circuit, and redirect.

Specifying a gateway connection

The following example shows how to set up a Frame Relay gateway connection for the configuration in Figure 7-8.

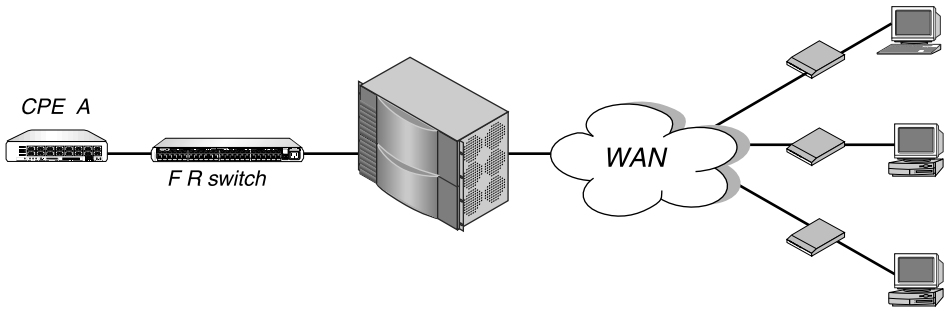


Figure 7-8. A gateway connection

In this example, the MAX TNT uses a Frame Relay profile named PacBell to communicate with a remote Frame Relay switch:

```
frdlink-MAXTNT-1 Password="ascend", User-Service=Dialout-Framed-User
   User-Name="PacBell",
   Ascend-FR-Type=Ascend-FR-DTE,
   Ascend-FR-Nailed-Grp=1,
   Ascend-FR-Link-Mgt=Ascend-FR-T1-617D,
   Ascend-FR-N391=20
```

To configure user profiles for the clients connecting to the remote IP network, specify the following settings:

```
permconn-MAXTNT-1 Password="ascend", User-Service=Dialout-Framed-User
   Framed-Protocol=FR,
   User-Name-"Terry",
   Ascend-FR-Profile-Name="PacBell",
   Ascend-FR-DLCI=57,
   Ascend-Route-IP=Route-IP-Yes,
   Framed-Route="10.0.200.33/29 10.0.200.37 1 n remote_router "

permconn-MAXTNT-2 Password="ascend", User-Service=Dialout-Framed-User
   Framed-Protocol=FR,
   User-Name-"Stephanie",
   Ascend-FR-Profile-Name="PacBell",
   Ascend-FR-DLCI=57,
   Ascend-Route-IP=Route-IP-Yes,
   Framed-Route="10.0.200.33/29 10.0.200.37 1 n remote_router "
```

```
permconn-MAXTNT-3 Password="ascend", User-Service=Dialout-Framed-User
   Framed-Protocol=FR,
   User-Name-"Catherine",
   Ascend-FR-Profile-Name="PacBell",
   Ascend-FR-DLCI=57,
   Ascend-Route-IP=Route-IP-Yes,
   Framed-Route="10.0.200.33/29 10.0.200.37 1 n remote_router "
```

Specifying a circuit connection

The following configuration sets up a circuit between UNI-DCE and UNI-DTE interfaces. The sample network looks like the one in Figure 7-9.

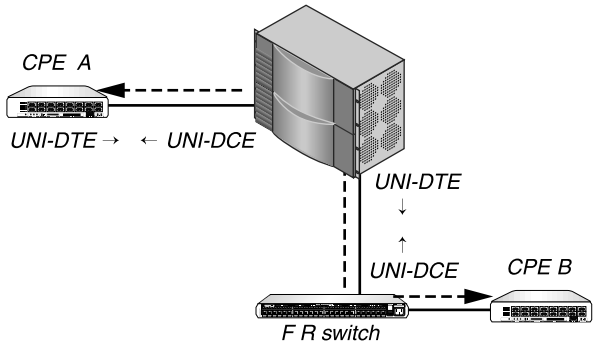


Figure 7-9. A Frame Relay circuit

The Frame Relay profile for the UNI-DCE interface in the MAX TNT is named FR Prof 1. For the UNI-DTE interface, the Frame Relay profile is named FR Prof 2.

The following Frame Relay profile specifies the UNI-DCE interface:

```
frdlink-MAXTNT-1 Password="ascend", User-Service=Dialout-Framed-User
   User-Name="FR Prof 1",
   Ascend-FR-Type=Ascend-FR-DCE,
   Ascend-FR-Nailed-Grp=1,
   Ascend-FR-LinkUp=Ascend-LinkUp-AlwaysUp,
   Ascend-FR-Link-Mgt=Ascend-FR-T1-617D
```

The following Frame Relay profile specifies the UNI-DTE interface:

```
frdlink-MAXTNT-2 Password="ascend", User-Service=Dialout-Framed-User
   User-Name="FR Prof 2",
   Ascend-FR-Type=Ascend-FR-DTE,
   Ascend-FR-Nailed-Grp=1,
   Ascend-FR-LinkUp=Ascend-LinkUp-AlwaysUp,
   Ascend-FR-Link-Mgt=Ascend-FR-T1-617D
```

The two user profiles are called Endpoint1 and Endpoint2:

```
permconn-MAXTNT-1 Password="ascend", User-Service=Dialout-Framed-User
   Framed-Protocol=FR-CIR,
   User-Name="EndPoint1",
   Ascend-FR-Profile-Name="FR Prof 1",
   Ascend-FR-DLCI=16,
   Ascend-FR-Circuit-Name="Circuit1"
```

```
permconn-MAXTNT-2 Password="ascend", User-Service=Dialout-Framed-User,
   Framed-Protocol=FR-CIR,
   User-Name="EndPoint2",
   Ascend-FR-Profile-Name="FR Prof 2",
   Ascend-FR-DLCI=23,
   Ascend-FR-Circuit-Name="Circuit1"
```

Setting Framed-Protocol=FR-CIR specifies that the packets the MAX TNT transmits and receives over the link do not go through the MAX TNT unit's bridge/router. Setting the Ascend-FR-Circuit-Name attribute to the same value in both user profiles tells the MAX TNT to pass packets transparently between FR Prof 1 (DLCI 16) and FR Prof 2 (DLCI 23).

Specifying a redirect connection

The following example shows how to configure two PPP dial-in connections for the MAX TNT to redirect to the Frame Relay network (Figure 7-10).

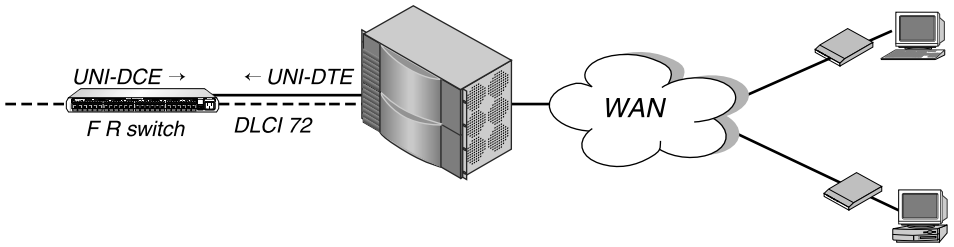


Figure 7-10. Redirect connection

In this example, the MAX TNT uses a Frame Relay profile named PacBell to communicate with a Frame Relay switch:

```
frdlink-MAXTNT-1 Password="ascend", User-Service=Dialout-Framed-User
   User-Name="PacBell",
   Ascend-FR-Type=Ascend-FR-DTE,
   Ascend-FR-Nailed-Grp=1,
   Ascend-FR-Link-Mgt=Ascend-FR-T1-617D,
   Ascend-FR-N391=20
```

To set up the user profiles for the redirect connection that uses DLCI 72, enter the following specifications:

```
permconn-MAXTNT-1 Password="ascend", User-Service=Dialout-Framed-User
   Framed-Protocol=PPP,
   User-Name="Michael",
   Ascend-FR-Direct-Profile="PacBell",
   Ascend-FR-DLCI=72

permconn-MAXTNT-2 Password="ascend", User-Service=Dialout-Framed-User
   Framed-Protocol=PPP,
   User-Name="Grace",
   Ascend-FR-Direct-Profile="PacBell",
   Ascend-FR-DLCI=72
```

Setting up a backup profile for a Frame Relay link

You can set the Ascend-Backup attribute in a user profile to bring up a backup connection when any of the DLCIs become unusable.

For example, consider the Frame Relay configuration in Figure 7-11. The MAX TNT connects to two remote routers, DTE 1 and DTE 2, through the Frame Relay switch. The PVC to DTE 1 consists of DLCIs 34 and 38, while the PVC to DTE 2 consists of DLCIs 33 and 39.

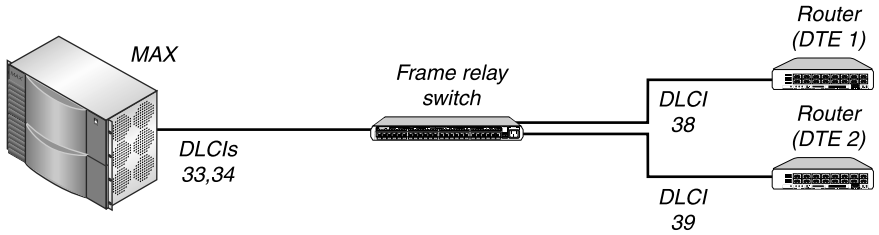


Figure 7-11. Configuring a backup profile for a Frame Relay link

Suppose DTE 2 suddenly becomes unreachable, either because the link between the Frame Relay switch and DTE 2 fails, or because the link between the Ascend unit and the Frame Relay switch fails. In either case, the Ascend unit brings up the backup for DTE 2 (specifically, the backup for the user profile that uses DLCI 33 or 39).

To set up a backup profile for a Frame Relay link, use the attributes listed in Table 7-8.

Table 7-8. Backup attributes

Attribute	Specifies	Possible values
Ascend-Backup (176)	Name of a backup profile for a nailed-up link whose physical connection fails.	Text string. The default value is null.
Ascend-FR-Type (159)	Type of Frame Relay connection.	Ascend-FR-DTE (0) Ascend-FR-DCE (1) Ascend-FR-DTE is the default.
Ascend-Idle-Limit (244)	Number of seconds the MAX TNT waits before clearing a call when a session is inactive.	Integer between 0 and 65535. The default value is 120. If you accept the default, and the Answer-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.

If the primary connection is a nailed-up link to a Frame Relay switch, proceed as follows:

1. In the Frame Relay profile for the primary connection, set Ascend-FR-Type= Ascend-FR-DTE or Ascend-FR-DCE.
2. In the user profile, set the Ascend-Backup attribute to the name of the backup RADIUS user profile.
3. In the backup RADIUS user profile, set the Ascend-Idle-Limit attribute.

   When the MAX TNT restores the primary nailed-up connection, it redirects traffic to the link, idling the secondary connection. The MAX TNT releases the secondary connection after the period of time specified by the Ascend-Idle-Limit attribute.

Setting Up Ascend Tunnel Management Protocol (ATMP)

8

This chapter covers the following topics:

Introducing Ascend Tunnel Management Protocol (ATMP)

ATMP is a UDP/IP-based protocol that provides a tunnelling mechanism between two Ascend units across the Internet or a Frame Relay network. Each Ascend unit can be a MAX TNT or a Pipeline 400. The protocol uses standard Generic Routing Encapsulation (GRE).

ATMP provides a Virtual Private Network (VPN) solution over the backbone resources of Internet Service Providers (ISPs) and carriers. Without ATMP, each mobile node and remote user has to dial directly into the network, resulting in long-distance charges. With ATMP, these users can make a local call and have the transmission securely tunnelled across the Internet or Frame Relay network.

As described in RFC 1701, GRE hides packet contents and enables transmission of packets that the Internet would otherwise not accept. When you use ATMP with the MAX TNT, these include IP packets that use unregistered addresses or IPX packets from roaming clients.

How ATMP connections work

ATMP creates and tears down the tunnel between two Ascend units. In effect, the tunnel collapses the Internet cloud and provides what looks like direct access to a home network from a remote node. ATMP applies only to IP or IPX networks.

Figure 8-1. shows a sample ATMP tunnel connection.

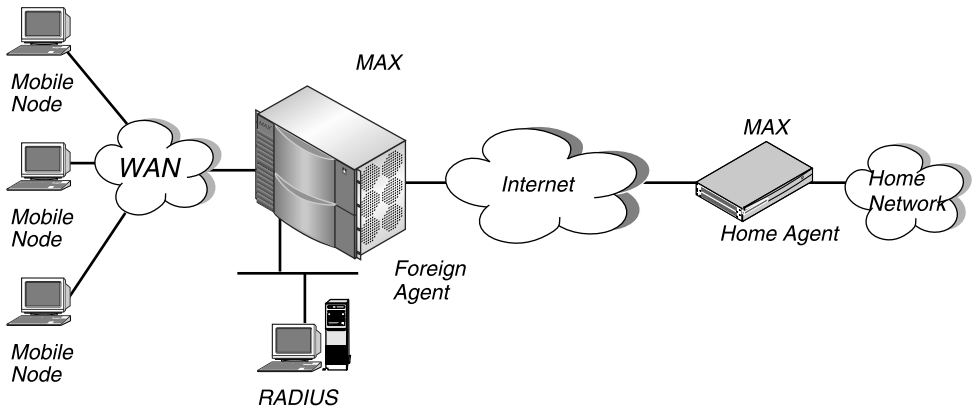


Figure 8-1. Sample cross-Internet ATMP tunnel

Table 8-1 lists the network elements that work together in an ATMP connection.

Table 8-1. ATMP network elements

Element	Description
Home network	A private corporate network. A private network is one that cannot communicate directly on the Internet. It might be an IPX network, or an IP network with an unregistered network number.
Mobile node	A user who accesses a private home network across the Internet. The mobile node could be a salesperson on the road who dials into a local ISP and logs into his or her home network.
Foreign agent	An Ascend unit that the mobile node dials into. It is the starting point of the ATMP tunnel. The foreign agent must be able to bring up an IP connection to the home agent, and it must authenticate the mobile node by means of a RADIUS user profile that includes ATMP attributes.
Home agent	An Ascend unit that represents the terminating part of the tunnel. It must be able to communicate with the home network directly, through another router, or across a nailed-up WAN connection.

To establish an ATMP connection with the home network, a mobile node initiates the following sequence of events:

1 The mobile node dials a connection to the foreign agent.

2 The foreign agent authenticates the mobile node by means of a RADIUS user profile.

3 The foreign agent locates a Connection profile or RADIUS user profile for the home agent.

4 The foreign agent connects to the home agent through a regular IP connection. The MAX TNT authenticates the connection in the usual way (for example, by using CHAP).

5 The foreign agent informs the home agent that the mobile node has connected, and requests a tunnel.

6 The foreign agent sends up to ten RegisterRequest messages at two-second intervals, timing out and logging a message if it receives no response to the requests.

7 The home agent requests authentication of the mobile node, by sending a challenge request to the foreign agent.

8 The foreign agent sends back a challenge reply to the home agent. The reply includes an encrypted version of the Ascend-Home-Agent-Password value in the mobile node's RADIUS profile. This password must match the value of the home agent's ATMP-Home-Agent-Password parameter in the ATMP subprofile of the IP-Interface profile.

9 The home agent returns a RegisterReply with a number that identifies the tunnel. If registration fails, the home agent logs a message and the foreign agent disconnects the mobile node. If registration succeeds, the MAX TNT creates a tunnel between the foreign agent and the home agent. At this point, the mobile node connects to the home network as though it had dialed locally, and can transfer data across the tunnel.

10 When the mobile node disconnects from the foreign agent, the foreign agent sends a DeregisterRequest to the home agent to close down the tunnel. The foreign agent can send its request a maximum of ten times, or until it receives a DeregisterReply. If the foreign agent receives packets for a mobile node whose connection has gone down, the foreign agent silently discards the packets.

ATMP router and gateway modes

You can configure the home agent as a router or a gateway to the home network.

Router mode

When you configure the home agent as a router, the home agent's routing module forwards packets it receives from the foreign agent onto the local network. The network can be the home network, or it can support another router that can connect to the home network. In either case, packet delivery relies on a routing mechanism, such as a static or dynamic route, and not on a WAN connection.

In the case of routing an IPX packet from the mobile node, the home agent must see the mobile node as connected to another IPX network. ATMP adds this virtual IPX network to the home agent's routing table on the basis of the IPX attributes it receives from the foreign agent. The RADIUS user profile for the mobile node must specify the IPX network number unique within the enterprise.

Gateway mode

When you configure the home agent as a gateway, the home agent tunnels packets from the foreign agent to the home network across an open WAN connection, as illustrated in Figure 8-2..

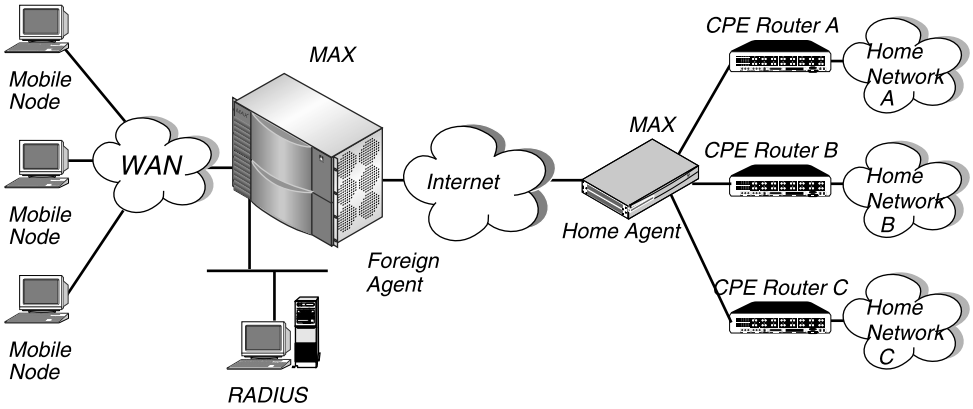


Figure 8-2. Gateway mode configuration

The WAN connection must be on line. The home agent does not bring up a WAN connection to the home network in response to a packet it receives through the tunnel. For this reason, the home agent must have a nailed-up WAN connection to the home network.

Overview of ATMP configuration tasks

To set up a basic ATMP tunnel across an IP or IPX connection, you must perform the tasks described in “Setting up an ATMP tunnel for an IP or IPX network” on page 8-6.

Depending on your configuration, you have the option of carrying out the following additional tasks:

- Configure an ATMP tunnel between two IP networks. (For information, see “Tunneling ATMP between two IP networks” on page 8-12.)
- Configure the MAX TNT to operate as either a foreign agent or a home agent. (For information, see “Setting up the MAX TNT as a multimode agent” on page 8-13.)
- Configure ATMP to completely bypass a foreign agent. (For information, see “Setting up ATMP to bypass a foreign agent” on page 8-14.)

Overview of ATMP attributes

The foreign agent must have a RADIUS user profile that authenticates the mobile node and specifies attributes listed Table 8-2.

Table 8-2. RADIUS attributes for ATMP connections

Attribute	Specifies	Possible values
Ascend-Home-Agent-Password (184)	Password that the foreign agent sends to the home agent during ATMP operation. Must match the home agent’s ATMP password.	Text string of up to 20 characters. The default value is null.
Ascend-Home-Network-Name (185)	Name of the Connection profile for the home agent’s nailed-up connection to the home network (required only if the home agent is operating in gateway mode).	Text string. The default value is null.
Ascend-IPX-Node-Addr (182)	Unique IPX node address on the network specified by Framed-IPX-Network. This value completes the IPX address of a mobile node.	12-digit ASCII string. The default value is 000000000001.
Framed-IPX-Network (23)	Virtual IPX network required for the home agent to route IPX packets to the mobile node. This network must be unique in the IPX routing domain.	Decimal value representing the IPX network number of the IPX router at the remote end of the connection. The default value is null.

Table 8-2. RADIUS attributes for ATMP connections (continued)

Attribute	Specifies	Possible values
Ascend-Primary-Home-Agent (129)	First home agent the foreign agent tries to reach when setting up an ATMP tunnel, and indicates the UDP port the foreign agent uses for the link. Both the home agent and the foreign agent must agree on the UDP port number.	**"*hostname* | *ip_address* [:*udp_port*]"** The ***hostname*** argument indicates the home agent's symbolic hostname. The default value is null. The ***ip_address*** argument indicates the home agent's IP address in dotted decimal notation. Specify an IP address if no DNS server exists for the home agent. You can specify a hostname or an IP address, but not both. The default value is 0.0.0.0. The optional ***udp_port*** argument indicates the UDP port on which the foreign agent communicates with the home agent. The default value is 5150. The colon (:) separates the hostname or IP address from the UDP port specification.
Ascend-Secondary-Home-Agent (130)	Secondary home agent the foreign agent tries to reach when the primary home agent (specified by Ascend-Primary-Home-Agent) is unavailable. Also indicates the UDP port the foreign agent uses for the link.	Same values as Ascend-Primary-Home-Agent.

Setting up an ATMP tunnel for an IP or IPX network

A private IP network is a network with an unregistered IP address. An ATMP tunnel enables a remote user to log into a private IP network across the Internet through a local ISP connection. An ATMP tunnel also enables a remote NetWare client to log into a corporate IPX network across the Internet by means of a local ISP connection.

Configuring the foreign agent

To configure the foreign agent for an IP or IPX tunnel, you must perform the following tasks:

- At the MAX TNT interface, set up ATMP in the foreign agent's IP-Interface profile.
- Configure the foreign agent to authenticate through RADIUS.
- Configure an outgoing RADIUS user profile to the home agent. (Instead of an outgoing RADIUS user profile, you can set up a Connection profile to the home agent. For details, see the *MAX TNT Network Configuration Guide*.)
- Create an incoming RADIUS user profile for the mobile node.

Then, depending on whether you are creating an IP or IPX tunnel, you must carry out one of the following additional tasks:

- For an IP tunnel, specify IP attributes for the mobile node's user profile.
- For an IPX tunnel, specify additional IPX attributes for the mobile node's user profile.

Configuring ATMP in the foreign agent's IP-Interface profile

To configure ATMP in the foreign agent's IP-Interface profile, perform the following tasks at the MAX TNT configuration interface:

1 Open the ATMP subprofile.

2 Set ATMP-Agent-Mode=ATMP-Foreign-Agent.

3 Set the ATMP-UDP-Port parameter to specify a UDP port number, or accept the default of 5150.

4 Save your changes.

Configuring the foreign agent to authenticate through RADIUS

To configure the foreign agent to authenticate through RADIUS, follow the instructions in "Configuring the MAX TNT to use the RADIUS server" on page 3-6.

Configuring an outgoing RADIUS user profile to the home agent

For the foreign agent, you must create an outgoing user profile to the home agent. Some configuration steps are required. Some steps are optional, and depend upon the needs of your site. To set required attributes in the foreign agent's outgoing RADIUS user profile, proceed as follows:

1 On the first line of the user profile, set the User-Name attribute to the name of the home agent, and append **`-Out`** to the user name.

2 Next to the User-Name specification, set Password="Ascend" and User-Service=Dialout-Framed-User.

3 On the second line of the user profile, set the User-Name attribute to the name of the home agent, without appending **`-Out`** to the user name.

4 Set the Framed-Protocol attribute to the encapsulation type in use on the line.

5 Set Ascend-Route-IP=Route-IP-Yes to enable IP routing.

6 Set the Ascend-Dial-Number attribute to the phone number the MAX TNT dials to reach the home agent.

To set optional attributes in the foreign agent's outgoing RADIUS user profile, proceed as follows:

1 Set the Framed-Address attribute to the foreign agent's IP address. If a subnet mask is in use, set the Framed-Netmask attribute as well.

2 Set the Framed-Routing attribute to specify RIP behavior.

3 Set the Ascend-Idle-Limit attribute to specify the number of seconds the MAX TNT waits before clearing a call when a session is inactive.

4 Set the Ascend-PRI-Number-Type attribute to the type of phone number the MAX TNT dials.

5 Set the Ascend-Send-Auth attribute to the authentication protocol 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.

6 If you request PAP or CHAP authentication, you must also specify a password with Ascend-Send-Secret or Ascend-Send-Passwd. (Use Ascend-Send-Passwd only if your version of the MAX TNT does not support Ascend-Send-Secret.)

Example of outgoing RADIUS user profile to the home agent

The following user profile enables a MAX TNT to dial calls to the device at 1-800-555-5555:

```
Alameda-Out Password="ascend", User-Service=Dialout-Framed-User
     User-Name="Alameda",
     Framed-Protocol=PPP,
     Ascend-Route-IP=Route-IP-Yes,
     Framed-Address=10.0.100.1,
     Framed-Netmask=255.255.255.0,
     Framed-Routing=None,
     Ascend-Idle-Limit=30,
     Ascend-Dial-Number=1-800-555-5555,
     Ascend-PRI-Number-Type=National-Number,
     Ascend-Send-Auth=Send-Auth-PAP,
     Ascend-Send-Secret="Password1"
```

Configuring an incoming RADIUS profile for the mobile node

Whether you are routing IP or IPX, you must create a RADIUS users profile for the mobile node. Proceed as follows:

1 Set the User-Name attribute to the name of the mobile node.

2 Set the Password attribute to the mobile node's password.

3 Set the Framed-Protocol attribute to the type of encapsulation in use for the call.

4 Set the Ascend-Primary-Home-Agent attribute to the IP address of the first home agent the foreign agent tries to reach when setting up the ATMP tunnel. You can also indicate the UDP port the foreign agent uses for the link. If you specify a non-default UDP port number in one unit's configuration, make sure that the other end of the tunnel specifies the same number.

5 Set the Ascend-Secondary-Home-Agent attribute.

6 Set the Ascend-Home-Agent-Password attribute to the home agent's password. You must specify the same password indicated by the home agent's ATMP-Home-Agent-Password parameter in the ATMP subprofile of the IP-Interface profile.

7 In gateway mode, set the Ascend-Home-Network-Name attribute to the home agent's resident Connection profile. The Connection profile must have the ATMP-Gateway parameter set to Yes in the Session-Options subprofile.

Specifying IP routing attributes in the mobile node's user profile

For an IP tunnel, specify the following additional attributes in the mobile node's user profile:

1. Set Ascend-Route-IP=Route-IP-Yes to enable IP routing.
2. Set the Framed-Address attribute to he mobile node's IP address.
3. If a subnet mask is in use on the network, set the Framed-Netmask attribute.

Specifying IPX routing attributes in the mobile node's user profile

The foreign agent must specify a virtual IPX network number for its mobile nodes. The network number must be unique within the IPX routing domain. Typically, the foreign agent's RADIUS profiles for mobile nodes all use the same virtual IPX network, with unique IPX node addresses on that virtual network. When the home agent receives IPX packets through the ATMP tunnel, it adds the unique virtual network number to its routing table.

For an IPX tunnel, specify the following additional attributes in the mobile node's user profile:

1. Set Ascend-Route-IPX=Route-IPX-Yes to enable IPX routing.
2. If the caller is a dial-in PPP client, set Ascend-IPX-Peer-Mode=IPX-Peer-Dialin.
3. Set the Framed-IPX-Network attribute to a unique, virtual IPX network number. You must specify the IPX network number in decimal format, not hexadecimal. All mobile nodes logging into an IPX home network through the same foreign agent typically use the same Framed-IPX-Network number.
4. Set the Ascend-IPX-Node-Addr attribute to a unique IPX node address on the Framed-IPX-Network. The number you indicate must be unique for each mobile node on the virtual IPX network.

Example of mobile node configuration for IP tunneling in router mode

The following user profile specifies a mobile node in router mode and a single home agent at the IP address 10.9.8.10:

```
Node1 Password="Top-secret"
      Framed-Protocol=PPP,
      Ascend-IP-Route=Route-IP-Yes,
      Framed-Address=200.1.1.2,
      Framed-Netmask=255.255.255.0,
      Ascend-Primary-Home-Agent=10.8.9.10,
      Ascend-Secondary-Home-Agent=10.8.9.11,
      Ascend-Home-Agent-Password="private"
```

When the mobile node logs into the foreign agent with the password Top-secret, the foreign agent authenticates the mobile node. The foreign agent then looks for a profile with an IP address that matches the Ascend-Primary-Home-Agent value. When it finds such a profile, it brings up an IP connection to the home agent.

Example of mobile node configuration for IP tunneling in gateway mode

The following profile specifies a mobile node in gateway mode and a single home agent at the IP address 10.9.8.10. The home agent uses the Homenet Connection profile to the home network.

```
Node2 Password="Top-secret"
      Framed-Protocol=PPP,
      Ascend-Route-IP=Route-IP-Yes,
      Framed-Address=200.1.1.2,
      Framed-Netmask=255.255.255.0,
      Ascend-Primary-Home-Agent=10.8.9.10,
      Ascend-Secondary-Home-Agent=10.8.9.11,
      Ascend-Home-Agent-Password="private",
      Ascend-Home-Network-Name="Homenet"
```

Note that for an ATMP gateway mode connection, you must set Ascend-Home-Network-Name to specify the name of the home agent's Connection profile to the home network.

Example of mobile node configuration for IPX tunneling in gateway mode

The following profile specifies a mobile node named Node2 and a single home agent at the IP address 10.9.8.10. The home agent uses the Homenet Connection profile to the home network, and the mobile node uses a virtual IPX network number of 4999.

```
Node2 Password="Top-secret"
     Framed-Protocol=PPP,
     Ascend-Route-IPX=Route-IPX-Yes,
     Ascend-IPX-Peer-Mode=IPX-Peer-Dialin,
     Framed-IPX-Network=4999,
     Ascend-IPX-Node-Addr="001122334567",
     Ascend-Primary-Home-Agent=10.8.9.10,
     Ascend-Secondary-Home-Agent=10.8.9.11,
     Ascend-Home-Agent-Password="private",
     Ascend-Home-Network-Name="Homenet"
```

Configuring the home agent

To configure the home agent, you must perform the following tasks:

- At the MAX TNT configuration interface, set up ATMP in the home agent's IP-Interface profile.
- Configure an outgoing RADIUS user profile to the foreign agent. (Instead of an outgoing RADIUS user profile, you can set up a Connection profile to the foreign agent. For details, see the *MAX TNT Network Configuration Guide*.)
- Configure a nailed-up Connection profile to the home network. The Connection profile to the home network must be a resident profile. You cannot configure this profile in RADIUS.

Configuring ATMP in the home agent's IP-Interface profile

To configure ATMP in the home agent's IP-Interface profile, perform the following tasks at the MAX TNT configuration interface:

1. Open the ATMP subprofile.
2. Set ATMP-Agent-Mode=ATMP-Home-Agent.
3. For a home agent in router mode, set ATMP-Agent-Type=ATMP-Home-Agent-Router.
4. For a home agent in gateway mode, set ATMP-Agent-Type=ATMP-Home-Agent-Gateway.
5. Set ATMP-Home-Agent-Password to the value of the Ascend-Home-Agent-Password attribute in the mobile node's RADIUS user profile. All mobile node profiles that access this home agent must specify the *same* password for Ascend-Home-Agent-Password.
6. Set the ATMP-UDP-Port parameter to specify a UDP port number, or accept the default of 5150.
7. Save your changes.

Configuring an outgoing RADIUS user profile to the foreign agent

For the home agent, you must create an outgoing user profile with the foreign agent as its destination. Some steps are required, and some are optional. To set required attributes in the home agent's outgoing RADIUS user profile, proceed as follows:

1. On the first line of the user profile, set the User-Name attribute to the name of the foreign agent, and append **`-Out`** to the user name.
2. Next to the User-Name specification, set Password="Ascend" and User-Service=Dialout-Framed-User.
3. On the second line of the user profile, set the User-Name attribute to the name of the foreign agent, without appending **`-Out`** to the user name.
4. Set the Framed-Protocol attribute to the encapsulation type in use on the line.
5. Set Ascend-Route-IP=Route-IP-Yes to enable IP routing.
6. Set the Ascend-Dial-Number attribute to the phone number the MAX TNT dials to reach the foreign agent.

To set optional attributes in the home agent's outgoing RADIUS user profile, proceed as follows:

1. Set the Framed-Address attribute to the foreign agent's IP address. If a subnet mask is in use, set the Framed-Netmask attribute as well.
2. Set the Framed-Routing attribute to specify RIP behavior.
3. Set the Ascend-Idle-Limit attribute to specify the number of seconds the MAX TNT waits before clearing a call when a session is inactive.
4. Set Ascend-PRI-Number-Type to the type of phone number the MAX TNT dials.
5. Set the Ascend-Send-Auth attribute to the authentication protocol 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.
6. If you request PAP or CHAP authentication, you must also specify a password with Ascend-Send-Secret or Ascend-Send-Passwd. (Use Ascend-Send-Passwd only if your version of the MAX TNT does not support Ascend-Send-Secret.)

Example of outgoing RADIUS user profile to the foreign agent

The following user profile enables a MAX TNT to call the device at 1-800-555-1111:

```
Boston-Out Password="ascend", User-Service=Dialout-Framed-User
     User-Name="Boston",
     Framed-Protocol=PPP,
     Ascend-Route-IP=Route-IP-Yes,
     Framed-Address=10.0.100.1,
     Framed-Netmask=255.255.255.0,
     Framed-Routing=None,
     Ascend-Idle-Limit=30,
     Ascend-Dial-Number=1-800-555-1111,
     Ascend-PRI-Number-Type=National-Number,
     Ascend-Send-Auth=Send-Auth-PAP,
     Ascend-Send-Secret="Password1"
```

Configuring a nailed-up connection to the home network

The home agent must have a nailed-up connection to the home network, because it will not dial the WAN connection on the basis of packets it receives through the tunnel. To configure a nailed-up connection to the home network, set Connection profile parameters at the MAX TNT configuration interface as follows:

1. Set the Station parameter to the name of the home agent. The value you enter must match the name specified by the Ascend-Home-Network-Name attribute in the mobile node's RADIUS user profile.
2. Open the Session-Options subprofile.
3. For a gateway connection, set ATMP-Gateway=Yes. For a router connection, set ATMP-Gateway=No.
4. Set Max-ATMP-Tunnels to the maximum number of ATMP tunnels supported for this home-network connection.
5. For an IP connection, set IP-routing parameters as described in the *MAX TNT Network Configuration Guide*.
6. For an IPX connection, set IPX-routing parameters, as described in the *MAX TNT Network Configuration Guide*. Make sure that IPX routing is enabled on at least one local interface.

Tunneling ATMP between two IP networks

Typically, the mobile node at the remote end of an ATMP tunnel is a dial-in user. If the home network is an IP network, ATMP can also enable LAN-to-LAN connectivity through the tunnel. An IP router can connect as a mobile node. This functionality does not apply to IPX home networks.

When configuring ATMP for LAN-to-LAN connectivity, you follow the same steps as when you configure ATMP for a dial-in user, keeping in mind the additional instructions in this section. For detailed information about configuring an ATMP tunnel, see "Setting up an ATMP tunnel for an IP or IPX network" on page 8-6.

The MAX TNT handles routes to and from the mobile node's LAN in different ways, depending on whether the home agent is in router mode or gateway mode.

Home agent in router mode

If the home agent connects directly to the home network, you must set setting Proxy-Mode=Always in the IP-Global profile so that the home agent can respond to ARP requests for the mobile node,

If the home agent does not connect directly to the home network, the situation is the same as for any remote network. You must enable the router to learn about routes through dynamic updates, or you must configure static routes. The mobile node always requires static routes to the home agent as well as to other networks it reaches through the home agent. (It cannot learn routes from the home agent.)

Home agent in gateway mode

If the home agent forwards packets from the mobile node across a nailed-up WAN link to the home IP network, the answering unit on the home network must have a static route to the mobile node's LAN. In addition, because the mobile node and the home agent do not exchange routing information, the mobile node's LAN can only support local subnets that fall within the network specified in the RADIUS entry.

For example, a mobile-node router at the address 10.168.6.21/28 could support two subnets with a subnet mask of 255.255.255.248. One subnet is at the 10.168.6.16 address, and the other at the 10.168.6.24 address. The answering unit on the home network would have only one route to the router itself (10.168.6.21/28).

Setting up the MAX TNT as a multimode agent

You can configure the MAX TNT to act as a home agent or a foreign agent on a tunnel-by-tunnel basis. Figure 8-3. illustrates a typical network topology.

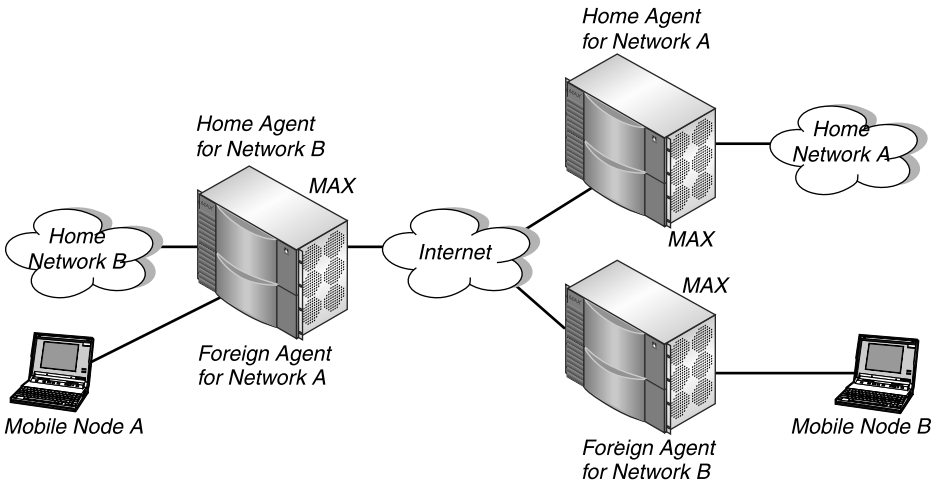


Figure 8-3. The MAX TNT acting as a home agent and a foreign agent

To configure the MAX TNT to act as a foreign agent and home agent on a tunnel-by-tunnel basis, you set up RADIUS as described in "Setting up an ATMP tunnel for an IP or IPX network" on page 8-6. When setting up the IP-Interface profile, however, you must perform the following tasks at the MAX TNT configuration interface:

1. Open IP-Interface profile.
2. Open the ATMP subprofile.
3. Set ATMP-Agent-Mode=ATMP-Home-and-Foreign-Agent to specify that the MAX TNT will function as both a home agent and foreign agent on a tunnel-by-tunnel basis.
4. Set the ATMP-Agent-Type parameter to ATMP-Home-Agent-Router or ATMP-Home-Agent-Gateway, as appropriate.
5. Set the ATMP-Home-Agent-Password parameter to the password the mobile node must specify when the unit acts as its home agent.
6. Set ATMP-SAP-Reply to Yes or No. This parameter applies only when the unit is acting as a home agent. It enables or disables a home agent's ability to reply to the mobile node's IPX Nearest Server Query.
7. Set the ATMP-UDP-Port parameter to specify the UDP port, or accept the default of 5150.
8. Save your changes.

Setting up ATMP to bypass a foreign agent

If a home agent MAX TNT has the appropriate RADIUS entry for a mobile node, the mobile node can connect directly to the home agent, bypassing the foreign agent entirely.

An ATMP-based RADIUS entry local to the home agent enables the mobile node to bypass a foreign agent connection, but it does not preclude a foreign agent. If both the home agent and the foreign agent have local RADIUS entries for the mobile node, the node can choose between a direct connection or a tunneled connection through the foreign agent.

The following RADIUS user profile authenticates a mobile NetWare client that connects directly to a home agent in gateway mode:

```
Mobile-IPX Password="unit"
        User-Service=Framed-User,
        Ascend-Route-IPX=Route-IPX-Yes,
        Framed-Protocol=PPP,
        Ascend-IPX-Peer-Mode=IPX-Peer-Dialin,
        Framed-IPX-Network=40000000,
        Ascend-IPX-Node-Addr=12345678,
        Ascend-Primary-Home-Agent=200.168.6.18,
        Ascend-Home-Network-Name="Dave's MAX TNT",
        Ascend-Home-Agent-Password="Pipeline"
```

If the home agent were in router mode, you would not include the Ascend-Home-Network-Name line in the user entry. The Ascend-Home-Network-Name attribute specifies the name of the answering unit across the WAN on the home IPX network.

Setting Up IP Routing for WAN Links

9

This chapter describes how to configure a RADIUS user profile for IP routing connections, and how to set up static IP routes. The chapter is divided into the following sections:

Before you begin

This section describes the tasks you must perform at the configuration interface and in RADIUS before you begin this chapter.

Preliminary MAX TNT tasks

Before you set up IP routing in RADIUS, you must set up the MAX TNT as a router.

In addition, you must set MAX TNT parameters if you plan to use RADIUS for any of the following tasks:

- Requiring a user to accept an IP address from the MAX TNT
- Configuring pool summaries
- Setting up multicast forwarding
- Setting up DHCP connections

The sections that follow briefly describe the preliminary tasks. For detailed information, see the *MAX TNT Network Configuration Guide*.

Requiring a user to accept an IP address from the MAX TNT

Before you require a RADIUS user to accept an IP address from the MAX TNT, you must perform the following tasks at the MAX TNT configuration interface:

1. Set Assign-Address=Yes in the IP-Answer subprofile of the Answer-Defaults profile. This parameter directs the MAX TNT to try to assign an IP address to a calling device.
2. Set Must-Accept-Address-Assign=Yes in the IP-Global profile. This setting requires the calling station to accept an IP address. If the calling station rejects the assignment, the MAX TNT ends the call.

   If you set Must-Accept-Address-Assign=No, the MAX TNT accepts the IP address the caller specifies.

Turning on the pool-summary feature

Before setting up the pool-summary feature in RADIUS, set Pool-Summary=Yes in the IP-Global profile.

Setting multicast forwarding parameters

If you plan to configure a RADIUS user profile for multicast forwarding, you must set multicast parameters in the IP-Interface and IP-Global profiles at the MAX TNT configuration interface.

Configuring authentication for DHCP connections

If you use RADIUS to authenticate users, and you do not authenticate users that request DHCP, set Use-Answer-For-All-Defaults=Yes in the Answer-Defaults profile. If you set Use-Answer-For-All-Defaults=No, the MAX TNT cannot act as a DHCP server for these clients.

Preliminary RADIUS tasks

Before you set IP attributes, you must configure a RADIUS user profile containing:

- User-Name, Password, and other authentication attributes
- WAN connection attributes

Table 9-1 lists references for more information.

Table 9-1. Preliminary RADIUS tasks for IP routing

Task	Reference
Setting User-Name, Password, and other authentication attributes	Chapter 4, “Setting Up RADIUS Authentication.”
Configuring a PPP, MP, or MP+ connection	Chapter 5, “Setting Up PPP, MP, and MP+ Connections.”
Setting up a terminal-server connection	Chapter 6, “Setting Up Terminal-Server Connections.”
Setting up a Frame Relay connection	Chapter 7, “Setting Up Frame Relay Connections.”

Introducing IP routing

The MAX TNT supports IP routing over PPP, MP, MP+, raw TCP, and Frame Relay connections. You can configure IP routing along with IPX routing and protocol-independent bridging. However, you cannot bridge and route TCP/IP packets across the same connection. When you configure the MAX TNT as an IP router, it routes IP packets at the network layer, and does not bridge them at the link layer. The MAX TNT bridges all other protocols, unless you turn off bridging.

All Ascend products implement system-based routing, in which the entire unit has a single IP address. For systems that have a single backbone connection, system-based routing is the simplest way to configure the MAX TNT. With an alternative method called interface-based routing, each physical or logical interface on the unit has its own IP address. Unless otherwise specified, all sections in this chapter describe how to set up system-based IP routing. For information about setting up interface-based IP routing, see “Setting up an interface-based IP routing connection” on page 9-23.

Types of IP routes

The sections that follow describe the kinds of routes the MAX TNT uses.

Static routes

A static route is a path, from one network to another, that specifies:

- The destination network
- The gateway (next-hop router) to get to that network

Each IP routing Connection profile, IP-Interface profile, and RADIUS user profile that specifies an explicit IP address defines a static route to the remote or local IP network.

Multipath routes

A multipath route is a static route that distributes the traffic load to a single destination across multiple interfaces.

Dynamic routes

A dynamic route is a path to another network that is “learned” dynamically rather than configured in a profile. Routers that use RIP broadcast their entire routing table every 30 seconds, updating other routers about which routes are usable. Hosts that run ICMP can also send ICMP Redirects to offer a better path to a destination network. OSPF routers propagate link-state changes as they occur.

How the MAX TNT builds the routing table

When you power on or reset the MAX TNT, it creates a routing table containing all the routes it knows about, including the following:

- Static routes from MAX TNT IP-Interface and IP-Route profiles
- Static routes from RADIUS pseudo-user profiles
- Static routes from MAX TNT Connection profiles
- Dynamic routes from Routing Information Protocol (RIP) updates
- Dynamic routes from Open Shortest Path First (OSPF) updates

The MAX TNT cannot read some static routes at power up. These routes do not become part of the routing table until they are up and usable. They include the following:

- Routes you configure in incoming RADIUS user profiles. (Every RADIUS user profile that specifies an explicit IP address is a static route.)
- Host routes to addresses that the MAX TNT adds dynamically from an IP address pool.
- Routes you add using the Iproute Add terminal-server command.
- Routes that SNMP MIB II places in the table.

How the MAX TNT routes IP packets

The MAX TNT routes IP packets between its Ethernet interfaces and across any WAN interface configured for IP routing. It consults its internal routing table to determine where to forward each IP packet it processes. First, the MAX TNT tries to find a match between the packet's destination address and a routing table Destination field. If it finds a match, it brings up the required connection (if necessary) to reach the next-hop router specified for that route, and forwards the packet.

If it does not find a match for the packet's destination address, it looks for a default route (destination address 0.0.0.0). If it finds a default route, it brings up the required connection (if necessary) and forwards the packet. If the routing table has no default route and no route that matches a packet's destination address, the MAX TNT drops the packet.

Overview of IP-routing configuration tasks

For all IP routing connections, you must:

- Make sure that IP routing is enabled.
- Specify the IP address of the caller (and, if a subnet is in use, the subnet mask).

All other tasks are optional, and depend upon the needs of your site. You can carry out one or more of the following:

- Specify RIP behavior. (For information, see "Specifying whether RIP sends and receives updates" on page 9-8.)
- Specify the caller's IP address for authentication. (For information, see "Requiring that a caller accept an IP address" on page 9-9.)
- Require that a caller accept an IP address. (For information, see "Requiring that a caller accept an IP address" on page 9-9.)
- Define an IP address pool. (For information, see "Defining a pool of addresses for dynamic assignment" on page 9-9.)
- Configure IP redirection. (For information, see "Setting up IP redirection" on page 9-15.)
- Specify a default route in a user profile. (For information, see "Setting up default routes on a per-user basis" on page 9-16.)
- Configure static IP routes. (For information, see "Setting up static IP routes" on page 9-17.)
- Summarize host routes in an IP address pool. (For information, see "Summarizing host routes in an IP address pool" on page 9-21.)
- Configure an interface-based IP routing connection. (For information, see "Setting up an interface-based IP routing connection" on page 9-23.)
- Configure IP multicast forwarding. (For information, see "Setting up IP multicast forwarding" on page 9-25.)
- Configure a DHCP connection. (For information, see "Setting up a DHCP connection" on page 9-27.)
- Configure Network Address Translation (NAT) for LAN. (For information, see "Setting up Network Address Translation (NAT) for LAN" on page 9-29.)

Enabling IP routing

By default, IP routing is enabled for all user profiles. If you have disabled IP routing, you can re-enable it by setting Ascend-Route-IP=Route-IP-Yes in a user profile.

Specifying a caller's IP address

RADIUS authenticates an incoming call by matching its IP address to one you specify in the RADIUS user profile. To specify the caller's IP address, set the Framed-Address attribute (and, optionally, the Framed-Netmask attribute). The sections that follow describe how to set this attribute depending upon whether the remote device is a dial-in PPP host or an IP router.

Note: The most common cause of trouble in establishing an IP connection is incorrect configuration of the IP address or subnet-mask specification for the remote host or calling device.

When the remote device is a dial-in PPP host

When a device connecting to the MAX TNT is a host running PPP dial-in software, the MAX TNT adds a host route to its routing table and functions as an IP router between its local and WAN interfaces. A host route is an IP address with a subnet mask of 255.255.255.255. It represents a single host rather than a remote router. A host route connection enables the dial-in host to keep its own IP address when logging into the MAX TNT IP network.

If the dial-in host has its own IP address, specify the address as the value of the Framed-Address attribute, and set the Framed-Netmask attribute to 255.255.255.255. If the remote device is a dial-in host that accept dynamic address assignment, accept the default values of 0.0.0.0 for the Framed-Address and Framed-Netmask attributes.

Example of configuring a host connection with a static IP address

In the following example, the PC is running PPP software and the TCP/IP stack and has an ISDN modem card. If a PC user telecommutes to one IP network and uses an ISP on another IP network, one of those connections can assign an IP address and the other can configure a host route to the PC (Figure 9-1.).

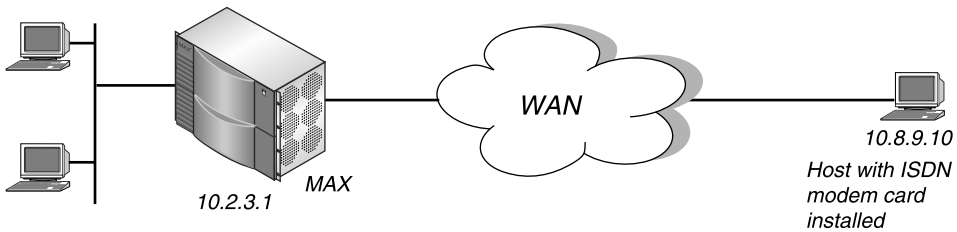


Figure 9-1. Dial-in user requiring a static IP address (a host route)

The PPP software includes settings like the following:

```
Username=Emma
Accept Assigned IP=N/A (or No)
IP address=10.8.9.10
Netmask=255.255.255.255
Default Gateway=N/A (or None)
Name Server=10.7.7.1
Domain suffix=abc.com
VAN Jacobsen compression ON
```

You would set up the RADIUS user profile as follows:

```
Emma Password="m2dan", User-Service=Framed-User
     Framed-Protocol=PPP,
     Ascend-Route-IP=Route-IP-Yes,
     Framed-Address=10.8.9.10,
     Framed-Netmask=255.255.255.255,
     Framed-Routing=None,
     Framed-Compression=Van-Jacobson-TCP-IP,
     Ascend-Idle-Limit=20
```

When the remote device is an IP router

When the device connecting to the MAX TNT is an IP router that belongs to an IP network, the connection results in a route to that remote network or subnet. For this type of configuration, set the Framed-Address attribute to the IP address of the router, and set the Framed-Netmask attribute to its subnet mask. If you omit the subnet mask, the MAX TNT inserts a default subnet mask that assumes that the entire remote network is accessible. In general, if the remote router's address includes a subnet mask, you should include it.

Example of configuring a router connection

In the following example, the MAX TNT is connected to a corporate IP network and needs a switched connection to another company that has its own IP configuration. Figure 9-2. shows the network diagram.

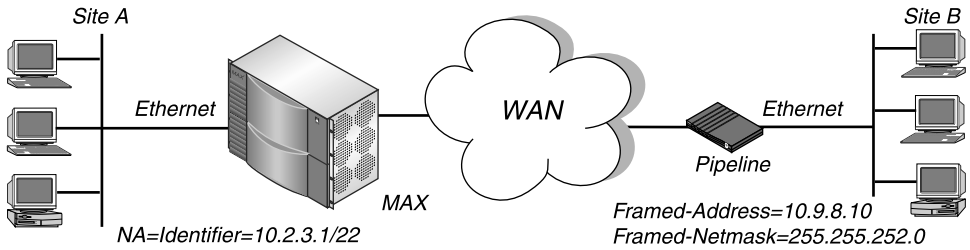


Figure 9-2. A router-to-router IP connection

To configure the site A MAX TNT for a connection to site B, you could set up the RADIUS user profile as follows:

```
PipelineB Password="m2dan", User-Service=Framed-User
          Framed-Protocol=PPP,
          Ascend-Route-IP=Route-IP-Yes,
          Framed-Address=10.8.9.10,
          Framed-Netmask=255.255.252.0,
          Framed-Routing=Broadcast,
          Framed-Compression=Van-Jacobson-TCP-IP,
          Ascend-Idle-Limit=20
```

Specifying whether RIP sends and receives updates

You can specify whether RIP sends routing-table updates, receives updates, or both. If you enable RIP to both send and receive RIP 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 may become quite large).

Setting the Framed-Routing attribute

To specify RIP behavior for the profile, set the Framed-Routing attribute. You can specify one of the values listed in Table 9-2.

Table 9-2. Framed-Routing settings

Setting	MAX TNT behavior
None (0)	Does not send or receive RIP updates. None is the default. Many sites turn off RIP on the WAN interface in order to avoid storing very large local routing tables. If you turn off RIP, the MAX TNT does not listen to RIP updates across the connection. To route to other networks through that connection, the MAX TNT must rely on static routes you specify in a pseudo-user profile. (For details, see “Setting up static IP routes” on page 9-17.)
Broadcast (1)	Sends RIP version 1 updates, but does not receive them.
Listen (2)	Receives RIP version 1 updates, but does not send them.
Broadcast-Listen (3)	Sends and receives RIP version 1 updates.
Broadcast-v2 (4)	Sends RIP version 2 updates, but does not receive them. Ascend recommends that you specify RIP version 2 updates only.
Listen-v2 (5)	Receives RIP version 2 updates, but does not send them. Ascend recommends that you specify RIP version 2 updates only.
Broadcast-Listen-v2 (6)	Sends and receives RIP version 2 updates. Ascend recommends that you specify RIP version 2 updates only.

Special considerations

Because routers send RIP updates every 30 seconds, you should carry out one of the following tasks when configuring WAN connections that use RIP:

- Set the Ascend-Idle-Limit attribute to a value less than 30, as described in “Configuring a time limit and idle connection attributes” on page 5-26.
- Apply a call filter for RIP updates on the WAN by setting the Ascend-Call-Filter attribute, as described in “Configuring an IP filter” on page 12-4.

If you don’t carry out one of these tasks, the connection never disconnects, because RIP traffic resets the idle timer.

Requiring that a caller accept an IP address

You have the option of requiring a caller to accept an IP address from the MAX TNT. The address can be static or dynamic. First, you must set the following parameters at the MAX TNT configuration interface:

- Assign-Address
- Must-Accept-Address-Assign

Then, you must specify a static address or IP address pool in the RADIUS user profile.

- To specify a static IP address, set the Framed-Address and Framed-Netmask attributes.
- To configure an IP address pool and specify the pool an incoming caller should use, follow the instructions in “Defining a pool of addresses for dynamic assignment” on page 9-9.

If the calling end accepts the IP address, the MAX TNT sets the Remote-Address parameter (in a Connection profile) or Framed-Address attribute (in a RADIUS user profile) to the assigned address. If a static address is already specified in a Connection profile or RADIUS user profile, it overrides any IP address from an IP address pool.

Note: In some TCP/IP implementations, when the workstation must receive the IP address from the MAX TNT, you must set the workstation’s address to 0.0.0.0. Setting the address to any other value tells the workstation to use that value and notify the MAX TNT.

Defining a pool of addresses for dynamic assignment

When the device connecting to the MAX TNT is a host running PPP dial-in software, the MAX TNT adds a host route to its routing table. If the host belongs to its own IP network, the MAX TNT must have a Connection profile or RADIUS user profile stating the host’s address and using a 32-bit subnet mask. If the host does *not* belong to an IP network, the MAX TNT can add it to the local IP network by assigning a local address from a designated pool of addresses. You can designate a pool of addresses on the MAX TNT or in RADIUS.

Introducing IP address pools

A pool is a range of contiguous IP addresses on your local network. The MAX TNT chooses an address from a pool and assigns it to an incoming call when Assign-Address=Yes, or when the calling station requests an address assignment. Assigning an address to a device is called

performing dynamic IP. Dynamic IP can apply when the calling end is a station. However, if the calling end is a router, that router usually rejects attempts to perform dynamic IP.

When you set up a pool of addresses, make sure that you do not include addresses that are in use. Although the MAX TNT will inform you of a configuration error if you try to specify a pool whose addresses overlap or conflict with an existing pool, it does not have automatic protection against duplication. If you allocate IP addresses on a separate IP network or subnet, you must make sure that other IP hosts on the local network know about the route to that new network or subnet.

Note: 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.

Overview of address-pool configuration tasks

You set up IP address allocation by configuring one of the following types of pools:

- A pool of addresses pre-assigned to each MAX TNT. For information, see “Configuring IP address pools for a single MAX TNT” on page 9-11.
- A global pool of addresses that several units share. For information, see “Configuring IP address pools shared by several MAX TNT units” on page 9-12.

Overview of attributes for IP address pools

Table 9-3 lists the attributes you use for setting up IP address pools.

Table 9-3. IP address pool attributes

Attribute	Specifies	Possible values
Ascend-Assign-IP-Client (144)	IP address of an Ascend unit that can use global IP address pools.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0.
Ascend-Assign-IP-Global-Pool (146)	Global address pool from which RADIUS should assign a user an address.	Text string. The default value is null.
Ascend-Assign-IP-Pool (218)	Address pool used by incoming calls.	Integer between 1 and 50. The default value is 1.
Ascend-Assign-IP-Server (145)	IP address of the host running `radipad`.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0.
Ascend-IP-Pool-Definition (217)	First IP address in an IP address pool, and the number of addresses in the pool.	**"*num first_ipaddr max_entries*"** The default pool number is 1, the default for the first IP address in the pool is 0.0.0.0, and the default number of entries is 0 (zero).

Configuring IP address pools for a single MAX TNT

To define a pool of IP addresses for a single MAX TNT, you must create a pseudo-user profile that contains the IP address pool definitions. To perform this task:

- Create the first line of the pseudo-user profile.
- Define one or more address pools.

Then, in a RADIUS user profile, you must specify the address pool from the which the caller receives an IP address.

Creating the first line of a pseudo-user profile for IP address pools

Create the first line of a RADIUS pseudo-user profile in the following way:

pools-*name* Password="ascend", User-Service=Dialout-Framed-User

where ***name*** is the system name of the MAX TNT (the name specified by the Name parameter in the System profile).

Defining the IP address pools in the pseudo-user profile

To define an address pool, set the Ascend-IP-Pool-Definition attribute. You can specify multiple instances of the attribute. Use the following format:

Ascend-IP-Pool-Definition="*num first_ipaddr max_entries*"

Table 9-4 describes each Ascend-IP-Pool-Definition argument.

Table 9-4. 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 indicate should not accept a subnet mask, because it always becomes a host route. The default value is 0.0.0.0.
max_entries	Maximum number of IP addresses in the pool. The MAX TNT assign addresses sequentially, from ***first_ipaddr*** on, up to the limit of addresses specified by ***max_entries***. The default value is 0 (zero).

Specifying an IP address pool in a RADIUS user profile

In each RADIUS user profile requiring dynamic addressing for dial-in users, set the Ascend-Assign-IP-Pool attribute to specify the address pool from which RADIUS should assign each user an address. If you set Ascend-Assign-IP-Pool=0, RADIUS chooses an address from any pool that has one available.

Do not set the Framed-Address attribute. If you do, the MAX TNT will require the caller to use the static IP address that the attribute specifies.

Example of configuring IP address pools for a single MAX TNT

Figure 9-3. shows a MAX TNT connected to a dial-in host with a modem and PPP software. The remote host requests a dynamic IP address, and the MAX TNT provides one.

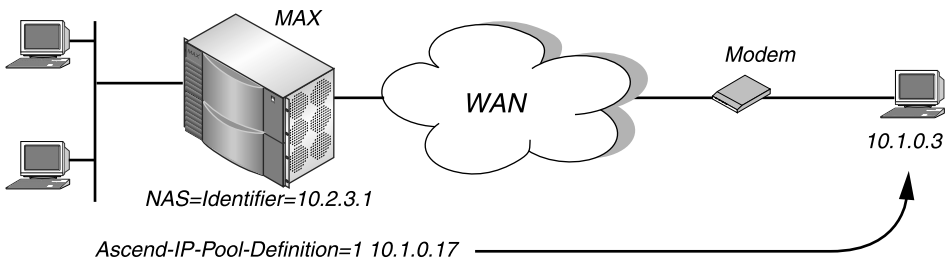


Figure 9-3. An IP routing connection with a dial-in host requiring dynamic IP addressing

The RADIUS pseudo-user profile contains the IP pool definitions. In this example, the profile creates two IP address pools for the MAX TNT to use. Address pool #1 contains a block of 7 IP addresses from 10.1.0.1 to 10.1.0.7. Address pool #2 contains a block of 48 IP addresses from 10.2.0.1 to 10.2.0.48.

```
pools-MAXTNT Password="ascend", User-Service=Dialout-Framed-User
    Ascend-IP-Pool-Definition="1 10.1.0.1 7",
    Ascend-IP-Pool-Definition="2 10.2.0.1 48"
```

In the user profile, you configure the host to request an address from address pool #1:

```
Emma Password="m2dan", User-Service=Framed-User
     Framed-Protocol=PPP,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Metric=2,
     Framed-Routing=None,
     Ascend-Assign-IP-Pool=1
```

Configuring IP address pools shared by several MAX TNT units

To define one or more global IP address pools that several MAX TNT units can share, you must perform the following tasks:

- Install `radipad`.
- Create a pseudo-user profile called radipa-hosts.
- Create a pseudo-user profile containing the global address pool definitions.
- In a RADIUS user profile, specify the global address pool from which the caller receives an IP address.

Installing radipad

For instructions on installing `radipad`, see "Installing radipad for global IP pools" on page 3-5.

Creating the radipa-hosts pseudo-user profile

The radipa-hosts pseudo-user profile contains the IP addresses of Ascend units that can use global IP pools, and specifies the IP address of the host running `radipad`. The RADIUS daemon reads this pseudo-user profile before connecting to the host. To create the radipa-hosts profile:

1. Specify the first line of the profile in the following format:

   ```
   radipa-hosts Password="ascend", User-Service=Dialout-Framed-User
   ```

2. Set the Ascend-Assign-IP-Client attribute to the IP address of an Ascend unit that can use global IP address pools. You can specify multiple instances of this attribute. (At present, the MAX TNT does not use the list of `radipad` client units.)

   If no Ascend-Assign-IP-Client attribute is present, the list of client units defaults to those present in the RADIUS `clients` file.

3. Set the Ascend-Assign-IP-Server attribute to the IP address of the host running `radipad`. Only one instance of this attribute can appear in the profile.

Creating the pseudo-user profile containing global pool definitions

Specify the first line in the following format:

`global-pool-`*`name`* `Password="ascend", User-Service=Dialout-Framed-User`

where ***`name`*** is a designation for any class of users you want to define.

Then, set the Ascend-IP-Pool-Definition attribute to define a global address pool. You can specify multiple instances of this attribute. For information about how to set the Ascend-IP-Pool-Definition attribute, see Table 9-4 on page 9-11.

Specifying a global IP address pool in a RADIUS user profile

In each RADIUS user profile requiring dynamic addressing for dial-in users, set the Ascend-Assign-IP-Global-Pool attribute to specify the global address pool from which RADIUS should assign each user an address. For the attribute's value, indicate the name of the pseudo-user profile containing the global IP pool definitions. The MAX TNT tries to allocate an address from the pools in order, and chooses an address from the pool with the first available IP address.

Do not set the Framed-Address attribute. If you do, the MAX TNT will require the caller to use the static IP address the attribute specifies.

Understanding log messages

At startup, the MAX TNT syslog notes RADIUS requests to release any RADIUS-allocated IP addresses. Some versions of the RADIUS server timeout the request, resulting in one of the following log messages:

```
RADIUS release global-pool address
```

```
RADIUS release all global-pool addresses
```

Example of configuring global IP pools

In the following example, two MAX TNT units are connected to several dial-in clients. The global IP pool configuration consists of:

- A pseudo-user profile containing the IP address of the host running `radipad`.
- A pseudo-user profile containing the global IP pool definitions.
- A user profile specifying the pseudo-user profile from which the MAX TNT assigns the user an IP address.

In the example, `radipad` is running on a host at IP address 10.4.0.1. The radipa-hosts pseudo-user profile is similar to the one that follows:

```
radipa-hosts Password="ascend", User-Service=Dialout-Framed-User
    Ascend-Assign-IP-Server=10.4.0.1
```

This profile creates three global IP address pools for the MAX TNT units to use. Address pool #1 contains a block of 7 IP addresses from 10.1.0.1 to 10.1.0.7. Address pool #2 contains a block of 48 IP addresses from 10.2.0.1 to 10.2.0.48. Address pool #3 contains a block of 49 addresses from 10.3.0.1 to 10.3.0.49. The global pools pseudo-user profile is configured in the following way:

```
global-pool-CA Password="ascend", User-Service=Dialout-Framed-User
    Ascend-IP-Pool-Definition="1 10.1.0.1 7",
    Ascend-IP-Pool-Definition="2 10.2.0.1 48"
    Ascend-IP-Pool-Definition=”3 10.3.0.1 49”
```

In the user profile, the client requests an address from an address pool you defined in the global-pool-CA pseudo-user profile:

```
Emma Password="m2dan", User-Service=Framed-User
     Framed-Protocol=PPP,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Metric=2,
     Framed-Routing=None,
     Ascend-Assign-Global-IP-Pool=Global-Pool-CA
```

Setting up IP redirection

You can configure a RADIUS user profile to automatically redirect incoming IP packets to a host you specify on the local IP network. When you specify IP redirection, the MAX TNT bypasses all internal routing and bridging tables, and simply sends all packets it receives on a connection's WAN interface to the specified IP address. IP redirection does not affect outbound packets.

To set up IP redirection:

1. Specify the User-Name and Password attributes, authentication attributes, and WAN connection attributes.
2. Set the Framed-Address attribute (and, optionally, the Framed-Netmask attribute) to specify the caller's IP address.
3. Set Ascend-Route-IP=Route-IP-Yes.
4. Set Ascend-Bridge=Bridge-No.
5. Set Ascend-IP-Direct to the IP address to which the MAX TNT redirects packets from the user. The default value is 0.0.0.0, which specifies that the MAX TNT does not perform IP redirection.
6. Set Framed-Routing=None.

   Ascend-IP-Direct connections typically turn off RIP. If you configure the connection to receive RIP, the MAX TNT keeps all RIP packets it receives from the remote end and forwards them to the IP address you specify.
7. Make certain that Framed-Protocol is not set to FR.

Note: Do not set Ascend-IP-Direct and Ascend-FR-Direct in the same user profile. If you do, an error occurs.

Example of configuring IP redirection

The following example shows IP redirection for a PPP link. In Figure 9-4., the MAX TNT redirects incoming packets from site B to the host at IP address 10.2.3.11.

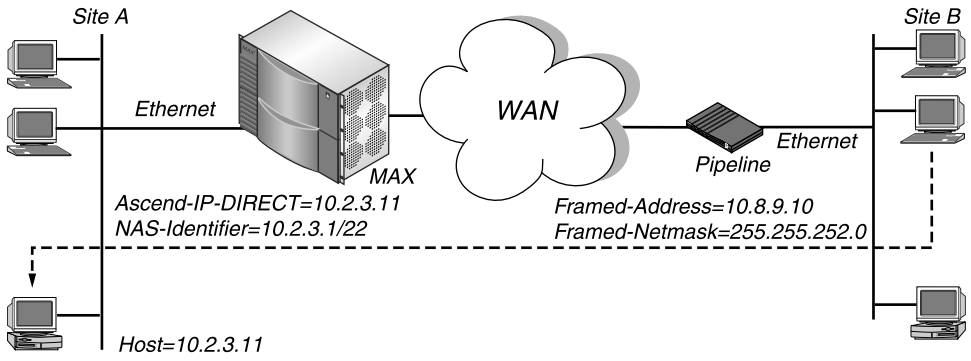


Figure 9-4. Directing incoming IP packets to one local host

The user profile is configured in the following way:

```
Emma Password="m2dan", User-Service=Framed-User
     Framed-Protocol=PPP,
     Framed-Address=10.8.9.10,
     Framed-Netmask=255.255.252.0,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Bridge=Bridge-No,
     Ascend-IP-Direct=10.2.3.11,
     Ascend-Metric=2,
     Framed-Routing=None,
     ...
```

Setting up default routes on a per-user basis

In each RADIUS user profile, you can specify the default route for IP packets coming from the user. The MAX TNT uses the per-user default under the following circumstances:

- If the next-hop address in the MAX TNT unit's routing table is the default route for the system (destination 0.0.0.0).
- If the normal routing logic fails to find a route and there is no system-wide default route.

To specify the default route in a RADIUS user profile, set the Ascend-Client-Gateway attribute to the IP address of the next hop router. Enter the IP address in dotted decimal notation. The Ascend unit must have a direct route to the address you specify. The direct route can take place via a profile or an Ethernet connection. If the Ascend unit does not have a direct route, it drops the packets on the connection.

The default value is 0.0.0.0. If you accept this value, the Ascend unit routes packets as the routing table specifies, using the system-wide default route if it cannot find a more specific route.

The per-user default route applies to all packets the MAX TNT receives for a given profile, regardless of the specific IP source address. Therefore, you can use this feature when the profile belongs to another router, and all hosts behind that router use the default gateway. The MAX TNT handles packets from other users or from the Ethernet network in the usual fashion. The global routing table is not altered. Therefore, when you diagnose routing problems with a profile that implements this feature, an error in a per-user gateway address is not apparent from inspection of the global routing table.

Example of configuring a default route

For example, suppose you specify the following setting in the profile Berkeley:

```
Ascend-Client-Gateway=10.0.0.3
```

IP packets from the user Berkeley, with destinations through the default route, go through the router at 10.0.0.3.

Setting up static IP routes

A static route is a path from one network to another. The path specifies the destination network and the router the data uses to get to that network. For routes that must be reliable, you can configure more than one path. In this case, the MAX TNT uses an assigned metric to choose the route.

A dynamic route can hide a static route to the same network if the dynamic route's metric is lower than that of the static route. However, dynamic routes age. If the MAX TNT does not receive route updates, the dynamic routes eventually expire. In that case, the hidden static route reappears in the routing table.

If the MAX TNT has a RADIUS user profile that defines a static route to a destination for which there is also a route in the MAX TNT unit's IP Route profiles or a RADIUS pseudo-user profile, the metric in the RADIUS user profile overrides the metric in the other profiles, but only when the RADIUS user connects.

For example, suppose a MAX TNT has a static route to network 1.10.1.10, with a metric of 10. A user profile in RADIUS has a metric of 7 in a static route to the same network. When the RADIUS user's route is not in use, the MAX TNT routing table indicates that the route has a metric of 10. When the route is in use, the MAX TNT routing table indicates that the route has a metric of 7, with an `r` in the flags column to indicate that the route came from RADIUS. Furthermore, the route with a metric of 10 remains in the routing table, with an asterisk (*) in the flags column, indicating that it is a hidden route.

Overview of static-route configuration tasks

In RADIUS, you can create a static route in one of the following ways:

- In a pseudo-user profile containing one or more explicit static routes
- In a pseudo-user profile containing multipath static routes
- In a user profile specifying a WAN connection

The sections that follow describe how to set up each type of configuration.

Configuring static IP routes in a pseudo-user profile

When you turn off RIP in a RADIUS user profile (Framed-Routing=None), the MAX TNT does not listen to RIP updates across that connection. To route to other networks through that connection, the MAX TNT must rely on static routes you define in a RADIUS pseudo-user profile.

If you configure the MAX TNT with a subnet address on a backbone network (using the IP-Address parameter in the MAX TNT unit's IP-Interface profile), you must set up a static route to the backbone router on the main network. If you do not, the MAX TNT can only see the subnets to which it is directly connected.

You cannot create static routes for IP addresses the MAX TNT dynamically assigns, because the actual route to those addresses changes with each dynamic assignment.

To set up static IP routes in a RADIUS pseudo-user profile, you must perform the following tasks:

- Create the first line of the pseudo-user profile.
- Set the Framed-Route attribute to specify one or more static IP routes.

Creating the first line of a pseudo-user profile for static IP routes

You can configure pseudo-users for both global and MAX TNT-specific configuration control of IP dialout routes. The MAX TNT adds the unit-specific dialout routes in addition to the global dialout routes.

For a unit-specific IP dialout route, specify the first line of a pseudo-user profile in the following format:

route-*name-num* Password="ascend", User-Service=Dialout-Framed-User

For a global IP dialout route, specify the first line of a pseudo-user profile in the following format:

route-*num* Password="ascend", User-Service=Dialout-Framed-User

The ***name*** argument is the system name of the MAX TNT (the name specified by the Name parameter in the System profile), while the ***num*** argument is a number in a sequential series, starting at 1.

Specifying static IP routes with the Framed-Route attribute

In each pseudo-user profile, specify one or more routes with the Framed-Route attribute. Use the following format:

Framed-Route="*host_ipaddr* [*/subnet_mask*] *router_ipaddr metric* [*private*] [*profile_name*]"

The MAX TNT fetches information from each pseudo-user profile in order to initialize its routing table. Table 9-5 describes each Framed-Route argument.

Table 9-5. Framed-Route arguments

Syntax element	Specifies
host_ipaddr/ subnet_mask	IP address of the destination host or subnet reached by this route. The default value is 0.0.0.0/0. This setting 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 9-5. 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 this 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.

How RADIUS adds static IP routes to the routing table

Whenever you power on or reset the MAX TNT, RADIUS adds IP dialout routes to the routing table as follows:

1. RADIUS looks for profiles having the format route-***name***-1, where ***name*** is the system name.
2. If at least one such profile exists, RADIUS loads all existing profiles with the format route-***name***-***num*** to initialize the IP routing table. The variable ***num*** is a number in a sequential series, starting with 1.
3. The MAX TNT queries route-***name***-1, then route-***name***-2, and so on, until it receives an authentication reject from RADIUS.
4. RADIUS loads the global configuration profiles. These configurations have the format route-***num***.
5. The MAX TNT queries route-1, then route-2, and so on, until it receives an authentication reject from RADIUS.

Example of configuring a static IP route

In Figure 9-5., the remote network for sites B and C does not use RIP, so the MAX TNT cannot learn about it dynamically.

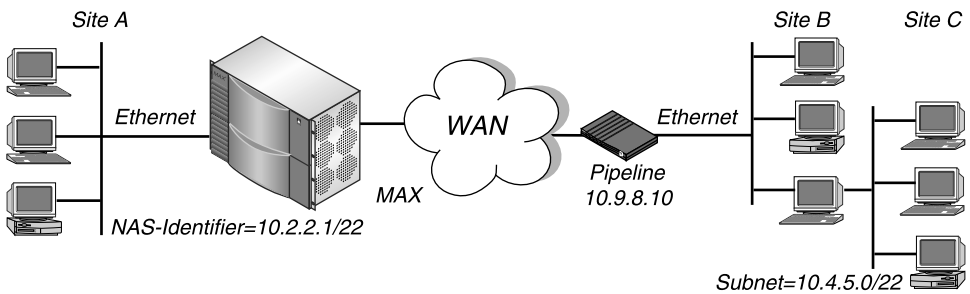


Figure 9-5. A two-hop connection that requires a static route when RIP is off

To enable the MAX TNT to reach site C, you must configure the following type of 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"
```

Configuring multipath static IP routes in a pseudo-user profile

Multipath static routes distribute the traffic to one destination across the aggregated bandwidth of multiple interfaces. A multipath route consists of two or more static routes that have same destination address, subnet mask, and metric, but different gateway addresses.

To create a multipath route, set up two or more routes by following the steps in "Configuring static IP routes in a pseudo-user profile" on page 9-17. Each Framed-Route specification must indicate the same value for ***host_ipaddr***, ***subnet_mask***, and ***metric***, but a different value for ***router_ipaddr***.

Example of configuring a multipath static route

To configure a multipath route to the network 10.4.5.0/22, configure the following type of pseudo-user profile:

```
route-1 Password="ascend", User-Service=Dialout-Framed-User
        Framed-Route="10.4.5.0/22 10.9.8.10 1 n inu-out",
        Framed-Route="10.4.5.0/22 10.9.8.11 1 n inu-out",
        Framed-Route="10.4.5.0/22 10.9.8.12 1 n inu-out"
```

Configuring static IP routes in a dial-in user profile

You can specify a static route in a dial-in profile by setting either the Framed-Address attribute or the Framed-Route attribute.

Every RADIUS user profile containing a Framed-Address setting specifies a static route.

In addition, suppose you wish to update the MAX TNT unit's routing tables each time it connects to a user whose profile specifies User-Service=Framed-User. In this case, you can set the Framed-Route attribute in an incoming user profile to specify the user's IP address and subnet mask with the ***host_ipaddr*** and ***subnet_mask*** arguments, respectively. The route you specify in this manner exists only during the time the call is online. However, when you enter a nonzero router address for the ***router_ipaddr*** argument, and it is different from the caller's address, the static route of a dial-in framed-user persists even after the connection goes offline.

Summarizing host routes in an IP address pool

By default, the MAX TNT adds dynamically assigned IP addresses to the routing table as individual host routes. However, to reduce the size of routing table advertisements, you can summarize the entire pool. When you do so, the router advertises a single route for the network you define in an address pool, rather than an individual host route for each address. The MAX TNT routes packets to a valid host address, and rejects packets with an invalid host address.

To set up the pool-summary feature, you must perform the following tasks:

- Make sure that each IP address pool is network aligned.
- Specify the static route for each summarized address pool.

Making sure that each IP address pool is network aligned

In the pseudo-user profile defining the address pools, set each Ascend-IP-Pool-Definition attribute to network align the IP address pool. (For instructions about setting up address pools, see “Defining a pool of addresses for dynamic assignment” on page 9-9.)

First, make sure that the first address in the pool is the first host address. The ***first_ipaddr*** argument specifies the first IP address in the pool. The value ***first_ipaddr*** – 1 determines the network alignment (the zero address on the subnet).

Second, the maximum number of entries you specify with the ***max_entries*** argument must be two less than the total number of addresses in the pool. The value ***max_entries*** + 2 determines the total number of addresses in the subnet. You can calculate the subnet mask on the basis of this total.

For example, suppose you have the following specification for Ascend-IP-Pool-Definition:

```
Ascend-IP-Pool-Definition="1 10.12.253.1 62"
```

Because ***first_ipaddr***=10.12.253.1, the network alignment address is 10.12.253.0 (***first_ipaddr*** – 1). Moreover, because ***max_entries***=62, you must specify a subnet mask for 64 addresses (***max_entries*** + 2). The subnet mask for 64 addresses is 255.255.255.192 (256–64=192). The Ascend notation for a 255.255.255.192 subnet mask is /26.

The resulting address-pool network is 10.12.253.0/26. This address and subnet mask become the first values you specify for the Framed-Route attribute in“Setting the Framed-Route attribute” on page 9-22.

Configuring the static route for each summarized address pool

In a pseudo-user profile, you must set the Framed-Route attribute to create a static IP route to each summarized network. This section provides guidelines for specifying the router in the static route configuration, and describes how to set each argument of the Framed-Route attribute.

(For basic instructions about setting up the pseudo-user profile containing the static IP routes, see “Setting up static IP routes” on page 9-17.)

Guidelines for specifying the router

Because the MAX TNT creates a host route for every address assigned from the pools, and because host routes override subnet routes, the MAX TNT correctly routes packets whose destination matches an assigned IP address from the pool. However, because the MAX TNT advertises the entire pool as a route, and only knows privately which IP addresses in the pool are active, a remote network might improperly send the MAX TNT a packet with an inactive IP address.

The router address handles all IP addresses not assigned to users. When the MAX TNT receives a packet whose IP address matches an unused IP address in a pool, it either returns the packet to the sender with an ICMP reject message, or simply discards the packet. To enable the router to handle packets with destinations to invalid hosts on the summarized network, you must specify one of the internal interfaces listed in Table 9-6 as the router.

Table 9-6. Internal interfaces for invalid hosts

Interface	Description
The reject interface (rj0)	The reject interface has an IP address of 127.0.0.2. When you specify this address as the router to the destination pool network, the MAX TNT rejects packets to an invalid host on that network, appending an ICMP Host Unreachable message.
The black-hole interface (bh0)	The black-hole interface has an IP address of 127.0.0.3. When you specify this address as the router to the destination pool network, the MAX TNT silently discards packets to an invalid host on that network.

Setting the Framed-Route attribute

The Framed-Route attribute has the following format:

Framed-Route="*host_ipaddr*[*/subnet_mask*] *router_ipaddr metric* [*private*] [*profile_name*]"

For each Framed-Route attribute:

1. Set the ***host_ipaddr*** argument to the address of the summarized network.
2. Set the ***subnet_mask*** argument to the associated subnet mask.
3. Set the ***router_ipaddr*** argument to the router address for each summarized network. For a discussion of how to set this argument, see “Guidelines for specifying the router” on page 9-22.
4. Set the ***metric*** argument to 0.
5. Set the ***private*** argument to **n** for No.
6. Set the ***profile_name*** argument to the name of the outgoing profile that uses the route.

For example, if you want to set up a static IP route with a reject interface for address pool network 10.12.253.0/26, enter the following setting:

```
Framed-Route="10.12.253.0/26 127.0.0.2 0 n Summary"
```

Setting up an interface-based IP routing connection

In some situations, it is useful to number some of the MAX TNT unit's interfaces—to have the MAX TNT operate partially as a system-based router and partially as an interface-based router. Reasons for using numbered interfaces include troubleshooting nailed-up point-to-point connections and forcing routing decisions between two links going to the same final destination. More generally, interface-based routing allows the MAX TNT to operate more as a multi-homed Internet host behaves.

You can configure each link in RADIUS as numbered (interface-based) or unnumbered (system-based). If no interfaces are numbered, the MAX TNT operates as a purely system-based router. The sections that follow describe special considerations for using interface-based routing, and provide an overview of RADIUS attributes. The remaining sections show you how to carry out one of the following tasks, depending on your setup:

- Add interface-based routing to a system-based configuration.
- Refer to the remote device by its interface address.
- Refer to the remote device by its system address.

Before you carry out interface-based routing tasks, be sure to set up the WAN connection, specifying system-based IP routing attributes. For information about configuring system-based IP routing, see the preceding sections of the chapter.

Special considerations

If a MAX TNT is using a numbered interface, you should be aware of the following features:

- IP packets that the MAX TNT generates and sends to the remote address have an IP source address corresponding to the numbered interface, not to the default (Ethernet) address of the MAX TNT.
- During authentication of a call the MAX TNT places through a numbered interface, the MAX TNT reports the address of the interface as its IP address.
- The MAX TNT adds all numbered interfaces in Connection profiles and RADIUS user profiles to its routing table.
- The MAX TNT accepts IP packets whose destination is a numbered interface in a Connection profile or a RADIUS user profile, considering the packets' destinations to be the MAX TNT itself. The packet might actually arrive over any interface, and the numbered interface corresponding to the packet's destination address need not be in the active state.

Overview of interface-based routing attributes

Table 9-7 lists the RADIUS attributes you set for interface-based routing.

Table 9-7. RADIUS attributes for interface-based routing

Attribute	Specifies	Possible values
Ascend-IF-Netmask (154)	Subnet mask in use for the local numbered interface to the WAN.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0.
Ascend-IF-Addr	IP address of the local numbered interface to the WAN.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0.
Ascend-Remote-Addr (155)	IP address of the remote numbered interface to the WAN.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The default value is 0.0.0.0.

Adding interface-based routing to a system-based configuration

If you are adding interface-based routing, and the MAX TNT already uses system-based routing, proceed as follows:

1 Set the Ascend-IF-Addr to the IP address of the local WAN interface.

2 Set the Ascend-IF-Netmask attribute to the subnet mask in use for the local interface.

3 Set the Ascend-Remote-Addr attribute to specify the remote WAN interface address.

Note: If you want to create static routes to hosts at the remote end, you can use the Ascend-Remote-Addr or Framed-Address value as the next hop (gateway) field.

When you make these specifications, the following events take place:

- The MAX TNT generates host routes to both Framed-Address and Ascend-Remote-Addr. The Ascend-Remote-Addr appears in the routing table as the next hop to Framed-Address.
- The MAX TNT generates a route to the remote system's subnet, showing the Ascend-Remote-Addr value as the next hop.
- An incoming PPP, MP, or MP+ call must report its IP address as the Ascend-Remote-Addr attribute (rather than the Framed-Address attribute). That is, the caller must be using a numbered interface, and its interface address must agree with the Ascend-Remote-Addr value on the receiving side.

Referring to the remote device by its interface address

You can omit the remote side's system address from the profile and use interface-based routing exclusively. If the remote system is on a backbone network that the remote administrator periodically reconfigures, you might want to refer to the remote system only by its interface address. Proceed as follows:

1. Set the Ascend-IF-Addr attribute to the IP address of the local interface.
2. Set the Ascend-IF-Netmask attribute to the subnet mask in use for the local interface.
3. For the Ascend-Remote-Addr attribute, accept the default address of 0.0.0.0. (Note that the Framed-Address attribute must always have a value, so if the only known address is the interface address, specify it using the Framed-Address attribute rather than the Ascend-Remote-Addr attribute.)

If the Framed-Address attribute specifies the remote system address, the following events take place:

- The MAX TNT creates a host route to Framed-Address.
- The MAX TNT creates a route to the subnet of the remote interface.
- An incoming PPP, MP, or MP+ call must report its IP address as Framed-Address.

Referring to the remote device by its system address

If interface-based routing is in use and the local interface is numbered, the remote address will usually be known. In practice, administrators at both sites must agree upon the subnet. It is possible, but not recommended, to number the local interface, omitting the interface address of the remote site and using only its system address. In this case, do not use the remote interface address in any static routes.

When a local interface is numbered but no corresponding remote interface address exists, the remote interface must have an address on the same subnet as the local, numbered interface. RADIUS rejects incoming PPP calls if the user profile numbers the local interface and the remote caller supplies an address not on the same subnet.

Setting up IP multicast forwarding

The MAX TNT implements Internet Group Membership Protocol (IGMP) version-1 and version-2, along with configuration options that enable the MAX TNT to communicate with multicast backbone (MBONE) routers and to forward multicast traffic.

What is the MBONE?

The MBONE is a virtual network layered on top of the Internet to support IP multicast routing across point-to-point links. It is used for transmitting audio and video on the Internet in real-time, because multicasting is a much cheaper and faster way to communicate the same information to multiple hosts.

What is a multicast network?

A multicast network is a network in which a router sends packets to all addresses on a subscriber list. This type of network is different from both a unicast network (in which the router sends packets to one user at a time) and a broadcast network (in which the router sends packets to all users, whether they appear on subscription lists or not). The MBONE is a virtual network that actually consists of groups of networks called *islands*. These islands are connected by tunnels and support IP.

How does the MAX TNT interact with the MBONE?

Figure 9-6. shows a MAX TNT acting as an MBONE client. The MAX TNT accesses an MBONE network and starts receiving the MBONE multicasts. It resends the multicast packets to all of its own clients connected to it for MBONE service. The clients wanting MBONE service must implement IGMP.

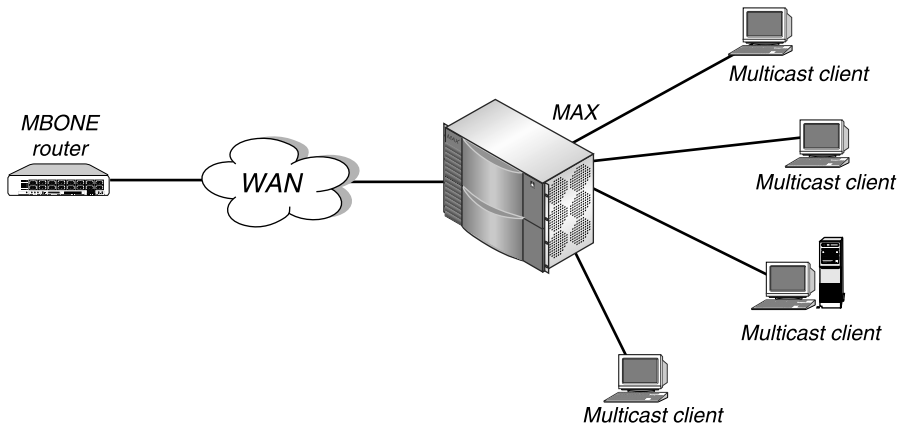


Figure 9-6. The MAX TNT interacting with an MBONE router and multicast clients

To the MBONE, the MAX TNT looks like a multicast client. It responds as a client to IGMP packets it receives from an MBONE router. The MBONE router can reside on the MAX TNT unit's Ethernet interface or across a WAN link. If the router resides across a WAN link, the MAX TNT can respond to multicast clients on its Ethernet interface as well as across the WAN.

To multicast clients on a WAN or Ethernet interface, the MAX TNT looks like a multicast router, although it simply forwards multicast packets on the basis of group memberships. In this implementation, multicast clients cannot source multicast packets—if they do, the MAX TNT discards the packets.

(For complete information about multicast forwarding, see the *MAX TNT Network Configuration Guide*.)

Configuring multicast forwarding attributes

To configure multicast forwarding in RADIUS, use the attributes listed in Table 9-8.

Table 9-8. Multicast forwarding attributes

Attribute	Description	Possible values
Ascend-Multicast-Client (152)	Specifies whether the user is a multicast client of the MAX TNT.	Multicast-No (0) Multicast-Yes (1) Multicast-No is the default.
Ascend-Multicast-Rate-Limit (153)	Specifies how many seconds the MAX TNT waits before accepting another packet from the multicast client. This parameter prevents multicast clients from creating response storms to multicast transmissions.	Any integer between 0 and 65,535. If you specify 0 (zero), the MAX TNT does not apply rate limiting.The default value is 100.

To configure multicast forwarding:

1. Set up the user profile, specifying the appropriate user name, password, encapsulation method, and IP routing parameters.
2. Set Ascend-Multicast-Client=Multicast-Yes to specify that the user is a multicast client of the MAX TNT.
3. Set Ascend-Multicast-Rate-Limit to specify how many seconds the MAX TNT waits before accepting another packet from the multicast client.

Setting up a DHCP connection

When you set up a Dynamic Host Configuration Protocol (DHCP) connection in a RADIUS user profile, the MAX TNT can assign a dynamic IP address to a remote DHCP client over a bridged connection. The MAX TNT becomes a DHCP server.

For example, suppose a group of DHCP clients resides on a LAN connected to a Pipeline, and the Pipeline connects to the MAX TNT over a bridged PPP connection (Figure 9-7.). The MAX TNT can assign dynamic IP addresses to any of the DHCP clients on the remote LAN.

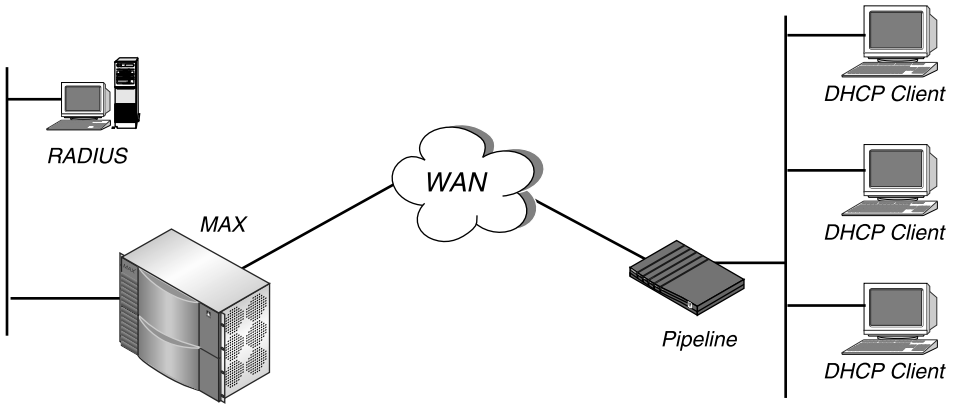


Figure 9-7. Pipeline connected to DHCP clients

The RADIUS server holds the configuration information the MAX TNT uses to identify and authenticate each DHCP client.

When the DHCP client requests an address, the MAX TNT allocates an IP address from one of its IP address pools and assigns it to the client for 30 minutes. The client must renew the IP address assignment before the 30-minute period expires. The MAX TNT uses its local memory to keep track of all IP addresses it has assigned. Therefore, it loses the entries for current, unexpired IP address assignments when you reset it.

A client can hold an unexpired IP address assignment when you reset the MAX TNT. After the reset, the MAX TNT might assign that address to a new client. The duplicate IP addresses cause network problems until the first assignment expires or one of the two clients reboots.

Overview of DHCP attributes

Table 9-9 lists the attributes you set for a DHCP connection.

Table 9-9. DHCP attributes

Attribute	Description	Possible values
Ascend-DHCP-Pool-Number (148)	Specifies the address pool used by incoming calls.	Integer between 1 and the number of defined IP address pools. The default value is 0 (zero), which represents the first defined IP address pool.
Ascend-DHCP-Reply (147)	Specifies whether the MAX TNT processes DHCP packets and acts as a DHCP server on this connection.	DHCP-Reply-No (0) DHCP-Reply-Yes (1) DHCP-Reply-No is the default.

Configuring DHCP attributes

To set up a DHCP connection:

1. Set up one or more IP address pools in a RADIUS pseudo-user profile. (For instructions, see “Defining a pool of addresses for dynamic assignment” on page 9-9.)
2. Configure a bridging connection in a RADIUS user profile. (For instructions, see “Setting Up Bridging for WAN Links” on page 11-1.)
3. In the RADIUS user profile, set Ascend-DHCP-Reply=DHCP-Reply-Yes to enable DHCP functionality.
4. In the RADIUS user profile, set the Ascend-DHCP-Pool-Number attribute to the number of the IP address pool the MAX TNT uses when allocating a dynamic IP address to this connection.

Setting up Network Address Translation (NAT) for LAN

Access to public networks requires the use of an official IP address that is unique across the entire network. Typically, a central authority assigns a range of addresses, and a local administrator distributes them. If access to a public network is not necessary, the local manager can assign addresses as he or she sees fit, even if the addresses are unofficial or belong to another company.

Because the supply of addresses is rapidly diminishing, a company might not be able to get official addresses for its entire network. A site might already have unofficial addresses, but now needs access to the Internet, where an official address is required. For these reasons, you might need a facility for borrowing an official address and dynamically translating between the local and official addresses.

NAT for LAN allows a Pipeline to connect a LAN to another network even if the devices on the LAN have addresses that are not valid for the remote network. The Pipeline translates between the local network addresses and the remote network addresses.

How NAT for LAN works

When you enable NAT for LAN, the Pipeline attempts to perform IP address translation on all packets it receives. The Pipeline has no notion of what are not official addresses on the LAN. The Pipeline acts as a DHCP client on behalf of all hosts on the LAN and relies on the MAX TNT unit (acting as the DHCP server) to provide addresses suitable for the remote network from its IP address pool. On the local network, the Pipeline and the hosts all have local addresses on the same network, and use them only for local communication between the hosts and the Pipeline over the Ethernet.

Figure 9-8. illustrates a basic NAT for LAN setup.

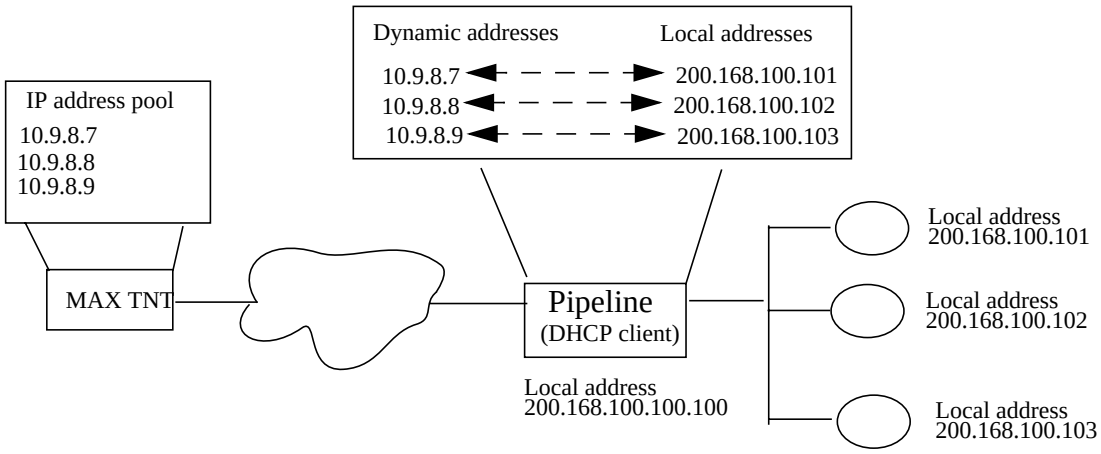


Figure 9-8. NAT for LAN setup

In Figure 9-8., the Pipeline itself does not have an address on the remote network. Therefore, clients can gain access to the Pipeline only from the local network, not from the WAN. When the first client on the LAN requests access to the remote network, the Pipeline gets an address for the client from the MAX TNT. When subsequent clients request access to the remote network, the Pipeline sends the MAX TNT a DHCP request packet, asking for an address. In return, the MAX TNT sends an address from its IP address pool. The Pipeline uses the dynamic addresses it receives from the MAX TNT to translate IP addresses on behalf of local clients.

As it receives packets on the LAN, the Pipeline determines whether the source IP address has a corresponding translated address. If so, the Pipeline translates the packet, and forwards it out the WAN. If the Pipeline has not assigned a translated address (and one is not pending), the Pipeline issues a new DHCP request for this IP address. While waiting for the MAX TNT to offer an IP address, the Pipeline drops corresponding source packets. For packets it receives from the WAN, the Pipeline checks the destination address against its table of translated addresses. If the destination address exists and is active, the Pipeline forwards the packet. If the destination address does not exit, or is not active, the Pipeline drops the packet.

Special considerations

The MAX TNT typically offers IP addresses for a limited duration, but the Pipeline automatically renews the lease on the addresses. If the connection to the remote server goes down, all leased addresses are considered revoked. Therefore, TCP connections do not persist across calls.

For a bridged connection, the MAX TNT responds to all DHCP requests. For a non-bridged connection, the MAX TNT responds only to NAT for LAN DHCP packets. Therefore, if you want your site to handle both NAT for LAN DHCP requests and ordinary DHCP requests, and the ordinary DHCP clients are using a non-bridged connection to the MAX TNT, you must have a separate DHCP server to handle their requests.

Configuring the Pipeline for NAT for LAN

For information about configuring NAT for LAN on the Pipeline, consult the Pipeline documentation.

Configuring the MAX TNT for NAT for LAN

To configure the MAX TNT for NAT for LAN, you can specify settings in the Answer-Defaults profile, a Connection profile, or a RADIUS user profile. This section describes how to set up a RADIUS user profile. For information about setting up the Answer-Defaults profile or a Connection profile, see the *MAX TNT Network Configuration Guide*.

To configure NAT for LAN in RADIUS, you use the attributes listed in Table 9-10.

Table 9-10. NAT for LAN attributes

Attribute	Description	Possible values
Ascend-DHCP-Pool-Number (148)	Specifies the address pool to use for allocating an IP address to a NAT for LAN client on this connection.	Integer between 1 and the number of defined IP address pools. The default value is 0 (zero), which represents the first defined IP address pool.
Ascend-DHCP-Reply (147)	Specifies whether the MAX TNT processes DHCP packets and acts as a DHCP server on this connection.	DHCP-Reply-No (0) DHCP-Reply-Yes (1) DHCP-Reply-No is the default.
Ascend-DHCP-Maximum-Leases (134)	Specifies the maximum number of dynamic addresses to assign to NAT for LAN clients using this connection	Integer between 1 and 254. The default value is 4.

To set up NAT for LAN for a MAX TNT in a RADIUS user profile:

1. Set up one or more IP address pools in a RADIUS pseudo-user profile. (For information, see “Defining a pool of addresses for dynamic assignment” on page 9-9.)
2. Set up routing or bridging in RADIUS. (For information about setting up routing, see the previous sections of the present chapter. For information about setting up bridging, see Chapter 11, “Setting Up Bridging for WAN Links.”)
3. Set Ascend-DHCP-Reply=DHCP-Reply-Yes.
4. Set the Ascend-DHCP-Pool-Number attribute to the number of the IP address pool the MAX TNT uses when allocating a dynamic IP address to the NAT for LAN client.
5. Set the Ascend-DHCP-Maximum-Leases attribute to specify the maximum number of addresses that the MAX TNT can give to the Pipeline.

Setting Up IPX Routing for WAN Links

10

This chapter describes how to configure a RADIUS user profile for IPX routing connections, and how to set up static IPX routes. The chapter is divided into the following sections:

Before you begin

This section describes the tasks you must perform at the configuration MAX TNT interface and in RADIUS before you begin this chapter.

Preliminary MAX TNT tasks

This section describes the tasks you carry out at the MAX TNT configuration interface. The first one is required for all configurations. The others depend upon the type of configuration you plan to set up.

Setting up the MAX TNT as an IPX router

Before you set up an IPX routing connection in RADIUS, you must set up the MAX TNT as an IPX router. For detailed information, see the *MAX TNT Network Configuration Guide*.

Specifying an authentication protocol

If you set up a RADIUS user profile that enables IPX routing (but not IP routing), you must specify an authentication protocol for name and password authentication of PPP, MP, and MP+ calls. In the Answer-Defaults profile's PPP-Answer subprofile, set the Receive-Auth-Mode parameter to PAP-PPP-Auth, CHAP-PPP-Auth, MS-CHAP-PPP-Auth, or Any-PPP-Auth. (For descriptions of these settings, see Table 4-5 on page 4-15.)

Unlike an IP routing configuration, in which the MAX TNT uniquely identifies the calling device by its IP address, an IPX routing configuration does not include a built-in way to uniquely identify callers. For this reason, you must use PAP, CHAP, or MS-CHAP password authentication, unless you configure IP routing in the same RADIUS user profile.

Specifying a network number for dial-in clients

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. To provide an IPX network number, you must define a virtual IPX network by means of the IPX Pool# parameter. The MAX TNT advertises the route to this virtual network and assigns it as the network address for dial-in clients. If the client does not supply its own unique node number, the MAX TNT assigns a unique node number as well.

Preliminary RADIUS tasks

Before you set IPX attributes, you must configure a RADIUS user profile containing:

- User-Name, Password, and other authentication attributes
- WAN connection attributes

Table 10-1 lists references for more information.

Table 10-1. Preliminary RADIUS tasks for IPX routing

Task	Reference
Setting User-Name, Password, and other authentication attributes	Chapter 4, “Setting Up RADIUS Authentication.”
Configuring a PPP, MP, or MP+ connection	Chapter 5, “Setting Up PPP, MP, and MP+ Connections.”
Setting up a Frame Relay connection	Chapter 7, “Setting Up Frame Relay Connections.”

Introducing IPX routing

The MAX TNT supports IPX routing between sites that run Novell NetWare version 3.11 or later. The MAX TNT operates as an IPX router with one interface on the local Ethernet and the other across the WAN. It supports IPX routing over PPP, MP, MP+, and Frame Relay connections. Each RADIUS user profile that sets up an IPX connection is an IPX WAN interface.

NetWare servers broadcast Service Advertising Protocol (SAP) packets every 60 seconds to make sure that routers (such as the MAX TNT) know about their services. Each router builds a SAP table with an entry for each service that each known server advertises. The router uses the SAP table to respond to client queries.

When a NetWare client sends a SAP request to locate a service, the MAX TNT consults its SAP table and replies with its own hardware address and the internal address of the requested server. The client can then transmit packets whose destination address is the internal address of the server. When the MAX TNT receives those packets, it consults its IPX RIP table. If it finds an entry for that destination address, it brings up the connection or forwards the packet across the active connection.

For complete information about IPX routing, see the *MAX TNT Network Configuration Guide.*

Overview of IPX-routing configuration tasks

You can carry out the following IPX configuration tasks:

- In a RADIUS user profile, set IPX routing attributes for the WAN connection. (For details, see “Setting up IPX routing in a user profile” on page 10-4.)
- In a pseudo-user profile, set up static IPX routes. (For details, see “Setting up static IPX routes” on page 10-5.)

Setting up IPX routing in a user profile

Table 10-2 lists the attributes relevant to IPX routing for a WAN connection.

Table 10-2. IPX routing attributes

Attribute	Description	Possible values
Ascend-IPX-Alias (224)	Specifies the network number you assign to a point-to-point link.	8-digit (4-byte) hexadecimal value. The default value is 00000000. You need to specify a value for this attribute only if the MAX TNT operates with a non-Ascend router that uses a numbered interface. It does not apply if you are routing from one MAX TNT to another, or to a router that does not use a numbered interface.
Ascend-IPX-Peer-Mode (216)	Specifies whether the caller is a dial-in PPP client, or an Ethernet client with its own IPX network address.	IPX-Peer-Router (0) indicates that the calling device is on the Ethernet network and has its own IPX address. IPX-Peer-Dialin (1) indicates that the caller is a dial-in NetWare client that incorporates PPP software and dial-out hardware, but does not have an Ethernet interface. IPX-Peer-Router is the default.
Ascend-Route-IPX (229)	Specifies whether the user profile can use IPX routing.	Route-IPX-No (0) Route-IPX-Yes (1) Route-IPX-No is the default.

To set up IPX routing in a RADIUS user profile:

1. Set Ascend-Route-IPX=Route-IPX-Yes.
2. If the MAX TNT operates with a non-Ascend router that uses a numbered interface, set the Ascend-IPX-Alias attribute to specify a network number for the link.
3. If the caller is a dial-in PPP client, set Ascend-IPX-Peer-Mode=IPX-Peer-Dialin.

   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.

Example of configuring a dial-in client connection

In the following example, a NetWare client dials into a corporate IPX network that supports both servers and clients (Figure 10-1.).

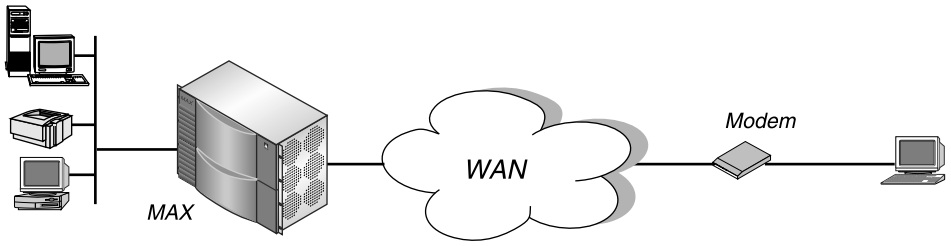


Figure 10-1. A dial-in NetWare client requiring dynamic IPX network assignment

In this example, the MAX TNT is connected to a corporate NetWare LAN and the dial-in client has a modem, NetWare client software, and PPP dial-up software. This example assumes that you have set the IPX Pool# parameter. To configure the MAX TNT to accept a connection from the PC dial-in user, enter the following specifications:

```
NetWareClient1 Password="m2dan", User-Service=Framed-User
     Framed-Protocol=PPP,
     Ascend-Route-IPX=Route-IPX-Yes,
     Ascend-IPX-Peer-Mode=IPX-Peer-Dialin,
     ...
```

Setting up static IPX routes

To create static IPX routes, you configure a pseudo-user profile containing the route specifications. After the MAX TNT unit clears its IPX RIP and SAP tables during a reset or power cycle, it adds the static routes upon initialization. Each static IPX route contains all the information necessary to reach one NetWare server on a remote network. When the MAX TNT receives an outbound packet for that server, it finds the corresponding RADIUS user profile and dials the connection.

You must manually update static routes whenever the administrator at the remote end removes the specified server or updates its address. You do not need to create IPX routes to servers that reside on the local Ethernet network.

Recommended configurations

Most sites configure only a few IPX routes and rely on IPX RIP for most other connections. If you have servers on both sides of the WAN connection, Ascend recommends that you define a static route to the remote site even if your environment requires dynamic routes. If you have one static route to a remote site, it should specify a master NetWare server that knows about many other services. NetWare workstations can then learn about other remote services by connecting to that remote NetWare server. If the MAX TNT does not receive IPX RIP broadcasts from a remote unit, you should configure a static route to at least one server on the remote network.

Configuring static IPX routes in a pseudo-user profile

To set up static IPX routes in a RADIUS pseudo-user profile, you must perform the following tasks:

- Create the first line of the pseudo-user profile.
- Set the Ascend-IPX-Route attribute to specify one or more static IPX routes.

Creating the first line of a pseudo-user profile for static IPX routes

You can configure pseudo-users for both global and MAX TNT-specific configuration control of IPX dialout routes. The MAX TNT loads the unit-specific dialout routes in addition to the global dialout routes.

For a unit-specific IPX dialout route, specify the first line of a pseudo-user profile in the following format:

ipxroute-*name*-*num* Password="ascend", User-Service=Dialout-Framed-User

For a global IPX dialout route, specify the first line of a pseudo-user profile in the following format:

ipxroute-*num* Password="ascend", User-Service=Dialout-Framed-User

The ***name*** argument is the system name of the MAX TNT (the name specified by the Name parameter in the System profile), and ***num*** is a number in a sequential series, starting at 1.

Specifying static IPX routes with the Ascend-IPX-Route attribute

In each pseudo-user profile, specify one or more routes with the Ascend-IPX-Route attribute. Use the following format:

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

The MAX TNT fetches information from each pseudo-user profile in order to gather routing information. Table 10-3 describes each Ascend-IPX-Route argument.

Table 10-3. 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 10-3. 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.

How the MAX TNT adds IPX dialout routes to the routing table

Whenever you power on or reset the MAX TNT, RADIUS adds IPX dialout routes to the routing table as follows:

1. RADIUS looks for profiles having the format ipxroute-***name***-1, where ***name*** is the system name.
2. If at least one such profile exists, RADIUS loads all existing profiles having the format ipxroute-***name***-***num*** to initialize the IPX routing table. The variable ***num*** is a number in a sequential series, starting with 1.
3. The MAX TNT queries ipxroute-***name***-1, then ipxroute-***name***-2, and so on, until it receives an authentication reject from RADIUS.
4. RADIUS loads the global configuration profiles. These configurations have the form ipxroute-***num***.
5. The MAX TNT queries ipxroute-1, then ipxroute-2, and so on, until it receives an authentication reject from RADIUS.

Example of configuring static IPX routes

The first example defines a unit-specific IPX route. The second example defines a global IPX route.

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

ipxroute-1 Password="ascend", User-Service=Dialout-Framed-User
        Ascend-IPX-Route="abc 1 2 3 4 5"
```

Setting Up Bridging for WAN Links

11

This chapter describes how to configure a RADIUS user profile for bridging connections, and how to set up bridge entries. The chapter is divided into the following sections:

Before you begin

Before you set up a bridging connection in RADIUS, you must set up the MAX TNT as a bridge. For instructions, see the *MAX TNT Network Configuration Guide*.

In addition, before you set bridging attributes, you must configure a RADIUS user profile containing:

- User-Name, Password, and other authentication attributes
- WAN connection attributes

Table 11-1 lists references for more information.

Table 11-1. Preliminary RADIUS tasks for bridging

Task	Reference
Setting User-Name, Password, and other authentication attributes	Chapter 4, "Setting Up RADIUS Authentication."
Configuring a PPP, MP, or MP+ connection	Chapter 5, "Setting Up PPP, MP, and MP+ Connections."
Setting up a terminal-server connection	Chapter 6, "Setting Up Terminal-Server Connections."
Setting up a Frame Relay connection	Chapter 7, "Setting Up Frame Relay Connections."

The most common cause of trouble when setting up a bridging connection is specifying the wrong name for the MAX TNT or the remote device. You must specify the name of the remote device or user exactly as it appears remotely, including case changes, dashes, and underscores.

Introducing bridging

The MAX TNT uses bridging to provide connectivity for protocols other than IP and IPX, although you can also use bridging to join segments of an IP or IPX network. Because a bridging connection forwards packets at the link layer, it does not distinguish between protocol types and requires no protocol-specific configuration.

When you configure the MAX TNT for bridging, it accepts all packets on the Ethernet network, and it forwards those that do not have a physical address on the local Ethernet segment or that have a broadcast address. A physical address is a unique, hardware-level address associated with a specific network controller. A device's physical address is also called its Media Access Control (MAC) address. A broadcast address is recognized by all nodes on a network. All devices on the same network receive packets with the same address (FFFFFFFFFFFF on Ethernet).

The MAX TNT is a transparent bridge (also called a learning bridge). As the MAX TNT forwards a packet, it notes the packet's source address and creates a bridge table that associates

node addresses with a particular interface. Figure 11-1. shows the physical addresses of some nodes on the local Ethernet and at a remote site. The MAX TNT at site A acts as a bridge.

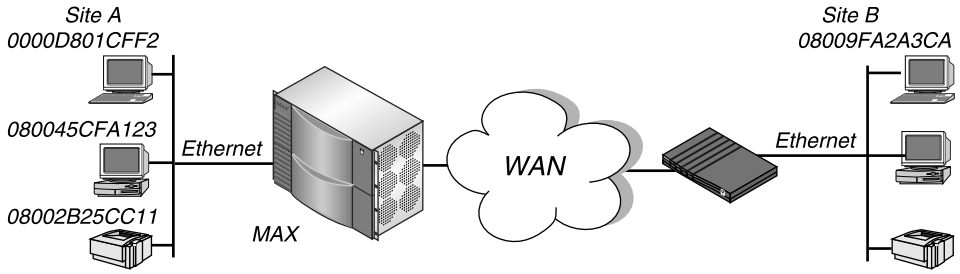


Figure 11-1. Bridging configuration

The MAX TNT at site A gradually learns addresses on both networks by looking at each packet's source address, and it develops a bridge table that includes the following entries:

```
0000D801CFF2        SITEA
080045CFA123        SITEA
08002B25CC11        SITEA
08009FA2A3CA        SITEB
```

If the MAX TNT receives a packet whose destination MAC address is not on the local network, it first checks its internal bridge table. If it find the packet's destination MAC address, the MAX TNT dials the connection and bridges the packet. If it does not find the address, the MAX TNT checks for active sessions that have bridging enabled. If one or more active bridging links are up, the MAX TNT forwards the packet across all active sessions that have bridging enabled.

The MAX TNT associates a Connection profile or RADIUS user profile with a bridging link either because the remote caller used the profile to dial the link, or because the profile matched an incoming call. You can also specify static bridge table entries in RADIUS pseudo-user profiles.

Overview of bridging configuration tasks

You can carry out the following bridging configuration tasks:

- In a RADIUS user profile, set bridging attributes for the WAN connection. (For details, see "Setting up bridging for a WAN connection" on page 11-4.)
- In a pseudo-user profile, set up bridge entries. (For details, see "Setting up bridge entries" on page 11-7.)

Setting up bridging for a WAN connection

This section describes how to set bridging attributes in a RADIUS user profile, and summarizes special requirements for bridging IPX. Table 11-2 lists the attributes you can set to configure a RADIUS user profile for protocol-independent bridging.

Table 11-2. Bridging attributes

Attribute	Description	Possible values
Ascend-Bridge (230)	Enables or disables protocol-independent bridging for the call.	Bridge-No (0) Bridge-Yes (1) Bridge-No is the default.
Ascend-Handle-IPX (222)	Specifies how the MAX TNT handles NCP watchdog requests on behalf of IPX clients during IPX bridging.	Handle-IPX-None (0) Handle-IPX-Client (1) Handle-IPX-Server (2) Handle-IPX-None is the default.
Ascend-Netware-timeout (223)	Sets how long, in minutes, the MAX TNT responds to NCP watchdog requests on behalf of IPX clients on the other side of an offline IPX bridging connection.	Integer between 0 and 65535. The default value is 0 (zero).

Configuring bridging attributes

To specify that bridging is available to a user profile:

1. Set Ascend-Bridge=Bridge-Yes.
2. If you wish to enable IPX routing for the link, set Ascend-Route-IPX=Route-IPX-Yes. This setting causes the Ascend-Handle-IPX attribute to act as though it is set to Handle-IPX-Server.
3. To specify special IPX bridging behavior, set the Ascend-Handle-IPX attribute. For information about the appropriate setting for your environment, see “Overview of special IPX bridging requirements” on page 11-5.
4. If you set Ascend-Handle-IPX=Handle-IPX-Server, set the Ascend-Netware-timeout attribute to indicate the maximum length of idle time during which the MAX TNT performs watchdog spoofing for NetWare connections.

Overview of special IPX bridging requirements

IPX bridging has special requirements for facilitating NetWare client-server logins across the WAN, and for preventing IPX RIP and SAP broadcasts from keeping a bridged connection up indefinitely. To specify special IPX bridging behavior, you use the Ascend-Handle-IPX attribute.

For the Ascend-Handle-IPX attribute to have any effect, the IPX Frame parameter in the MAX TNT configuration interface must specify the IPX frame type in use. Your setting for Ascend-Handle-IPX depends upon your bridging configuration. The following sections describe different types of bridging configurations.

Bridging when the local network supports only NetWare clients

If the local Ethernet supports NetWare clients only and no NetWare servers, the bridging connection should enable a local client to bring up the WAN connection by querying (broadcasting) for a NetWare server on a remote network. However, the connection should not stay up indefinitely on the basis of RIP or SAP broadcasts. If your configuration matches this one, set Ascend-Handle-IPX=Handle-IPX-Client.

Bridging when only the local network supports NetWare servers

If the local network supports NetWare servers (or a combination of clients and servers), and the remote network supports NetWare clients only, the bridging connection should enable the MAX TNT to respond to NCP watchdog requests on behalf of remote clients but bring down inactive connections whenever possible. In this case, set Ascend-Netware-timeout=30 (for example), and Ascend-Handle-IPX=Handle-IPX-Client.

Bridging when both sides of the link support NetWare servers

If NetWare servers reside on both sides of the WAN connection, Ascend strongly recommends that you use an IPX routing configuration instead of bridging IPX. If you bridge IPX in this type of environment, client-server logins are lost when the MAX TNT brings down an inactive WAN connection.

IPX routing and bridging on the same connection

When you enable IPX routing for a connection, the MAX TNT routes only one frame type for IPX packets across that connection. For example, if the IPX frame type is 802.3, the MAX TNT routes only 802.3 packets. If some NetWare servers on the local network use a different frame type, such as 802.2, the MAX TNT bridges those packets if you enable bridging, or discards them if you do not.

If IPX Frame=802.3 on the MAX TNT, the settings you make in RADIUS have the following effects:

- If Ascend-Route-IPX=Route-IPX-Yes and Ascend-Bridge=Bridge-No in the RADIUS user profile, the MAX TNT routes only 802.3 IPX packets, and drops all other packets.
- If Ascend-Route-IPX=Route-IPX-Yes and Ascend-Bridge=Bridge-Yes in the RADIUS user profile, the MAX TNT routes 802.3 IPX packets and bridges all other packets, including IPX packets in other frame types. For example, if the MAX TNT receives an IPX packet in the 802.2 packet frame, it uses the physical address in that packet to bridge it across all active bridging sessions.

Example of configuring an IPX bridge for local clients

In Figure 11-2., the local Ethernet supports NetWare clients, and the remote network supports both NetWare servers and clients.

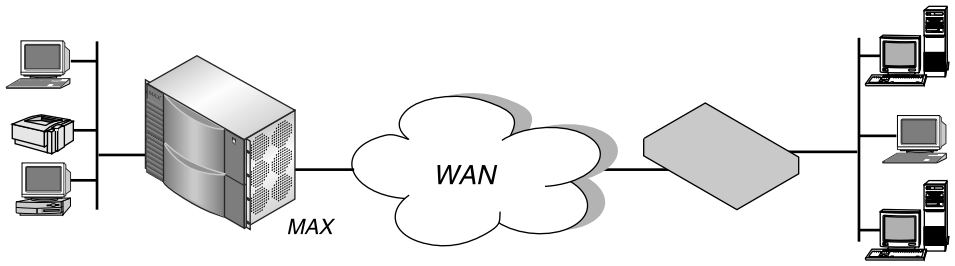


Figure 11-2. A sample IPX client bridging connection

To configure the MAX TNT in this example, you might use a profile like the following:

```
MAXTNT1 Password="m2dan", User-Service=Framed-User
     Framed-Protocol=PPP,
     Ascend-Route-IPX=Route-IPX-No,
     Ascend-Bridge=Bridge-Yes,
     Ascend-Handle-IPX=Handle-IPX-Client,
     Ascend-Netware-timeout=30
```

Example of configuring an IPX bridge for local servers

In Figure 11-3., the local network supports a combination of NetWare clients and servers, and the remote network supports clients only.

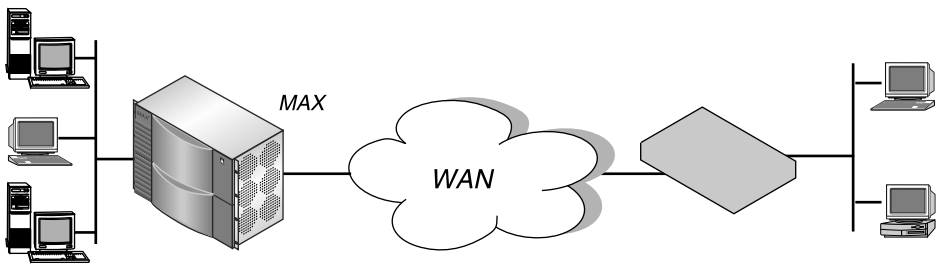


Figure 11-3. A sample IPX server bridging connection

To configure the MAX TNT in this example, you might use a profile like the following:

```
MAXTNT1 Password="m2dan", User-Service=Framed-User
     Framed-Protocol=PPP,
     Ascend-Route-IPX=Route-IPX-No,
     Ascend-Bridge=Bridge-Yes,
     Ascend-Handle-IPX=Handle-IPX-Server,
     Ascend-Netware-timeout=30
```

Setting up bridge entries

To create bridge entries for the bridging table, you configure a pseudo-user profile in the following manner:

- Create the first line of the pseudo-user profile
- Specify one or more bridge entries with the Ascend-Bridge-Address attribute

Creating the first line of a pseudo-user profile for bridge entries

You can create bridge entries for a single MAX TNT. Specify the first line of the pseudo-user profile in the following format:

`bridge-`*`name-num`*` Password="ascend", User-Service=Dialout-Framed-User`

where the ***`name`*** argument is the system name of the MAX TNT (the name specified by the Name parameter in the System profile), and ***`num`*** is a number in a sequential series, starting at 1.

Specifying bridge entries with the Ascend-Bridge-Address attribute

Each Ascend-Bridge-Address setting specifies the IP address and associated MAC address of a device on a remote LAN to which the MAX TNT can form a bridging connection. When your MAX TNT receives an ARP request for one of the IP addresses you specify, the MAX TNT replies with the corresponding MAC address and uses the profile to bring up a connection to that address. Because the MAX TNT replies to these ARP requests as if the IP devices were local, you must have user profiles that bridge IP packets to each device.

For each pseudo-user profile, specify one or more bridge entries with the Ascend-Bridge-Address attribute. Use the following format:

`Ascend-Bridge-Address="`*`MAC_address profile_name IP_address`*`"`

Table 11-3 describes Ascend-Bridge-Address arguments.

Table 11-3. Ascend-Bridge-Address arguments

Argument	Specifies
`MAC_address`	MAC address in standard 12-digit hexadecimal format (yyyyyyyyyyyy) or in colon-separated format (yy:yy:yy:yy:yy:yy). If the leading digit of a colon-separated pair is 0 (zero), you do not need to enter it. That is, **`:y`** is the same as **`:0y`**. The default value is 000000000000.
`profile_name`	Name of the dialout profile the MAX TNT uses to bring up the connection. You can specify either a Connection profile or a RADIUS user profile. The MAX TNT looks for a local profile first.
`IP_address`	IP address in dotted decimal notation. The default value is 0.0.0.0.

How the MAX TNT adds bridge entries to the bridging table

Whenever you power on or reset the MAX TNT, RADIUS looks for profiles having the format bridge-***name***-***num***, where ***name*** is the system name and ***num*** is a number in a sequential series, starting with 1. If it finds one or more such profiles, it loads the data to create the bridging tables.

Example of configuring bridge entries

The following example creates two bridging table entries:

```
bridge-CA-1 Password="ascend", User-Service=Dialout-Framed-User
        Ascend-Bridge-Address="2:2:3:10:11:12 Prof1 1.2.3.4 1",
        Ascend-Bridge-Address="2:2:3:13:14:15 Prof2 5.6.7.8 2"
```

Setting Up Filters

12

This chapter describes how to configure filters, and consists of the following sections:

Before you begin

If you plan to configure RADIUS to accept filter-change requests, you must specify settings in the Rad-Auth-Server subprofile of the External-Auth profile. For information about how to carry out this task, see “Configuring the MAX TNT for RADIUS client requests” on page 3-9.

Overview of packet filters

A packet filter contains rules that instruct the MAX TNT on what to do when it encounters different types of packets. When you specify a packet filter in a RADIUS user profile, the MAX TNT monitors the data stream associated with that profile and takes a specified action when packet contents match the filter rules. Each filter specification either forwards or drops packets. You can apply a filter to inbound packets, outbound packets, or both. In addition, you can specify that the MAX TNT forward or drop those packets that match the rules, or all packets *except* those that match the rules.

Types of packet filters

The MAX TNT supports two types of packet filters: generic and IP. The sections that follow describe each type of filter.

Generic filters

A generic filters examine the byte- or bit-level contents of a packet. It focuses on certain bytes or bits and compare them with a value defined in the filter. To use generic filters effectively, you need to know the contents of certain bytes in the packets you wish to filter. Protocol specifications are usually the best source of such information.

IP filters

An IP filter examines higher level fields specific to IP packets. It focuses on known fields, such as source or destination address, protocol number, and so forth. An IP filter operates on logical information that is relatively easy to obtain.

Ways to apply packet filters

You can apply a generic or IP filter as either a data filter of a call filter. The sections that follow describe each method.

Data filters for dropping or forwarding certain packets

A data filter defines which packets the MAX TNT can transmit on a connection. Many sites use data filters for security purposes, but you can apply data filters to any purpose that requires the MAX TNT to drop or forward only specific packets. For example, you can use data filters to drop packets addressed to particular hosts or to prevent broadcasts from going across the WAN. You can also use data filters to allow users to access only specific devices across the WAN.

When you apply a data filter, its forward or drop action affects the actual data stream by preventing certain packets from reaching the Ethernet from the WAN, or vice versa (Figure 12-1.).

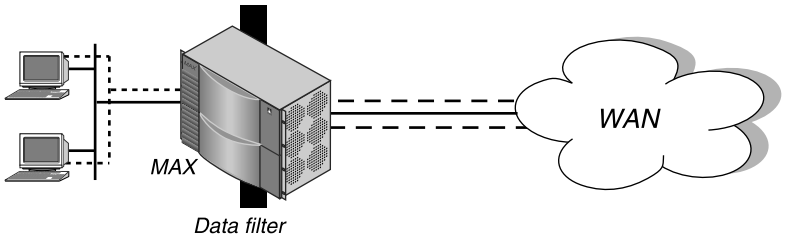


Figure 12-1. Data filters can drop or forward certain packets

Data filters do not affect the idle timer, and a data filter applied to a RADIUS user profile does not affect the answering process.

Call filters for managing connections

A call filter defines which packets can or cannot bring up a connection or reset the idle timer for an established link (Figure 12-2.).

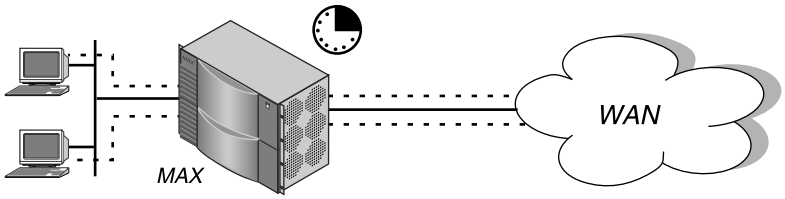


Figure 12-2. Call filters can prevent certain packets from resetting the timer

A call filter prevents unnecessary connections and helps the MAX TNT distinguish active traffic from "noise." By default, any traffic to a remote site triggers a call, and any traffic across an active connection resets the connection's idle timer.

When you apply a call filter, its forwarding action does not affect which packets are sent across an active connection. The forwarding action of a call filter determines which packets can initiate a connection or reset a session's timer. When a session's idle timer expires, the MAX TNT terminates the session. The idle timer is set to 120 seconds by default, so if a connection is inactive for two minutes, the MAX TNT terminates the connection.

How packet filters work

You can specify several filters in a RADIUS user profile. Filter entries apply on a first-match basis. Therefore, the order in which you specify filter entries is significant. When you define a filter in a RADIUS user profile, it applies to data the user sends or receives. If you make changes to a filter, the changes do not take affect until a call uses that profile.

A match occurs at the first successful comparison between a filter and the packet being examined. When a comparison succeeds, the filtering process stops and the MAX TNT applies the forward or drop action to the packet.

If no comparisons succeed, the packet does not match the filter. However, the MAX TNT does not forward the packet. When no filter is in use, the MAX TNT forwards all packets. However, once you apply a filter to a connection, this default is *reversed*. For security purposes, the MAX TNT does not automatically forward non-matching packets. It requires a rule that explicitly allows those packets to pass.

In a generic filter, all settings work together to specify a location in a packet and a number that the MAX TNT compares to the value in that location. In an IP filter, the MAX TNT makes a set of distinct comparisons in order. When a comparison fails, the packet goes on to the next comparison. When a comparison succeeds, the filtering process stops and the MAX TNT applies the forward or drop action to the packet. The IP filter tests proceed in the following order:

1 Compare the source address specified by the filter to the source address of the packet. If they are not equal, the comparison fails.

2 Compare the destination address specified by the filter to the destination address in the packet. If they are not equal, the comparison fails.

3 If the protocol specified by the filter is zero (which matches any protocol), the comparison succeeds. If it is non-zero and not equal to the protocol field in the packet, the comparison fails.

4 If the source port specified by the filter does not compare to the source port of the packet as the filter indicates, the comparison fails.

5 If the destination port specified by the filter does not compare to the destination port of the packet as the filter indicates, the comparison fails.

6 If the filter specifies a match only if a TCP session is already established, and a TCP session is up, the comparison succeeds.

Overview of filter configuration tasks

When you set up filters, you can:

- Set up an IP filter, as described in “Configuring an IP filter” on page 12-4.
- Set up a generic filter, as described in “Configuring a generic filter” on page 12-7.
- Set up a client to request filter changes, as described in “Setting up filter changes” on page 12-11.

Configuring an IP filter

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 is shown here on multiple lines for printing purposes only.

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*]]"**

Table 12-1 describes each element of the syntax.

Table 12-1. IP filter syntax elements

Keyword or argument	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_ipaddrsubnet_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 this keyword and its IP address specification are not present, the filter matches all IP packets.
srcip *src_ipaddrsubnet_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 this 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 12-1. IP filter syntax elements (continued)

Keyword or argument	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).

Example of configuring an IP data filter for prevention of IP address spoofing

IP address spoofing occurs when a remote device illegally acquires a local address to break through a firewall. The following example show you how to define filters to prevent break-ins that use address spoofing. Proceed as follows:

1 Define a filter that drops incoming packets whose source address is on the local IP network (200.100.50.128):

```
Ascend-Data-Filter="ip in drop srcip 200.100.50.128"
```

Because ***action*** is set to **drop**, if an incoming packet has the local address, the MAX TNT does not forward it.

2 Define a filter that drops packets whose source address is the loopback address (127.0.0.0):

```
Ascend-Data-Filter="ip in drop srcip 127.0.0.0"
```

3 Define a filter that specifies every other source address (0.0.0.0) and indicates that the MAX TNT should forward all other packets:

```
Ascend-Data-Filter="ip in forward"
```

4 Define a filter that specifies that the MAX TNT should forward packets originating on the local network:

```
Ascend-Data-Filter="ip out forward srcip 200.100.50.128"
```

Configuring a generic filter

Use the following format for a generic data filter entry:

Ascend-Data-Filter="generic *dir action offset mask value compare* [more]"

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

Use the following format for a generic call filter entry:

Ascend-Call-Filter="generic *dir action offset mask value compare* [more]"

Table 12-2 describes each element of the syntax.

Table 12-2. Generic filter syntax elements

Keyword or argument	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 cannot exceed 6 bytes (12 hexadecimal digits). A one bit in the mask indicates a bit to compare. A zero bit indicates a bit to ignore. The length of the mask specifies the length of the comparison.

Table 12-2. Generic filter syntax elements (continued)

Keyword or argument	Description
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.

Understanding generic data filters

Generic filters can affect any packet, regardless of its protocol type or header fields. This section provides some background information about how a generic filter specification works. The section describes a data filter with the following setting:

```
Ascend-Data-Filter="generic in drop 2
ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff
aa:aa:03:00:00:00:80:f3:00:00:00:00"
```

Determining whether inbound or outbound data is examined

In this example, the filter examines inbound data only.

Specifying an offset to the bytes in a packet to be examined

The ***offset*** argument specifies a byte offset from the start of a frame to the data the MAX TNT tests against the filter. For example, suppose you specify 2 for the ***offset*** argument, and the packet contents look like the following:

```
2A 31 97 FE 45 70 12 22 33 99 B4 80 75
```

The MAX TNT ignores the first two byes in the packet (2A and 31).

Linking the filter to the next one in sequence

If the **more** argument is present, the MAX TNT includes the next filter before determining whether the frame matches the filter. In this case, the **more** argument is not present, so the MAX TNT does not include the next filter.

Masking the value before comparison

The ***mask*** argument specifies a 12-byte mask to apply to the ***value*** argument before the MAX TNT compares it to the packet contents at the specified offset. You can use the mask to finetune exactly which bits you want to compare.

After the mask and value are both translated into binary format, the MAX TNT applies the mask to the specified value with a logical AND. The mask hides the bits that appear behind each binary 0 (zero) in the mask. A mask of all ones (FF:FF:FF:FF:FF:FF:FF:FF) masks no bits, so the full specified value must match the packet contents. For example, suppose you specify the following values:

***offset*=2**

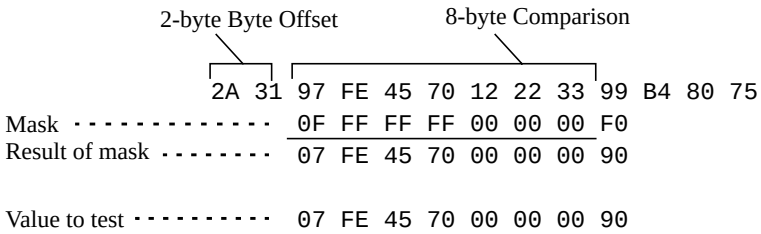
***mask*=0f:ff:ff:ff:00:00:00:f0:00:00:00:00**

***value*=07:fe:45:70:00:00:00:90:00:00:00:00**

and the packet contents the following data:

```
2A 31 97 FE 45 70 12 22 33 99 B4 80 75
```

The MAX TNT applies the mask as shown below, resulting in a value that matches the setting for the ***value*** argument.



The packet matches the filter. Because the ***action*** argument is set to **drop**, the MAX TNT drops the packet. The byte comparison works as follows:

- The MAX TNT ignores 2A and 31 because of the two-byte offset.
- The MAX TNT ignores 9 in the lower half of the third byte, because the mask has a 0 (zero) in its place. The 7 in the third byte matches the ***value*** argument's 7 in the upper half of that byte.
- F and E in the fourth byte match the ***value*** specified by the filter for that byte.
- 4 and 5 in the fifth byte match the ***value*** specified by the filter for that byte.
- 7 and 0 in the sixth byte match the ***value*** specified by the filter for that byte.
- The MAX TNT ignores 12 and 22 and 33 in the seventh, eighth and ninth bytes because the mask has a 0 (zero) in those places.
- 9 in the tenth byte matches the ***value*** argument's 9 in the lower half of the byte. The MAX TNT ignores the second 9 in the upper half of the packet's tenth byte because the mask has a 0 (zero) in its place.

Using a generic call filter for AppleTalk traffic

In the following scenario, several Macintosh workstations are running Open Transport on the local LAN, and you want only IP traffic destined for the WAN to bring up a connection. To ensure that AppleTalk packets with destinations on the local LAN do not bring up a connection, you must specify several generic call filters.

Configure a separate filter to carry out each of the following tasks. You must create the filters in the specified order.

1 Drop AppleTalk Address Resolution Protocol (AARP) packets. The following filter specification keeps AARP packets (protocol ID 80f3) from bringing up a connection:

```
Ascend-Call-Filter="generic out drop 14 ffffffffffffffff
aaaa0300000080f3"
```

2 Forward non-AppleTalk traffic. AppleTalk has the protocol 809b. The following filter specification forwards all non-AppleTalk packets:

```
Ascend-Call-Filter="generic out forward 14 ffffffffffffffff
aaaa03080007809b !="
```

From this point on, any additional filters deal only with AppleTalk traffic.

3 Drop AppleTalk Echo Protocol (AEP) packets. The following filter specification keeps AEP packets from bringing up a connection:

```
Ascend-Call-Filter="generic out drop 32 ffffff0000000000
0404040000000000 !="
```

4 Forward all traffic not destined for an AppleTalk multicast address. (AppleTalk uses a multicast address, rather than a broadcast address.) The following filter specification forwards all packets not destined for that multicast address:

```
Ascend-Call-Filter="generic out forward 32 ffffffffffff0000
090007ffffff0000 !="
```

5 Forward Name Binding Protocol (NBP) lookup packets, but only those that the Chooser makes use of (that is, only those with a wildcard entity name). The following filter specification indicates that the filter forwards NBP packets:

```
Ascend-Call-Filter="generic out forward 32 ff00fff000000000
0200022000000000 more"
```

The `more` value indicates that the MAX TNT must examine the next specification before making the decision to forward a packet. The next specification indicates that the MAX TNT should forward only those packets with a wildcard entity name:

```
Ascend-Call-Filter="generic out forward 42 ffff000000000000
013d000000000000"
```

Setting up filter changes

If you write a special RADIUS client program to change filters, the MAX TNT can accept RADIUS requests from clients to change a filter for a particular session, user, or IP address. The following sections describe how to configure filter-change requests.

Overview of filter-change attributes

A RADIUS Change-Filter-Request packet (code 43) contains the attributes necessary for making a filter-change request. Table 12-3 lists these attributes.

Table 12-3. Filter-change attributes

Attribute	Description	Possible values
Acct-Session-Id (44)	Identifies a bridging, routing, or terminal-server session.	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.
Ascend-Data-Filter (242)	Specifies the data filter to use.	See page 12-4 and page 12-7.
Ascend-Call-Filter (243)	Specifies the call filter to use.	See page 12-5 and page 12-7.
Ascend-Session-Svr-Key (151)	Enables the MAX TNT to match a user session with a client request.	Text string of up to 16 characters. The default value is null.
Framed-Address (8)	Specifies the IP address of the user. The MAX TNT changes filters for all routing or bridging sessions associated with the specified address. If you specify User-Name as well, the MAX TNT changes filters only for routing/bridging sessions associated with both attributes.	IP address in dotted decimal notation *n.n.n.n*, where *n* is an integer between 0 and 255. The MAX TNT ignores the default address of 0.0.0.0.
User-Name (1)	Specifies the user's name. The MAX TNT changes filters for all routing or bridging sessions associated with the user name. If you specify Framed-Address as well, the MAX TNT changes filters for only routing/bridging sessions associated with both attributes.	Text string of up to 252 characters. The default value is null. The string need not be null terminated.

Configuring attributes for filter-change requests

The MAX TNT sends the session key and session ID in all RADIUS access requests. You can also obtain the session key, session ID, and user name through RADIUS accounting or from the accounting MIB (for systems that support SNMP accounting). If the MAX TNT assigns the IP address from a pool, RADIUS accounting or the accounting MIB can provide the address as well.

Note: The Auth-Session-Key and Auth-Attribute-Type parameters in the External-Auth profile's Rad-Auth-Server subprofile determine the attributes the MAX TNT uses when handling the filter-change request. For complete information about setting these parameters, see "Specifying session key parameters" on page 3-11.

To set up a RADIUS user profile that requests a filter change, you must carry out the following steps:

1. Specify the values for the User-Name and Password attributes. These attributes must identify a user at the IP address indicated by the Auth-Client or Auth-Netmask parameters in the External-Auth profile's Rad-Auth-Server subprofile.
2. Set the Ascend-Data-Filter attribute to specify the data filter to use. You can specify this attribute more than once.
3. Set the Ascend-Call-Filter attribute to specify the call filter to use. You can specify this attribute more than once.

Depending upon the needs of your site, you can carry out the following additional steps:

1. To identify the session by IP address, set the Framed-Address attribute.
2. To identify the session by its ID number, set the Acct-Session-Id attribute. The number you specify must match the session reference number used in SNMP accounting or RADIUS accounting.
3. To identify the session by a session key, set the Ascend-Session-Svr-Key attribute.

How the MAX TNT handles filter-change requests

The MAX TNT silently discards a Change-Filter-Request packet if one of the following conditions is true:

- The packet is badly formatted.
- The client is not on the list of clients allowed to send RADIUS requests to the server.
- The authenticator field is incorrect.
- The packet contains invalid attribute values.

If RADIUS finds at least one routing/bridging session whose filters it can change, the response code is 44 (Change-Filter-Request-ACK). Otherwise, the code is 45 (Change-Filter-Request-NAK). RADIUS does not return any attributes in the response.

Setting Up RADIUS Accounting

13

This chapter discusses how to set up RADIUS accounting. It consists of the following sections:

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 3-3.

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 13-2. Other system-wide settings are optional, as described in “Performing optional accounting configuration tasks” on page 13-3.

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 13-4.)
- Configure accounting with dynamic IP addressing. (For instructions, see “Setting up accounting with dynamic IP addressing” on page 13-7.)
- Gather information on user sessions. (For instructions, see “Classifying user sessions in RADIUS” on page 13-8.)
- Use the SNMP Set command to specify the primary accounting server. (For instructions, see “Using SNMP to specify the primary accounting server” on page 13-9.)

Finally, to start up the RADIUS accounting server, follow the instructions in “Starting the RADIUS daemon with accounting enabled” on page 13-10.

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

Depending on the needs of your site, you have the option of specifying the following accounting values:

- Timeout value
- Session-report interval
- Numeric base for the session ID
- Source for RADIUS accounting requests

You set each value in the Rad-Acct-Client subprofile of the External Auth profile.

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 to a value between 1 and 10. The default value is 1.

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 13-8.)

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 for the Acct-Id-Base parameter:

- 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 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.

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 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.
- Both servers.

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 specified in Table 13-1.

Table 13-1. 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.
Ascend-User-Acct-Time (143)	Specifies the number of seconds the MAX TNT waits for a response to a RADIUS accounting request.	Integer from 1 to 10. The default value is 1.
Ascend-User-Acct-Type (138)	Specifies the RADIUS accounting server 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 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. If Ascend-User-Acct-Type=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

The following user profile sets up per-user accounting for the user Emma:

```
Emma Password="m2dan", User-Service=Framed-User
     Framed-Protocol=PPP,
     Framed-Address=200.250.55.9,
     Framed-Netmask=255.255.255.248,
     Ascend-Link-Compression=Link-Comp-Stac,
     Framed-Compression=Van-Jacobson-TCP-IP,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Metric=2,
     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 information, but not the IP address of the caller.

To track calls during the authentication period, you must set up one or more IP address pools as described in “Defining a pool of addresses for dynamic assignment” on page 9-9. 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 RADIUS accounting entries. The MAX TNT returns the address to the pool only 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, and 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, such as for the purpose of 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 (as long as the Auth-Type parameter on the MAX TNT is not set to RADIUS-Logout). 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 Auth-Sess-Interval parameter in the External-Auth profile's Rad-Auth-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:

- Where accounting records are stored
- What kinds of packets RADIUS accounting uses
- Which attributes appear in each type of packet

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 packets and Accounting Stop packets.

Accounting Start packets

Accounting Start packets signal a Start session event. When the MAX TNT begins a terminal-server, bridging, 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. At the end of a session, including cases in which a user fails authentication, the MAX TNT sends an Accounting Stop packet. Information from an Accounting Stop packet appears in a Stop record or Failure-to-start record in the log file.

Non-accounting attributes in accounting records

An accounting record can contain attributes that are not accounting specific. Table 13-2 lists them. Of the attributes listed in Table 13-2, only the NAS-Identifier attribute can appear in a Failure-to-start record.

Table 13-2. Non-accounting attributes in accounting records

Attribute	Description
Ascend-Dial-Number (227)	Indicates the phone number of the device that originated the connection.
Caller-Id (31)	Indicates the calling-party number, which is the phone number of the user that has connected to the MAX TNT.
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.

Table 13-2. Non-accounting attributes in accounting records (continued)

Attribute	Description
Framed-IPX-Network (23)	Indicates the network number of the router at the remote end of the connection. The default value is null.
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 an Accounting-Stop packet for a Failure-start-session event.
NAS-Port (5)	Indicates the network port on which the MAX TNT received the call. This attribute does not appear in an Accounting-Stop packet for a Failure-start-session event.
User-Name (1)	Indicates the name of the user starting the session.

Accounting attributes in Start records

Table 13-3 lists the accounting-specific attributes that can appear in a Start record.

Table 13-3. 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 bridging, 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.

Table 13-3. Accounting-specific attributes in Start records (continued)

Attribute	Description
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-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 connection.
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 13-4 lists the accounting attributes that can appear in a Stop record.

Table 13-4. 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.	Auth-Type parameter not set to RADIUS-Logout. 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.	Auth-Type parameter not set to RADIUS-Logout.
Acct-Input-Octets (42)	Indicates the number of octets the MAX TNT received during the session.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated.
Acct-Input-Packets (47)	Indicates the number of packets the MAX TNT received during the session.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated. A framed protocol must be in use.
Acct-Output-Octets (43)	Indicates the number of octets the MAX TNT sent during the session.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated.
Acct-Output-Packets (48)	Indicates the number of packets the MAX TNT sent during the session.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated. A framed protocol must be in use.

Table 13-4. Accounting-specific attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
Acct-Session-Id (44)	Consists of a unique numeric string identified with the bridging, routing, or terminal-server session reported in the Accounting packet. The string is a random number 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.	Auth-Type parameter not set to RADIUS-Logout.
Acct-Session-Time (46)	Indicates the number of seconds the session has been logged in.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated.
Acct-Status-Type (40)	Requests that have Acct-Status-Type=Start are 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.	Auth-Type parameter not set to RADIUS-Logout.
Ascend-Connect-Progress (196)	Indicates the state of the connection before it disconnects.	Auth-Type parameter not set to RADIUS-Logout.
Ascend-Data-Rate (197)	Indicates the data rate of the connection in bits per second.	Auth-Type parameter not set to RADIUS-Logout.
Ascend-Disconnect-Cause (195)	Indicates the reason a connection was taken offline.	Auth-Type parameter not set to RADIUS-Logout.
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.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated.

Table 13-4. Accounting-specific attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
Ascend-Multilink-ID (187)	Reports the ID number of the Multilink bundle when the session closes.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated.
Ascend-Num-In-Multilink (188)	Records the number of sessions remaining in a Multilink bundle when the session closes.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated.
Ascend-Number-Sessions (202)	Indicates the number of active user sessions of a given class (as specified by the Class attribute). In the case of multi-channel 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.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated.
Ascend-Pre-Input-Packets (192)	Reports the number of packets the MAX TNT received before authentication.	The Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated.
Ascend-Pre-Output-Octets (191)	Reports the number of octets the MAX TNT sent before authentication.	Auth-Type parameter not set to RADIUS-Logout. Session must be authenticated.
Ascend-Pre-Output-Packets (193)	Reports the number of packets the MAX TNT sent before authentication.	Auth-Type parameter not set to RADIUS-Logout. 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.	Auth-Type parameter not set to RADIUS-Logout.
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.

Table 13-4. Accounting-specific attributes in Stop records (continued)

Attribute	Description	Conditions for inclusion
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.

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 13-4 on page 13-14.

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

A Pipeline 25 dialing into a MAX TNT

When a Pipeline 25 dials into a MAX TNT with PPP, the Start record might look like the following:

```
Tue Feb 18 12:00:41 1997 /* Session startup time */
   User-Name="ht-net" /* The name of the Pipeline 25 */
   NAS-Identifier=206.65.212.46 /* The IP address of the MAX 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=64000 /* Data rate in bits per second */
   Ascend-PreSession-Time=0 /*Secs from connection to authentication*/
   Ascend-Pre-Input-Octets=174 /* Input octets pre-authentication */
   Ascend-Pre-Output-Octets=204 /* Output octets pre-authentication */
   Ascend-Pre-Input-Packets=7 /* Input packets pre-authentication */
   Ascend-Pre-Output-Packets=8 /* Output packets pre-authentication */
   Ascend-First-Dest=10.81.44.111 /* Dest IP address of 1st packet */
   Ascend-Multilink-ID=64 /* ID number of Multilink bundle */.
   Ascend-Num-In-Multilink=0 /* # of sessions in Multilink bundle */
   Client-Port-DNIS="3142" /* Called-party number */
   Framed-Protocol=PPP /* PPP call */
   Framed-Address=11.0.0.1 /* IP address of the Pipeline 25 */
```

A modem calling into a MAX 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=64000 /* Data rate in bits per second */
   Ascend-PreSession-Time=0 /*Secs from connection to authentication*/
   Ascend-Pre-Input-Octets=174 /* Input octets pre-authentication */
   Ascend-Pre-Output-Octets=204 /* Output octets pre-authentication */
   Ascend-Pre-Input-Packets=7 /* Input packets pre-authentication */
   Ascend-Pre-Output-Packets=8 /* Output packets pre-authentication */
   Ascend-First-Dest=10.81.44.111 /* Dest IP address of 1st packet */
   Ascend-Multilink-ID=64 /* ID number of Multilink bundle *.
   Ascend-Num-In-Multilink=0 /* # of sessions in Multilink bundle */
   Client-Port-DNIS="3143" /* Called-party number */
   Login-Service=Unframed-User /* Modem call */
```

Reference to RADIUS Attributes

14

This chapter discusses RADIUS attributes found in user and pseudo-user profiles. Each listing 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.

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) when the Auth-Type parameter is not set to RADIUS-Logout.

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 or when a session fails authentication (Acct-Status-Type=Stop), and the Auth-Type parameter is not set to RADIUS-Logout.

Acct-Input-Octets (42)

Description: Indicates how many octets the MAX TNT received during the session.

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 Auth-Type parameter is not set to RADIUS-Logout.

Acct-Input-Packets (47)

Description: Indicates how many packets the MAX TNT received during the session.

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 all of the following conditions are true:

- The session has been authenticated.
- The Auth-Type parameter is not set to RADIUS-Logout.
- A framed protocol is in use.

Acct-Output-Octets (43)

Description: Indicates how many octets the MAX TNT has sent during the session.

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 Auth-Type parameter is not set to RADIUS-Logout.

Acct-Output-Packets (48)

Description: Indicates how many packets the MAX TNT has sent during the session.

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 all of the following conditions are true:

- The Auth-Type parameter is not set to RADIUS-Logout.
- The session is authenticated.
- A framed protocol is in use.

Acct-Session-Id (44)

Description: Identifies the bridging, 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 of up to seven digits, with a range from 1 to 2,137,383,647. For every session, RADIUS generates a unique session ID, thereby preventing the same session ID from applying to more than one session.

Dependencies: 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, or when a session failed authentication (Acct-Status-Type=Stop), and the Auth-Type parameter is not set to RADIUS-Logout.

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 both of the following conditions are true:

- The session has been authenticated.
- The Auth-Type parameter is not set to RADIUS-Logout.

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 bridging, 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, or when a session fails authentication (when Acct-Status-Type=Stop), but only if the Auth-Type parameter is not set to RADIUS-Logout.

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 between 1 and 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: "Configuring DBA in RADIUS" on page 5-25,
"Ascend-Base-Channel-Count (172)" on page 14-8,
"Ascend-DBA-Monitor (171)" on page 14-27,
"Ascend-Dec-Channel-Count (237)" on page 14-27,
"Ascend-History-Weigh-Type (239)" on page 14-42,
"Ascend-Inc-Channel-Count (236)" on page 14-45,
"Ascend-Maximum-Channels (235)" on page 14-50,
"Ascend-Minimum-Channels (173)" on page 14-54,
"Ascend-Remove-Seconds (241)" on page 14-65,
"Ascend-Seconds-Of-History (238)" on page 14-68, and
"Ascend-Target-Util (234)" on page 14-71.

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: "Configuring IP address pools shared by several MAX TNT units" on page 9-12,
"Ascend-Assign-IP-Global-Pool (146)" on page 14-6, and
"Ascend-Assign-IP-Server (145)" on page 14-7.

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: “Configuring IP address pools shared by several MAX TNT units” on page 9-12 and “Ascend-IP-Pool-Definition (217)” on page 14-47.

Ascend-Assign-IP-Pool (218)

Description: Specifies the MAX TNT-specific address pool from which RADIUS assigns the user an IP 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 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: "Configuring IP address pools for a single MAX TNT" on page 9-11 and "Ascend-IP-Pool-Definition (217)" on page 14-47.

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.

See Also: "Configuring IP address pools shared by several MAX TNT units" on page 9-12.

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. The default is the value of the Name parameter in the System profile on the MAX TNT.

Example: The following example uses the Ascend-Authen-Alias attribute in an outgoing profile:

```
Homer-Out Password="ascend", User-Service=Dialout-Framed-User
      User-Name="Homer",
      Ascend-Authen-Alias="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. When the physical connection fails due to loss of a T1 line or serial WAN port, the MAX TNT automatically diverts traffic to the backup connection. When the primary connection is back online, traffic again uses the primary connection.

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.
- Outgoing Frame Relay packets are the only packets that follow the primary profile definitions. All other packets follow the backup profile definitions.
- 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.
- If you configure a RADIUS user profile for Frame Relay and for backup, the MAX TNT brings up the backup connection when any one of the DLCIs becomes unusable.
- Do not use the Ascend-Backup attribute to provide alternative lines for getting to a single destination.

Ascend-BACP-Enable (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.

See Also: “Setting up a Nailed/MPP connection” on page 5-16.

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: "Configuring DBA in RADIUS" on page 5-25,
"Ascend-Add-Seconds (240)" on page 14-5,
"Ascend-DBA-Monitor (171)" on page 14-27,
"Ascend-Dec-Channel-Count (237)" on page 14-27,
"Ascend-History-Weigh-Type (239)" on page 14-42,
"Ascend-Inc-Channel-Count (236)" on page 14-45,
"Ascend-Maximum-Channels (235)" on page 14-50,
"Ascend-Minimum-Channels (173)" on page 14-54,
"Ascend-Remove-Seconds (241)" on page 14-65,
"Ascend-Seconds-Of-History (238)" on page 14-68, and
"Ascend-Target-Util (234)" on page 14-71.

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 on an ISDN BRI line 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: "Setting up CLID authentication" on page 4-20 and
"Caller-Id (31)" on page 14-76.

Ascend-Bridge (230)

Description: Enables or disables protocol-independent bridging for the user profile.

Usage: Specify one of the following values:

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

Example: The following user profile specifies an IPX bridging link:

```
MAXTNT1 Password="m2dan", User-Service=Framed-User
     Framed-Protocol=PPP,
     Ascend-Route-IPX=Route-IPX-No,
     Ascend-Bridge=Bridge-Yes,
     Ascend-Handle-IPX=Handle-IPX-Client,
     Ascend-Netware-timeout=30
```

See Also: "Setting up bridging for a WAN connection" on page 11-4 and "Ascend-Bridge-Address (168)" on page 14-10.

Ascend-Bridge-Address (168)

Description: Specifies the IP address and associated MAC address of a device on a remote LAN.

Usage: The Ascend-Bridge-Address attribute has the following format:

`Ascend-Bridge-Address="`*`MAC_address profile_name IP_address`*`"`

Table 14-1 describes Ascend-Bridge-Address arguments.

Table 14-1. Ascend-Bridge-Address arguments

Argument	Specifies
`MAC_address`	MAC address in standard 12-digit hexadecimal format (yyyyyyyyyyyy) or in colon-separated format (yy:yy:yy:yy:yy:yy). If the leading digit of a colon-separated pair is 0 (zero), you do not need to enter it. That is, **`:y`** is the same as **`:0y`**. The default value is 000000000000.
`profile_name`	Name of the dialout profile the MAX TNT uses to bring up the connection. You can specify either a Connection profile or a RADIUS user profile. The MAX TNT looks for a local profile first.
`IP_address`	IP address in dotted decimal notation. The default value is 0.0.0.0.

Dependencies: When your MAX TNT receives an ARP request for one of the IP addresses you specify, the MAX TNT replies with the corresponding MAC address, and uses the specified profile to bring up a connection to that address. Because the MAX TNT replies to the ARP requests as if the IP devices were local, you must have user profiles that bridge IP packets to each device.

Example: The following pseudo-user profile creates two bridging-table entries:

```
bridge-CA-1 Password="ascend", User-Service=Dialout-Framed-User
        Ascend-Bridge-Address="2:2:3:10:11:12 Prof1 1.2.3.4 1",
        Ascend-Bridge-Address="2:2:3:13:14:15 Prof2 5.6.7.8 2"
```

See Also: "Setting up bridge entries" on page 11-7 and "Ascend-Bridge (230)" on page 14-10.

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: "Setting up the MAX TNT for callback" on page 4-19.

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 14-2 lists the services available for each service provider.

Table 14-2. Ascend-Call-By-Call settings

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

Ascend-Call-Filter (243)

Description: 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_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 14-3 describes each element of the syntax. None of the keywords are case sensitive.

Table 14-3. IP call filter syntax elements

Keyword or argument	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.
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).

Table 14-3. IP call filter syntax elements (continued)

Keyword or argument	Description
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 14-4 describes each element of the syntax. None of the keywords are case sensitive.

Table 14-4. Generic call filter syntax elements

Keyword or argument	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**.

Table 14-4. Generic call filter syntax elements (continued)

Keyword or argument	Description
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 cannot exceed 6 bytes (12 hexadecimal digits). A one bit in the mask indicates a bit to compare. A zero bit indicates a bit to ignore. The length of the mask specifies the length of the comparison.
value	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 14-19.

Ascend-Call-Type (177)

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

Usage: Table 14-5 lists the settings you can specify for Ascend-Call-Type.

Table 14-5. 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-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-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 14-6.

Table 14-6. Ascend-Connect-Progress codes

Code	Explanation
0	No progress.
1	Not applicable.
2	The progress of the call is unknown.
10	The call is up.
30	The modem is up.
31	The modem is waiting for DCD.
32	The modem is waiting for result codes.
40	The terminal-server session has started up.
41	The MAX TNT is establishing the TCP connection.
42	The MAX TNT is establishing the immediate Telnet connection.

Table 14-6. Ascend-Connect-Progress codes (continued)

Code	Explanation
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.
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.
60	The LAN session is up.
61	LCP negotiations are allowed.
62	CCP negotiations are allowed.
63	IPNCP negotiations are allowed.
64	Bridging NCP negotiations are allowed.
65	LCP is in the Open state.
66	CCP is in the Open state.
67	IPNCP is in the Open state.
68	Bridging NCP is in the Open state.
69	LCP is in the Initial state.
70	LCP is in the Starting state.
71	LCP is in the Closed state.
72	LCP is in the Stopped state.
73	LCP is in the Closing state.
74	LCP is in the Stopping state.
75	LCP is in the Request Sent state.
76	LCP is in the ACK Received state.
77	LCP is in the ACK Sent state.
80	IPXNCP is in the Open state.
90	V.110 is up.
91	V.110 is in the Open state.
92	V.110 is in the Carrier state.
93	V.110 is in the Reset state.

Table 14-6. Ascend-Connect-Progress codes (continued)

Code	Explanation
94	V.110 is in the Closed state.

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

- The session has ended or has failed authentication (Acct-Status-Type=Stop).
- The Auth-Type parameter is not set to RADIUS-Logout.

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 14-7 describes each element of the syntax. None of the keywords are case sensitive.

Table 14-7. IP data filter syntax elements

Keyword or argument	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`**.

Table 14-7. IP data filter syntax elements (continued)

Keyword or argument	Description
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.
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).

Table 14-7. IP data filter syntax elements (continued)

Keyword or argument	Description
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 14-8 describes each element of the syntax. None of the keywords are case sensitive.

Table 14-8. Generic data filter syntax elements

Keyword or argument	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**.

Table 14-8. Generic data filter syntax elements (continued)

Keyword or argument	Description
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 cannot exceed 6 bytes (12 hexadecimal digits). A one bit in the mask indicates a bit to compare. A zero bit indicates a bit to ignore. The length of the mask specifies the length of the comparison.
value	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 14-12.

Ascend-Data-Rate (197)

Description: Specifies the data rate of 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 both of the following conditions are true:

- The session has ended or has failed authentication (Acct-Status-Type=Stop).
- The Auth-Type parameter is not set to RADIUS-Logout.

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 14-9. The data service you specify must be available end-to-end.

Table 14-9. Ascend-Data-Svc settings

Setting	Description
Switched-Voice-Bearer (0)	Applies only to calls made over an ISDN BRI or T1 PRI line. When you specify this setting, 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.
Switched-64KR (3)	Contains restricted data and connects to the Switched-64 data service.

Table 14-9. Ascend-Data-Svc settings (continued)

Setting	Description
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.

Table 14-9. Ascend-Data-Svc settings (continued)

Setting	Description
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.
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.

Table 14-9. Ascend-Data-Svc settings (continued)

Setting	Description
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-inherited (37)	Applies to calls placed by a device connected to a local ISDN BRI line from a Host/BRI module. The call connects with the data service as requested by the caller on the local ISDN BRI line.
Switched-restricted-bearer-x30 (38)	Specifies the 56-Kbps X.30 switched data service available from DPNSS and DASS 2 switches.
Switched-clear-bearer-v110 (39)	Specifies the 64-Kbps V.110 switched data service available from DPNSS and DASS 2 switches.
Switched-restricted-64-x30 (40)	Specifies the 64-Kbps X.30 switched data service available from DPNSS and DASS 2 switches. For most DASS 2 and DPNSS installations, select Switched-restricted-64-x30.
Switched-clear-56-v110 (41)	Specifies the 56-Kbps V.110 switched data service available from DPNSS and DASS 2 switches.
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, MP+, and X.25/PAD 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: "Configuring DBA in RADIUS" on page 5-25,
"Ascend-Add-Seconds (240)" on page 14-5,
"Ascend-Base-Channel-Count (172)" on page 14-8,
"Ascend-Dec-Channel-Count (237)" on page 14-27,
"Ascend-History-Weigh-Type (239)" on page 14-42,
"Ascend-Inc-Channel-Count (236)" on page 14-45,
"Ascend-Maximum-Channels (235)" on page 14-50,
"Ascend-Minimum-Channels (173)" on page 14-54,
"Ascend-Remove-Seconds (241)" on page 14-65,
"Ascend-Seconds-Of-History (238)" on page 14-68, and
"Ascend-Target-Util (234)" on page 14-71.

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 between 1 and 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: "Configuring DBA in RADIUS" on page 5-25,
"Ascend-Add-Seconds (240)" on page 14-5,
"Ascend-Base-Channel-Count (172)" on page 14-8,
"Ascend-DBA-Monitor (171)" on page 14-27,
"Ascend-History-Weigh-Type (239)" on page 14-42,
"Ascend-Inc-Channel-Count (236)" on page 14-45,
"Ascend-Maximum-Channels (235)" on page 14-50,

"Ascend-Minimum-Channels (173)" on page 14-54,
"Ascend-Remove-Seconds (241)" on page 14-65,
"Ascend-Seconds-Of-History (238)" on page 14-68, and
"Ascend-Target-Util (234)" on page 14-71.

Ascend-DHCP-Maximum-Leases (134)

Description: Specifies the maximum number of dynamic addresses the MAX TNT can assign to Network Address Translation (NAT) for LAN clients.

Usage: Specify a value between 1 and 254. The default value is 4.

See Also: "Setting up Network Address Translation (NAT) for LAN" on page 9-29,
"Ascend-DHCP-Pool-Number (148)" on page 14-28, and
"Ascend-DHCP-Reply (147)" on page 14-29.

Ascend-DHCP-Pool-Number (148)

Description: Specifies the address pool from which the MAX TNT assigns a dynamic IP address to the Dynamic Host Configuration Protocol (DHCP) client specified by the user profile.

Usage: Specify an integer between 1 and the number of address pools you define. The default value is 0 (zero), which specifies that the MAX TNT uses the first defined IP address pool.

Dependencies: When the DHCP client requests an address, the MAX TNT allocates an IP address from one of its IP address pools and assigns it to the client for 30 minutes. The client must renew the IP address assignment before the 30-minute period expires. The MAX TNT uses its local memory to keep track of all IP addresses it has assigned. Therefore, it loses the entries for current, unexpired IP address assignments when you reset it.

A client can hold an unexpired IP address assignment when you reset the MAX TNT. After the reset, the MAX TNT might assign that address to a new client. The duplicate IP addresses cause network problems until the first assignment expires or one of the two clients reboots.

See Also: "Setting up a DHCP connection" on page 9-27,
"Ascend-DHCP-Maximum-Leases (134)" on page 14-28, and
"Ascend-DHCP-Reply (147)" on page 14-29.

Ascend-DHCP-Reply (147)

Description: Specifies whether the MAX TNT processes DHCP packets and acts as a DHCP server.

Usage: Specify one of the following settings:

- DHCP-Reply-Yes specifies that the MAX TNT processes DHCP packets. For a bridged connection, the MAX TNT responds to all DHCP requests. For a non-bridged connection, the MAX TNT responds only to Network Address Translation (NAT) for LAN DHCP packets.
- DHCP-Reply-No specifies that the MAX TNT does not process DHCP packets, but routes or bridges DHCP packets as any other packet. DHCP-Reply-No is the default.

See Also: "Setting up a DHCP connection" on page 9-27,
"Setting up Network Address Translation (NAT) for LAN" on page 9-29,
"Ascend-DHCP-Maximum-Leases (134)" on page 14-28, and
"Ascend-DHCP-Pool-Number (148)" on page 14-28.

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.

See Also: "Controlling access to digital modems" on page 6-12.

Ascend-Dial-Number (227)

Description: Specifies the phone number the MAX TNT dials to reach the bridge, 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 14-10.

Table 14-10.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, or between Terminal Equipment (TEs) on a local ISDN BRI line. The call type is port-to-port in the former case, TE-to-TE in the latter. In a port-to-port call, the second digit specifies the slot of a Dual/Host or Host/6 card. In a TE-to-TE call, the second digit specifies the slot of a Host/BRI module. If you enter 0 (zero) for the second digit, the call connects to any available AIM port and ignores the third digit. If you enter a non-zero value for the second digit, the third digit selects the AIM port (for a port-to-port call) or a local ISDN BRI port (for a TE-to-TE call). If you enter 0 (zero) for the third digit, the call connects to any available AIM port or local ISDN BRI line in the module selected by the second digit.

Ascend-Disconnect-Cause (195)

Description: Indicates the reason a connection went offline.

Usage: Ascend-Disconnect-Cause can return any of the values listed in Table 14-11.

Table 14-11.Ascend-Disconnect-Cause codes

Code	Description
0	No reason.
1	The event was not a disconnect.
2	The reason for the disconnect is unknown. The code can appear when the remote connection goes down.
3	The call has disconnected.
4	CLID authentication has failed.
The following codes can appear if a disconnect occurs during the initial modem connection.	
10	The modem never detected DCD.

Table 14-11.Ascend-Disconnect-Cause codes (continued)

Code	Description
11	The modem detected DCD, but became inactive.
12	The result codes could not be parsed.
The following codes are related to immediate Telnet and raw TCP disconnects during a terminal-server session.	
20	The user exited normally from the terminal server.
21	The user exited from the terminal server because the idle timer expired.
22	The user exited normally from a Telnet session.
23	The user could not switch to SLIP or PPP because the remote host had no IP address or because the dynamic pool could not assign one.
24	The user exited normally from a raw TCP session.
25	The login process ended because the user failed to enter a correct password after three attempts.
26	The raw TCP option is not enabled.
27	The login process ended because the user typed Ctrl-C.
28	The terminal-server session has ended.
29	The user closed the virtual connection
30	The virtual connection has ended.
31	The user exited normally from an Rlogin session
32	The user selected an invalid Rlogin option.
33	The MAX TNT has insufficient resources for the terminal-server session.
The following codes concern PPP connections.	
40	PPP LCP negotiation timed out while waiting for a response from a peer.
41	There was a failure to converge on PPP LCP negotiations.
42	PPP PAP authentication failed.
43	PPP CHAP authentication failed.
44	Authentication failed from the remote server.
45	The peer sent a PPP Terminate Request.
46	LCP got a close request from the upper layer while LCP was in an open state.

Table 14-11.Ascend-Disconnect-Cause codes (continued)

Code	Description
47	LCP closed because no NCPs were open.
48	LCP closed because it could not determine to which MP bundle it should add the user.
49	LCP closed because the MAX TNT could not add any more channels to an MP session.
The following codes are related to immediate Telnet and raw TCP disconnects, and contain more specific information that the Telnet and TCP codes listed earlier in this table.	
50	The Raw TCP or Telnet internal session tables are full.
51	Internal resources are full.
52	The IP address for the Telnet host is invalid.
53	The MAX TNT could not resolve the hostname.
54	The MAX TNT detected a bad or missing port number.
The TCP stack can return the following disconnect codes during an immediate Telnet or raw TCP session.	
60	The host reset the TCP connection.
61	The host refused the TCP connection.
62	The TCP connection timed out.
63	A foreign host closed the TCP connection.
64	The TCP network was unreachable.
65	The TCP host was unreachable.
66	The TCP network was administratively unreachable.
67	The TCP host was administratively unreachable.
68	The TCP port was unreachable.
The following are additional disconnect codes.	
100	The session timed out because there was no activity on a PPP link.
101	The session failed for security reasons.
102	The session ended for callback.
120	One end refused the call because the protocol was disabled or unsupported.
150	RADIUS requested the disconnect.
160	The allowed retries for V.110 synchronization have been exceeded.

Table 14-11.Ascend-Disconnect-Cause codes (continued)

Code	Description
170	PPP authentication has timed out.
180	The call disconnected as the result of a local hangup.
185	The call disconnected because the remote end hung up.
190	The call disconnected because the T1 line that carried it was quiesced.
195	The call disconnected because the call duration exceeded the maximum amount of time allowed by Ascend-Maximum-Call-Duration attribute.

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

- The session has ended or has failed authentication (Acct-Status-Type=Stop).
- The Auth-Type parameter is not set to RADIUS-Logout.

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) when Auth-Type=RADIUS-Logout. 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 14-56 and
“NAS-Identifier (4)” on page 14-86.

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 14-11.

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 all of the following conditions are true:

- The session has been authenticated.
- The session has ended (Acct-Status-Type=Stop).
- The Auth-Type parameter is not set to RADIUS-Logout.

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. A circuit specification defines two DLCI endpoints of a PVC, with one endpoint specified in each RADIUS user profile or Connection profile.

Usage: Specify a text string 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.

See Also: "Configuring a Frame Relay circuit connection" on page 7-15.

Ascend-FR-DCE-N392 (162)

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

Usage: Specify an integer between 1 and 10. The default value is 3.

Dependencies: 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 14-35 and "Ascend-FR-Type (159)" on page 14-40.

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 between 1 and 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 14-40.

Ascend-FR-Direct (219)

Description: Specifies whether the MAX TNT uses a redirect connection for Frame Relay packets.

Usage: Specify one of the following values:

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

See Also: "Redirect connections (rarely used)" on page 7-12,
"Configuring a Frame Relay redirect connection" on page 7-15,
"Ascend-FR-Direct-DLCI (221)" on page 14-36, and
"Ascend-FR-DLCI (179)" on page 14-37.

Ascend-FR-Direct-DLCI (221)

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

Usage: Specify an integer between 16 and 991. The default value is 16. Many redirect connections can use the same DLCI.

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

See Also: "Redirect connections (rarely used)" on page 7-12,
"Configuring a Frame Relay redirect connection" on page 7-15,
"Ascend-FR-Direct (219)" on page 14-36, and
"Ascend-FR-Direct-Profile (220)" on page 14-36.

Ascend-FR-Direct-Profile (220)

Description: Specifies the name of the Frame Relay profile that carries the redirect connection.

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 alphanumeric characters. The default value is null.

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

See Also: "Redirect connections (rarely used)" on page 7-12,
"Configuring a Frame Relay redirect connection" on page 7-15,
"Ascend-FR-Direct (219)" on page 14-36, and
"Ascend-FR-Direct-DLCI (221)" on page 14-36.

Ascend-FR-DLCI (179)

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

Usage: Specify an integer between 16 and 991. The default value is 16. You must assign each gateway connection its own DLCI.

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

See Also: "Gateway connections" on page 7-11,
"Configuring a Frame Relay gateway connection" on page 7-14,
"Ascend-FR-Direct (219)" on page 14-36, and
"Ascend-FR-Profile-Name (180)" on page 14-39.

Ascend-FR-DTE-N392 (163)

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

Usage: Specify an integer between 1 and 10. The default value is 3.

Dependencies: 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 14-37 and
"Ascend-FR-Type (159)" on page 14-40.

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 between 1 and 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 14-40.

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.

See Also: "Setting up the logical link to a Frame Relay switch" on page 7-3.

Ascend-FR-LinkUp (157)

Description: Specifies whether the Frame Relay link comes up automatically.

Usage: Specify one of the following values:

- Ascend-LinkUp-Default (0) specifies that the datalink does not come up unless a DLCI brings it up, and shuts down after the last DLCI has been removed. This value is the default.
- Ascend-LinkUp-AlwaysUp (1) specifies that the datalink comes up automatically and stays up even when the last DLCI has been removed.

See Also: "Setting up the logical link to a Frame Relay switch" on page 7-3.

Ascend-FR-N391 (161)

Description: Specifies the interval, in seconds, at which the MAX TNT requests a Full Status Report.

If you configure a Frame Relay connection for link management, it regularly requests updates on the status of the link. If the Frame Relay unit at the other end of the link does not respond to the requests, or if the response indicates a DLCI failure, the MAX TNT considers the link inactive.

Usage: Specify an integer between 1 and 255. The default value is 6.

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

See Also: "Ascend-FR-Type (159)" on page 14-40.

Ascend-FR-Nailed-Grp (158)

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

Usage: Specify a number between 1 and the maximum number of nailed-up channels that your MAX TNT allows. The default value is 1.

Dependencies: Do not associate a group with more than one active Frame Relay profile.

See Also: “Setting up Frame Relay user connections” on page 7-11.

Ascend-FR-Profile-Name (180)

Description: Specifies the name of the Frame Relay profile that carries the gateway connection.

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 alphanumeric characters. The default value is null.

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

See Also: “Gateway connections” on page 7-11,
“Configuring a Frame Relay gateway connection” on page 7-14,
“Ascend-FR-Direct (219)” on page 14-36, and
“Ascend-FR-DLCI (179)” on page 14-37.

Ascend-FR-T391 (166)

Description: Specifies the Link Integrity Verification polling timer.

Usage: Specify a number of seconds between 5 and 30. The default value is 10.

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

See Also: “Ascend-FR-Type (159)” on page 14-40.

Ascend-FR-T392 (167)

Description: Sets up the timer for the verification of the polling cycle (the length of time the MAX TNT should wait between Status Enquiry messages). The MAX TNT records an error if it does not receive a Status Enquiry within the number of seconds you specify.

Usage: Specify a number of seconds between 5 and 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 14-40.

Ascend-FR-Type (159)

Description: Specifies the type of Frame Relay connection that the Frame Relay profile uses.

Usage: Specify one of the following values:

- Ascend-FR-DTE (0) specifies a UNI-DTE interface (the default). When you specify this value, the MAX TNT acts as a DTE that can connect to a Frame Relay switch.
- Ascend-FR-DCE (1) specifies a UNI-DCE interface. When you specify this value, the MAX TNT acts as a DCE that can connect to a Frame Relay DTE unit.
- Ascend-FR-NNI (2) specifies an NNI interface. When you specify this value, the MAX TNT can connect to another NNI unit (a Frame Relay switch).

See Also: "Types of logical links between the MAX TNT and a Frame Relay switch" on page 7-3.

Ascend-FT1-Caller (175)

Description: Specifies whether the MAX TNT initiates an FT1-AIM or 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. By the same token, 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 between 1 and 60 for Ascend-Group. The default value is 1.
- If you set Ascend-Call-Type=Nailed/Mpp, you can use the Ascend-Group attribute to assign multiple nailed-up groups to the profile. Specify a single number, or specify a list of numbers between 1 and 60, separated by commas, with no spaces. The default value is 1.

Dependencies: Consider the following:

- The Ascend-Group attribute does not apply if the link consists entirely of switched channels.
- If you add channels for the Ascend-Group attribute, the MAX TNT adds the channels to any online connection that uses the group.
- Do not duplicate group numbers in active profiles (that is, choose a value for Ascend-Group that no other profile is using).
- Although you can assign multiple groups to a user profile, do not mix the Serial WAN circuit with nailed-up BRI or T1/E1 channels.

Example: If 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-Handle-IPX (222)

Description: Specifies how the MAX TNT handles NCP watchdog requests on behalf of IPX clients during IPX bridging.

Usage: Specify one of the following values:

- Handle-IPX-None (0) specifies that special IPX behavior does not take place. Handle-IPX-None is the default.
- Handle-IPX-Client (1) specifies that the MAX TNT discards Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) periodic broadcasts at its WAN interface, but forwards RIP and SAP queries.
- Handle-IPX-Server (2) specifies that the MAX TNT discards all Routing Information Protocol (RIP) and Service Advertising Protocol (SAP) periodic broadcasts and queries at its WAN interface. This mode enables the MAX TNT to bring down calls during idle periods without breaking client/server or peer-to-peer connections.

Dependencies: Consider the following:

- If you specify Ascend-Handle-IPX=Handle-IPX-Server, you must also specify a value for the Ascend-Netware-timeout attribute, indicating the maximum length of idle time during which the MAX TNT performs watchdog spoofing for NetWare connections.
- If the connection does not bridge (Ascend-Bridge=Bridge-No), the Ascend-Handle-IPX attribute does not apply.
- Although Ascend-Handle-IPX does not apply if Ascend-Bridge=Bridge-No, the MAX TNT automatically performs watchdog spoofing just as though you had set Ascend-Handle-IPX=Handle-IPX-Server. However, the MAX TNT does not filter as though you had set Ascend-Handle-IPX=Handle-IPX-Server.

See Also: "Overview of special IPX bridging requirements" on page 11-5 and "Ascend-Netware-timeout (223)" on page 14-56.

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: "Configuring DBA in RADIUS" on page 5-25,
"Ascend-Add-Seconds (240)" on page 14-5,
"Ascend-Base-Channel-Count (172)" on page 14-8,
"Ascend-DBA-Monitor (171)" on page 14-27,
"Ascend-Dec-Channel-Count (237)" on page 14-27,
"Ascend-Inc-Channel-Count (236)" on page 14-45,
"Ascend-Maximum-Channels (235)" on page 14-50,
"Ascend-Minimum-Channels (173)" on page 14-54,
"Ascend-Remove-Seconds (241)" on page 14-65,
"Ascend-Seconds-Of-History (238)" on page 14-68, and
"Ascend-Target-Util (234)" on page 14-71.

Ascend-Home-Agent-Password (184)

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 nodes 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.

See Also: "Setting up an ATMP tunnel for an IP or IPX network" on page 8-6.

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 between 0 and 65535. The default value is 5150.

Dependencies: If you specify a value for the ***udp_port*** argument of Ascend-Primary-Home-Agent or Ascend-Secondary-Home-Agent, or if you accept the default of 5150 for ***udp_port***, you need not specify the Ascend-Home-Agent-UDP-Port attribute.

See Also: "Setting up an ATMP tunnel for an IP or IPX network" on page 8-6, "Ascend-Primary-Home-Agent (129)" on page 14-61, and "Ascend-Secondary-Home-Agent (130)" on page 14-67.

Ascend-Home-Network-Name (185)

Description: Specifies the name of the Connection profile on which the home agent sends all packets it receives from the mobile node during Ascend Tunnel Management Protocol (ATMP) operation.

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.

See Also: "Setting up an ATMP tunnel for an IP or IPX network" on page 8-6.

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 make 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: The following pseudo-user profile sets up a host list for a MAX TNT named Cal:

```
initial-banner-Cal Password="ascend", User-Service=Dialout-Framed-User
     Reply-Message="Up to 16 lines of up to 80 characters each",
     Reply-Message="will be accepted. ",
     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 14-88.

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 between 0 and 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: Consider the following:

- 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 in preference to it.
- The Ascend-Idle-Limit attribute does not apply to nailed-up links.

See Also: “Configuring a time limit and idle connection attributes” on page 5-26,
“Ascend-MPP-Idle-Percent (254)” on page 14-54, and
“Ascend-Preempt-Limit (245)” on page 14-59.

Ascend-IF-Addr

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: “Setting up an interface-based IP routing connection” on page 9-23,
“Ascend-IF-Netmask (154)” on page 14-45, and
“Ascend-Remote-Addr (155)” on page 14-65.

Ascend-IF-Netmask (154)

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

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

See Also: "Setting up an interface-based IP routing connection" on page 9-23,
"Ascend-IF-Addr" on page 14-44, and
"Ascend-Remote-Addr (155)" on page 14-65.

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 between 1 and 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 cannot exceed the maximum number of channels available.

See Also: "Configuring DBA in RADIUS" on page 5-25,
"Ascend-Add-Seconds (240)" on page 14-5,
"Ascend-Base-Channel-Count (172)" on page 14-8,
"Ascend-DBA-Monitor (171)" on page 14-27,
"Ascend-Dec-Channel-Count (237)" on page 14-27,
"Ascend-History-Weigh-Type (239)" on page 14-42,
"Ascend-Maximum-Channels (235)" on page 14-50,
"Ascend-Minimum-Channels (173)" on page 14-54,
"Ascend-Remove-Seconds (241)" on page 14-65,
"Ascend-Seconds-Of-History (238)" on page 14-68, and
"Ascend-Target-Util (234)" on page 14-71.

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 and bridging 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, bridging is not enabled, 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: The following user profile specifies that the MAX TNT redirects incoming packets to the host at IP address 10.2.3.11:

```
Emma Password="m2dan", User-Service=Framed-User
     Framed-Protocol=PPP,
     Framed-Address=10.8.9.10,
     Framed-Netmask=255.255.252.0,
     Ascend-Route-IP=Route-IP-Yes,
     Ascend-Bridge=Bridge-No,
     Ascend-IP-Direct=10.2.3.11,
     Ascend-Metric=2,
     Framed-Routing=None,
     ...
```

See Also: "Setting up IP redirection" on page 9-15 and "Framed-Routing (10)" on page 14-84.

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*"

Table 14-12 describes each Ascend-IP-Pool-Definition argument.

Table 14-12.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.
max_entries	Maximum number of IP addresses in the pool. The MAX TNT assign addresses sequentially, from ***first_ipaddr*** on, up to the limit of addresses specified by ***max_entries***. The default value is 0 (zero).

Example: In the following example, the pseudo-user profile creates 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: “Configuring IP address pools for a single MAX TNT” on page 9-11 and “Ascend-Assign-IP-Pool (218)” on page 14-6.

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: "Setting up IPX routing in a user profile" on page 10-4,
"Ascend-IPX-Peer-Mode (216)" on page 14-48,
"Ascend-IPX-Route (174)" on page 14-49, and
"Ascend-Route-IPX (229)" on page 14-67.

Ascend-IPX-Node-Addr (182)

Description: Specifies a unique IPX node address on the network specified by Framed-IPX-Network. The node address completes the IPX address of a mobile node for Ascend Tunnel Management Protocol (ATMP) operation.

Usage: Specify a 12-digit ASCII string enclosed in double-quotes. The RADIUS server passes the attributes in the mobile node's profile to the foreign agent. The foreign agent sends the attributes when connecting with the home agent.

See Also: "Setting up an ATMP tunnel for an IP or IPX network" on page 8-6 and
"Framed-IPX-Network (23)" on page 14-79

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 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 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: "Setting up IPX routing in a user profile" on page 10-4,
"Ascend-IPX-Route (174)" on page 14-49, and
"Ascend-Route-IPX (229)" on page 14-67.

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 14-13 describes each Ascend-IPX-Route argument.

Table 14-13.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.)
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: The following pseudo-user profile defines an IPX route:

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

See Also: "Setting up IPX routing in a user profile" on page 10-4,
"Ascend-IPX-Alias (224)" on page 14-48,
"Ascend-IPX-Peer-Mode (216)" on page 14-48, and
"Ascend-Route-IPX (229)" on page 14-67.

Ascend-Link-Compression (233)

Description: Turns data compression on or off for a PPP, MP, or MP+ link.

Usage: Specify one of the following values:

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

Dependencies: To turn on data compression, each side of the link must set the Ascend-Link-Compression attribute (in RADIUS) or the Link-Compression parameter (on the MAX TNT).

See Also: "Framed-Compression (13)" on page 14-79.

Ascend-Maximum-Call-Duration (125)

Description: Specifies the maximum number of minutes an incoming call can remain connected.

Usage: Specify an integer between 0 and 1440. The MAX TNT checks the connection once per minute, so the actual time the call is connected is slightly longer than the time you set. The default value is 0 (zero), which specifies that the MAX TNT does not set a limit on the duration of an incoming call.

See Also: "Configuring a time limit and idle connection attributes" on page 5-26.

Ascend-Maximum-Channels (235)

Description: Specifies the maximum number of channels the MAX TNT allows on an MP+ call.

Usage: Specify an integer between 1 and the maximum number of channels your system supports. The default value is 1.

Dependencies: 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: "Configuring DBA in RADIUS" on page 5-25,
"Ascend-Add-Seconds (240)" on page 14-5,
"Ascend-Base-Channel-Count (172)" on page 14-8,
"Ascend-DBA-Monitor (171)" on page 14-27,
"Ascend-Dec-Channel-Count (237)" on page 14-27,
"Ascend-History-Weigh-Type (239)" on page 14-42,
"Ascend-Inc-Channel-Count (236)" on page 14-45,
"Ascend-Minimum-Channels (173)" on page 14-54,
"Ascend-Remove-Seconds (241)" on page 14-65,
"Ascend-Seconds-Of-History (238)" on page 14-68, and
"Ascend-Target-Util (234)" on page 14-71.

Ascend-Maximum-Time (194)

Description: Specifies the maximum length of time in seconds that any session can remain online. Once a session reaches the time limit, its connection goes offline.

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

See Also: "Configuring a time limit and idle connection attributes" on page 5-26.

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 menu items display 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 14-14 lists each argument. If any entry consists of an option containing more that the maximum number of characters allowed, the RADIUS server discards the entry.

Table 14-14.Ascend-Menu-Item arguments

Argument	Description
command	Specifies the string sent to the terminal server when the user selects the menu item. The ***command*** specification must be in a format that the Ascend terminal server understands. It can contain up to 80 characters.
text	Specifies the text that displays to the user. The maximum length for ***text*** is 31 characters.
match	Specifies the pattern the user must type to select the item. The maximum length for ***match*** is 10 characters. 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: "Setting up a custom menu and an input prompt" on page 6-7 and "Ascend-Menu-Selector (205)" on page 14-53.

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: "Setting up a custom menu and an input prompt" on page 6-7 and "Ascend-Menu-Item (206)" on page 14-51.

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 between 1 and 15. The default value is 7.

Dependencies: Consider the following:

- The Ascend-Metric attribute does not apply to bridged connections.
- 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 14-66 and
"Framed-Route (22)" on page 14-82.

Ascend-Minimum-Channels (173)

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

Usage: Specify a number between 1 and 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: "Configuring DBA in RADIUS" on page 5-25,
"Ascend-Add-Seconds (240)" on page 14-5,
"Ascend-Base-Channel-Count (172)" on page 14-8,
"Ascend-DBA-Monitor (171)" on page 14-27,
"Ascend-Dec-Channel-Count (237)" on page 14-27,
"Ascend-History-Weigh-Type (239)" on page 14-42,
"Ascend-Inc-Channel-Count (236)" on page 14-45,
"Ascend-Maximum-Channels (235)" on page 14-50,
"Ascend-Remove-Seconds (241)" on page 14-65,
"Ascend-Seconds-Of-History (238)" on page 14-68, and
"Ascend-Target-Util (234)" on page 14-71.

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 an integer between 0 and 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 in preference to it.

See Also: "Configuring a time limit and idle connection attributes" on page 5-26, "Ascend-Idle-Limit (244)" on page 14-44, and "Ascend-Preempt-Limit (245)" on page 14-59.

Ascend-Multicast-Client (152)

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 (153)" on page 14-55.

Ascend-Multicast-Rate-Limit (153)

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 (152)" on page 14-55.

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 all of the following conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).
- The Auth-Type parameter is not set to RADIUS-Logout

See Also: "Ascend-Num-In-Multilink (188)" on page 14-57.

Ascend-Netware-timeout (223)

Description: Specifies how long, in minutes, the MAX TNT responds to NCP watchdog requests on behalf of IPX clients on the other side of an offline IPX bridging connection. Responding to watchdog requests on behalf of clients is commonly called *watchdog spoofing*.

Usage: Specify an integer between 0 and 65535. The default value is 0 (zero), which allows the MAX TNT to respond to watchdog requests without a time limit.

The timer begins counting down as soon as the WAN bridging link goes offline. At the end of the selected time, the MAX TNT releases the client-server connections. If the WAN session reconnects, the MAX TNT cancels the timeout.

Dependencies: Ascend-Netware-timeout applies to IPX bridging connections when the MAX TNT is on the server LAN and not on the client LAN (that is, when Ascend-Handle-IPX= Handle-IPX-Server).

See Also: "Setting up bridging for a WAN connection" on page 11-4 and "Ascend-Handle-IPX (222)" on page 14-41.

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 14-33 and "Class (25)" on page 14-78.

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 all of the following conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).
- The Auth-Type parameter is not set to RADIUS-Logout.

See Also: "Ascend-Multilink-ID (187)" on page 14-56.

Ascend-PPP-Address (253)

Description: Specifies the MAX TNT unit's IP address as reported to the calling unit during PPP IPCP negotiations.

Usage: Specify an IP address in dotted decimal notation. The default value is 0.0.0.0, which specifies that IPCP negotiates with the value of the IP-Address parameter in the IP-Interface profile on the MAX TNT.

If you specify a valid IP address, IPCP negotiates with that IP address. If you specify 255.255.255.255, IPCP negotiates with the address 0.0.0.0.

Dependencies: You can assign Ascend-PPP-Address a value different from the MAX TNT unit's true IP address, as long as the user requesting access is aware of the discrepancy.

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 hex 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 14-79.

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 an integer between 0 and 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: "Configuring a time limit and idle connection attributes" on page 5-26, "Ascend-Idle-Limit (244)" on page 14-44, and "Ascend-MPP-Idle-Percent (254)" on page 14-54.

Ascend-Pre-Input-Octets (190)

Description: Reports the number of octets received before authentication.

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 session has ended (Acct-Status-Type=Stop).
- The Auth-Type parameter is not set to RADIUS-Logout.

Ascend-Pre-Input-Packets (192)

Description: Reports the number of packets received before authentication.

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 all of the following conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).
- The Auth-Type parameter is not set to RADIUS-Logout.

Ascend-Pre-Output-Octets (191)

Description: Reports the number of octets transmitted before authentication.

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 session has ended (Acct-Status-Type=Stop).
- The Auth-Type parameter is not set to RADIUS-Logout.

Ascend-Pre-Output-Packets (193)

Description: Reports the number of packets transmitted before authentication.

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 all of the following conditions are true:

- The session was authenticated.
- The session has ended (Acct-Status-Type=Stop).
- The Auth-Type parameter is not set to RADIUS-Logout.

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 both of the following conditions are true:

- The session has ended or has failed authentication (Acct-Status-Type=Stop).
- The Auth-Type parameter is not set to RADIUS-Logout.

Ascend-Primary-Home-Agent (129)

Description: Specifies the first home agent the foreign agent tries to reach when setting up an Ascend Tunnel Management Protocol (ATMP) tunnel, and the UDP port the foreign agent uses for the link.

The RADIUS server passes the attributes in the mobile node's RADIUS user profile to the foreign agent. The foreign agent sends the attributes when connecting with the home agent.

Usage: Specify the primary home agent in the following format:

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

Table 14-15 lists each element of the syntax.

Table 14-15.Ascend-Primary-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 hostname or an IP address, but not both.
`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 Ascend-Primary-Home-Agent attribute, you need not specify a value for ***`udp_port`***.
- If you specify a value for the ***`udp_port`*** argument of Ascend-Primary-Home-Agent, or if you accept the default of 5150, you need not specify the Ascend-Home-Agent-UDP-Port attribute.
- Use Ascend-Primary-Home-Agent 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:

```
Ascend-Primary-Home-Agent="max1.home.com:6001"
```

```
Ascend-Primary-Home-Agent="10.0.0.1:6001"
```

The following RADIUS profile authenticates a mobile NetWare client that connects directly to the home agent. The home agent is in gateway mode. It forwards packets from the mobile node across a nailed-up WAN link to the home IPX network.

```
Mobile-IPX Password="unit"
        User-Service=Framed-User,
        Ascend-Route-IPX=Route-IPX-Yes,
        Framed-Protocol=PPP,
        Ascend-IPX-Peer-Mode=IPX-Peer-Dialin,
        Framed-IPX-Network=40000000,
        Ascend-IPX-Node-Addr=12345678,
        Ascend-Primary-Home-Agent="max1.home.com:6001",
        Ascend-Secondary-Home-Agent="max2.home.com:6001",
        Ascend-Home-Network-Name="Dave's MAX TNT",
        Ascend-Home-Agent-Password="Pipeline"
```

See Also: "Setting up an ATMP tunnel for an IP or IPX network" on page 8-6, "Ascend-Home-Agent-Password (184)" on page 14-42, "Ascend-Home-Agent-UDP-Port (186)" on page 14-43, "Ascend-Home-Network-Name (185)" on page 14-43, and "Ascend-Secondary-Home-Agent (130)" on page 14-67.

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 14-16.

Table 14-16.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-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 14-17 lists each argument.

Table 14-17.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 starting with the number 19.

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", User-Service=Login-User, Ascend-PW-Expira-
tion="January 1, 1997"
...
```

See Also: "Configuring password expiration" on page 4-7 and "Ascend-PW-Lifetime (208)" on page 14-64.

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", User-Service=Login-User, Ascend-PW-Expira-
tion="Jan 1, 1997"
     Ascend-PW-Lifetime=30
```

See Also: "Configuring password expiration" on page 4-7 and "Ascend-PW-Expiration (21)" on page 14-63.

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 necessary 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"
```

See Also: "Configuring CACHE-TOKEN authentication" on page 4-37 and "Configuring PAP-TOKEN-CHAP authentication" on page 4-39.

Ascend-Remote-Addr (155)

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: "Setting up an interface-based IP routing connection" on page 9-23,
"Ascend-IF-Addr" on page 14-44,
"Ascend-IF-Netmask (154)" on page 14-45, and
"Ascend-Route-IP (228)" on page 14-66.

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 between 1 and 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: "Configuring DBA in RADIUS" on page 5-25,
"Ascend-Add-Seconds (240)" on page 14-5,
"Ascend-Base-Channel-Count (172)" on page 14-8,
"Ascend-DBA-Monitor (171)" on page 14-27,
"Ascend-Dec-Channel-Count (237)" on page 14-27,
"Ascend-History-Weigh-Type (239)" on page 14-42,
"Ascend-Inc-Channel-Count (236)" on page 14-45,
"Ascend-Maximum-Channels (235)" on page 14-50,
"Ascend-Minimum-Channels (173)" on page 14-54,

"Ascend-Seconds-Of-History (238)" on page 14-68, and
"Ascend-Target-Util (234)" on page 14-71.

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",
        ...
```

See Also: "External authentication after CLID authentication" on page 4-25, "PAP, CHAP, or MS-CHAP after CLID authentication" on page 4-26, and "External authentication after called-number authentication" on page 4-32.

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: "Enabling IP routing" on page 9-6 and "Framed-Route (22)" on page 14-82.

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: "Setting up IPX routing in a user profile" on page 10-4,
"Ascend-IPX-Alias (224)" on page 14-48,
"Ascend-IPX-Peer-Mode (216)" on page 14-48, and
"Ascend-IPX-Route (174)" on page 14-49.

Ascend-Secondary-Home-Agent (130)

Description: Specifies the secondary home agent the foreign agent tries to reach when the primary home agent (Ascend-Primary-Home-Agent) is unavailable, and 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 14-18 lists each element of the syntax.

Table 14-18.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 hostname or an IP address, but not both.
`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:

```
Ascend-Primary-Home-Agent="max1.home.com:6001"
```

```
Ascend-Secondary-Home-Agent="max2.home.com:6002"
```

The foreign agent first tries max1.home.com on UDP port 6001. If the name cannot be resolved, or if max1.home.com does not respond, the foreign agent then tries max2.home.com on UDP port 6002.

See Also: "Setting up an ATMP tunnel for an IP or IPX network" on page 8-6,
"Ascend-Home-Agent-Password (184)" on page 14-42,
"Ascend-Home-Agent-UDP-Port (186)" on page 14-43,
"Ascend-Home-Network-Name (185)" on page 14-43, and
"Ascend-Primary-Home-Agent (129)" on page 14-61.

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 using the algorithm specified by the Ascend-History-Weigh-Type attribute.

Usage: Specify a number between 1 and 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 may want the MAX TNT to establish a longer historical time period. If, on the other hand, traffic patterns consist of many spikes that are short in duration, you may want to specify a shorter period of time. Doing so assigns less weight to the short spikes.

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 attribute and the Ascend-Remove-Seconds attribute relative to the value of Ascend-Seconds-Of-History, the system becomes less responsive to quick spikes.
- The easiest way to determine the proper values for all the attributes is to observe usage patterns. If the system is not responsive enough, the value of Ascend-Seconds-Of-History is too high.

See Also: "Configuring DBA in RADIUS" on page 5-25,
"Ascend-Add-Seconds (240)" on page 14-5,
"Ascend-Base-Channel-Count (172)" on page 14-8,
"Ascend-DBA-Monitor (171)" on page 14-27,
"Ascend-Dec-Channel-Count (237)" on page 14-27,
"Ascend-History-Weigh-Type (239)" on page 14-42,

"Ascend-Inc-Channel-Count (236)" on page 14-45,
"Ascend-Maximum-Channels (235)" on page 14-50,
"Ascend-Minimum-Channels (173)" on page 14-54,
"Ascend-Remove-Seconds (241)" on page 14-65, and
"Ascend-Target-Util (234)" on page 14-71.

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.

See Also: "Requesting an access protocol for outgoing calls" on page 4-17,
"Ascend-Send-Passwd (232)" on page 14-69, and
"Ascend-Send-Secret (214)" on page 14-70.

Ascend-Send-Passwd (232)

Description: Specifies the password that the RADIUS server sends to the remote end of a connection on an outgoing call.

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: "Requesting an access protocol for outgoing calls" on page 4-17,
"Ascend-Send-Auth (231)" on page 14-69, and
"Ascend-Send-Secret (214)" on page 14-70.

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: "Requesting an access protocol for outgoing calls" on page 4-17,
"Ascend-Send-Auth (231)" on page 14-69, and
"Ascend-Send-Passwd (232)" on page 14-69.

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.

See Also: "Setting up disconnects" on page 5-31 and
"Setting up filter changes" on page 12-11.

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-Target-Util (234)

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

Usage: Specify an integer between 0 and 100. The default value is 70. When the value is 70%, the device adds bandwidth when it exceeds a 70 percent utilization rate, and subtracts bandwidth when it falls below that number.

Dependencies: 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: "Configuring DBA in RADIUS" on page 5-25,
"Ascend-Add-Seconds (240)" on page 14-5,
"Ascend-Base-Channel-Count (172)" on page 14-8,
"Ascend-DBA-Monitor (171)" on page 14-27,
"Ascend-Dec-Channel-Count (237)" on page 14-27,
"Ascend-History-Weigh-Type (239)" on page 14-42,
"Ascend-Inc-Channel-Count (236)" on page 14-45,
"Ascend-Maximum-Channels (235)" on page 14-50,
"Ascend-Minimum-Channels (173)" on page 14-54,
"Ascend-Remove-Seconds (241)" on page 14-65, and
"Ascend-Seconds-Of-History (238)" on page 14-68.

Ascend-Third-Prompt (213)

Description: Specifies the value you set for the Third-Login-Prompt parameter at the MAX TNT configuration interface.

Usage: The Ascend-Third-Prompt attribute can contain up to 80 characters and does not appear in a user profile. If you enter more than 80 characters for Third-Login-Prompt, the MAX TNT truncates the input to 80. If you do 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 lifetime of the cached token in minutes. 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 sets up CACHE-TOKEN authentication with a 90-minute token cache. Notice that the Ascend-Token-Expiry attribute must appear on the first line of the profile, along with the user name and password.

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

See Also: "Configuring CACHE-TOKEN authentication" on page 4-37, "Ascend-Token-Idle (199)" on page 14-72, and "Ascend-Token-Immediate (200)" on page 14-72.

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 sets up CACHE-TOKEN authentication with a 90-minute token cache and an 80-minute idle limit. Notice that the Ascend-Token-Idle attribute must appear on the first line of the profile.

```
Jim  Password="ACE", Ascend-Token-Expiry=90, Ascend-Token-Idle=80
     Ascend-Receive-Secret="shared secret"
```

See Also: "Configuring CACHE-TOKEN authentication" on page 4-37, "Ascend-Token-Expiry (204)" on page 14-71, and "Ascend-Token-Immediate (200)" on page 14-72.

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: The following user profile specifies that the MAX TNT must send the password it receives from the login user to the ACE server. The user derives the password from a hand-held token card.

```
Connor  Password="ACE", Ascend-Token-Immediate=Tok-Imm-Yes
        Ascend-Receive-Secret="shared-secret",
        User-Service=Login-User,
        ...
```

See Also: “Configuring CACHE-TOKEN authentication” on page 4-37, “Ascend-Token-Expiry (204)” on page 14-71, and “Ascend-Token-Idle (199)” on page 14-72.

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 an ISDN BRI line, T1 access line, or voice interface:

- 288 selects AT&T.
- 222 selects MCI.
- 333 selects Sprint.

The default value is null. If you accept the default, the MAX 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 between 0 and 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 14-74.

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: The following profile specifies that the user must be idle for 90 seconds before the MAX TNT disconnects the session:

```
Default Password="UNIX"
       User-Service=Login-User,
       Ascend-TS-Idle-Limit=90,
       Ascend-TS-Idle-Mode=TS-Idle-Input
```

Dependencies: Ascend-TS-Idle-Mode does not apply if you are using a Frame Relay or raw TCP connection.

See Also: “Ascend-TS-Idle-Limit (169)” on page 14-73.

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 14-75,
"Ascend-User-Acct-Key (141)" on page 14-75,
"Ascend-User-Acct-Port (140)" on page 14-75,
"Ascend-User-Acct-Time (143)" on page 14-76, and
"Ascend-User-Acct-Type (138)" on page 14-76.

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 13-4,
"Ascend-User-Acct-Base (142)" on page 14-74,
"Ascend-User-Acct-Key (141)" on page 14-75,
"Ascend-User-Acct-Port (140)" on page 14-75,
"Ascend-User-Acct-Time (143)" on page 14-76, and
"Ascend-User-Acct-Type (138)" on page 14-76.

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 13-4,
"Ascend-User-Acct-Base (142)" on page 14-74,
"Ascend-User-Acct-Host (139)" on page 14-75,
"Ascend-User-Acct-Port (140)" on page 14-75,
"Ascend-User-Acct-Time (143)" on page 14-76, and
"Ascend-User-Acct-Type (138)" on page 14-76.

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 between 1 and 32767.

See Also: "Setting up accounting on a per-user basis" on page 13-4,
"Ascend-User-Acct-Base (142)" on page 14-74,
"Ascend-User-Acct-Host (139)" on page 14-75,
"Ascend-User-Acct-Key (141)" on page 14-75,
"Ascend-User-Acct-Time (143)" on page 14-76, and
"Ascend-User-Acct-Type (138)" on page 14-76.

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 between 1 and 10. The default value is 0 (zero).

See Also: "Setting up accounting on a per-user basis" on page 13-4,
"Ascend-User-Acct-Base (142)" on page 14-74,
"Ascend-User-Acct-Host (139)" on page 14-75,
"Ascend-User-Acct-Key (141)" on page 14-75,
"Ascend-User-Acct-Port (140)" on page 14-75, and
"Ascend-User-Acct-Type (138)" on page 14-76.

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 13-4,
"Ascend-User-Acct-Base (142)" on page 14-74,
"Ascend-User-Acct-Host (139)" on page 14-75,
"Ascend-User-Acct-Key (141)" on page 14-75,
"Ascend-User-Acct-Port (140)" on page 14-75, and
"Ascend-User-Acct-Time (143)" on page 14-76.

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.

Dependencies: Consider the following:

- If you set CLID-Auth-Mode=CLID-Prefer in the Answer-Defaults profile, the MAX TNT checks the calling party's phone number against the value of the Caller-Id attribute whenever CLID authentication is available. If the MAX TNT finds a match and requires no further identification, it accepts the call.
- If you set CLID-Auth-Mode=CLID-Require in the Answer-Defaults profile, the calling party's phone number must match the value of the Caller-Id attribute before the MAX TNT can answer the call. If CLID is not available, the MAX TNT does not answer the call.

Example: The following user profile sets up CLID authentication with a name, password, and caller ID:

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

See Also: "CLID authentication using a name, password, and caller ID" on page 4-23 and "CLID authentication using a caller ID only" on page 4-24.

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, such as for the purpose of 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 (as long as the Auth-Type parameter is not set to RADIUS-Logout)

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 13-8 and "Ascend-Number-Sessions (202)" on page 14-56.

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 may dial 555-1234, while a long distance caller may dial 1-415-555-1234. In cases such as these, you need only specify the rightmost digits the calls have in common. In this example, you would specify only 1234.

Example: The following user profile sets up called-number authentication in addition to name and password authentication:

```
Clara-p50 Password="ascend", Client-Port-DNIS=1234
     User-Service=Framed-User,
     Framed-Protocol=PPP,
     Framed-Address=200.10.11.12,
     Framed-Netmask=255.255.255.248
```

See Also: "Authentication using a name, password, and called-party number" on page 4-30.

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 14-80.

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.

See Also: "Ascend-Link-Compression (233)" on page 14-50.

Framed-IPX-Network (23)

Description: Specifies a virtual IPX network required for the Ascend Tunnel Management Protocol (ATMP) home agent to route IPX packets to the mobile node. When you specify it in a user profile, the Framed-IPX-Network attribute instructs the answering unit to advertise an additional IPX route.

Usage: Specify the IPX network number of the IPX router at the remote end of the connection. The default value is null.

RADIUS requires that Framed-IPX-Network have a decimal value (base 10), but IPX network numbers generally appear as hexadecimal values (base 16). In order to give Framed-IPX-Network a value, you must convert the hexadecimal IPX network number to decimal format.

See Also: "Setting up an ATMP tunnel for an IP or IPX network" on page 8-6 and "Ascend-IPX-Node-Addr (182)" on page 14-48.

Framed-MTU (12)

Description: Specifies the maximum number of bytes the MAX TNT can receive in a single packet on a PPP, MP, MP+, Frame Relay, EU-UI, or EU-RAW 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 between 1 and 1524 (for a PPP, MP, MP+, EU-UI, or EU-RAW link) or between 128 and 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 14-19).

Table 14-19.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 14-79.

Framed-Protocol (7)

Description: Specifies the type of framed protocol the link can use. When you set this attribute, the link cannot use any other type of framed protocol.

Usage: Table 14-20 lists the values you can specify for Framed-Protocol. By default, the MAX TNT does not limit the protocols a link can access.

Table 14-20.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.
MPP (256)	Does not apply to incoming calls.	Outgoing calls request MP+ framing.
EURAW (257)	A user requesting access can dial in with EU-RAW framing. If the user dials in with any other type of framing, the MAX TNT rejects the call.	Outgoing calls use EU-RAW framing.
EUUI (258)	A user requesting access can dial in with EU-UI framing. If the user dials in with any other type of framing, the MAX TNT rejects the call.	Outgoing calls use EU-UI framing.
FR (261)	Does not apply to incoming calls.	Outgoing calls use Frame Relay (RFC 1490) framing.
FR-CIR (263)	Specifies a Frame Relay circuit.	Specifies a Frame Relay circuit.

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.

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

```
Ascend Password="Pipeline"
       User-Service=Framed-User,
       Framed-Protocol=PPP,
       Framed-Address=10.0.200.225,
       Framed-Netmask=255.255.255.0,
       Ascend-Metric=2,
       Framed-Routing=None,
       Framed-Route="10.0.220.0 10.0.200.225 1",
       Ascend-Idle-Limit=30
       ...
```

See Also: “User-Service (6)” on page 14-90.

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*]"

Table 14-21 describes each Framed-Route argument.

Table 14-21.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.
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.

Example: The following example shows two RADIUS pseudo-user profiles defining global static IP routes:

```
route-1   Password="ascend", User-Service=Dialout-Framed-User
   Framed-Route="10.0.200.33/29 10.0.200.37 1 n lala-gw-out ",
   Framed-Route="10.0.200.50/29 10.0.200.37 1 n lala-gw-out ",
   Framed-Route="10.0.200.47/29 10.0.200.49 1 n nana-gw-out "

route-2   Password="ascend", User-Service=Dialout-Framed-User
   Framed-Route="11.0.200.33/29 11.0.200.37 1 n zzz-gw-out ",
   Framed-Route="12.0.200.47/29 11.0.200.49 1 n kk-gw-out "
```

See Also: "Setting up static IP routes" on page 9-17 and
"Ascend-Route-IP (228)" on page 14-66.

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 may 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: "Requiring that a caller accept an IP address" on page 9-9,
"Setting up static IP routes" on page 9-17, and
"Ascend-Route-IP (228)" on page 14-66.

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.

See Also: "Enabling Telnet, TCP, and Rlogin connections" on page 6-4,
"Login-Service (15)" on page 14-85, and
"User-Service (6)" on page 14-90.

Login-Service (15)

Description: Specifies the type of terminal-server connection a dial-in user makes to 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: "Enabling Telnet, TCP, and Rlogin connections" on page 6-4, "Login-Host (14)" on page 14-85, and "Login-TCP-Port (16)" on page 14-86.

Login-TCP-Port (16)

Description: Specifies the port number to which a TCP session connects when Login-Service=TCP-Clear.

Usage: Specify an integer between 1 and 65535. The default value is 23.

See Also: "Enabling Telnet, TCP, and Rlogin connections" on page 6-4 and "Login-Service (15)" on page 14-85.

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: Specifies the network port on which the MAX TNT receives a call. The MAX TNT sends NAS-Port to the RADIUS server in an Access-Request packet and an Accounting-Request packet.

Usage: On the first line of the user profile, specify the User-Name, Password, and NAS-Port attributes. For NAS-Port, use 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.

You must specify a decimal value for each number. This value must translate to a bit-encoded number that specifies each shelf, slot, line, and channel. The default value for the RADIUS daemon appears in the `/etc/services` file.

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.

Example: To restrict an ISDN user to channel 2 on line 2 for slot 2 and shelf 1, use the NAS-Port setting specified in the first line of the following user profile:

```
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 value NAS-Port=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 14-86.

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.

See Also: "Specifying a password" on page 4-6.

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: Here is an example of a pseudo-user profile setting up message text for a MAX TNT named Cal:

```
initial-banner-Cal Password="ascend", User-Service=Dialout-Framed-User
    Reply-Message="Up to 16 lines of up to 80 characters each",
    Reply-Message="will be accepted. ",
    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 14-43.

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: For example, consider the following first line of a user profile:

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

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

The following profile uses CLID authentication with the incoming phone number as the User-Name:

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

Finally, the following example shows User-Name in a pseudo-user profile for a static route:

```
route-1 Password="ascend", User-Service=Dialout-Framed-User
        Framed-Route="10.4.5.0/22 10.9.8.10 1 n inu-out"
```

See Also: "Setting up name and password authentication" on page 4-5,
"Setting up CLID authentication" on page 4-20,
"Setting up called-number authentication" on page 4-28,
"Setting up an outgoing PPP, MP, or MP+ connection" on page 5-9,
"Setting up the message text and a list of hosts" on page 6-10,
"Setting up the logical link to a Frame Relay switch" on page 7-3,
"Setting up Frame Relay user connections" on page 7-11,
"Defining a pool of addresses for dynamic assignment" on page 9-9,
"Setting up static IP routes" on page 9-17,
"Setting up static IPX routes" on page 10-5, and
"Setting up bridge entries" on page 11-7.

User-Service (6)

Description: Specifies the type of services the link can use.

If RADIUS authenticates an incoming call by means of the User-Name and Password attributes, and the type of call matches the value of the User-Service attribute, the MAX TNT applies the attributes specified in the user profile to the call. If the type of call does not match the User-Service attribute, the MAX TNT rejects the call.

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 V.110 modules, or the call must be X.75 or 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.

Troubleshooting

A

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.

The sections that follow describe each task in detail.

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, you can feel certain that 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 specify an attribute in a profile only when 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 or RADIUS-Logout. 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 A-1 provides a partial list of error messages.

Table A-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.

Table A-1. Log file error messages (continued)

Message	Explanation
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
- V.110 module call status information

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 both of the following conditions are true:

- The session has ended or has failed authentication (Acct-Status-Type=Stop).
- The Auth-Type parameter is not set to RADIUS-Logout.

For information about the values returned for the Ascend-Connect-Progress attribute, see Table 14-6 on page 14-17.

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 both of the following conditions are true:

- The session has ended or has failed authentication (Acct-Status-Type=Stop).
- The Auth-Type parameter is not set to RADIUS-Logout.

For information about the values returned for the Ascend-Disconnect-Cause attribute, see Table 14-11 on page 14-30.

Attribute and Parameter Cross Reference

B

This appendix contains tables that cross reference RADIUS attributes and MAX TNT parameters. The appendix consists of the following sections:

Parameters and analogous attributes

Table B-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 B-1. Parameters and analogous attributes

Profile > Subprofile	Parameter	Analogous attribute
Answer-Defaults	Force-56kbps	Ascend-Force-56
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
	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
	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

Table B-1. Parameters and analogous attributes (continued)

Profile > Subprofile	Parameter	Analogous attribute
	Encapsulation-Protocol= TCP-Raw	Login-Service=TCP-Clear
	Shared-Prof	Ascend-Shared-Profile-Enable
	Station	User-Name
Connection > Bridging-Options	Bridge	Ascend-Bridge
Connection > IP-Options	Address-Pool	Ascend-Assign-IP-Pool
	Client-Default-Gateway	Ascend-Client-Gateway
	IP-Direct	Ascend-IP-Direct
	Local-Address	NAS-Identifier
	Multicast-Allowed	Ascend-Multicast-Client
	Multicast-Rate-Limit	Ascend-Multicast-Rate-Limit
	Netmask-Remote	Framed-Netmask
	Remote-Address	Framed-Address
	RIP	Framed-Routing
	IP-Routing-Enabled	Ascend-Route-IP
	VJ-Header-Prediction	Framed-Compression
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
	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

Table B-1. Parameters and analogous attributes (continued)

Profile > Subprofile	Parameter	Analogous attribute
Connection > PPP-Options	Link-Compression	Ascend-Link-Compression
	MRU	Framed-MTU
	Recv-Password	Password Ascend-Receive-Secret
	Send-Password	Ascend-Send-Passwd Ascend-Send-Secret
Connection > Session-Options	Idle-Timer	Ascend-Idle-Limit
	TS-Idle-Mode	Ascend-TS-Idle-Mode
	TS-Idle-Timer	Ascend-TS-Idle-Limit
Connection > Telco-Options	Billing-Number	Ascend-Billing-Number
	Callback	Ascend-Callback
	Call-By-Call	Ascend-Call-By-Call
	Call-Type	Ascend-Call-Type
	Data-Service	Ascend-Data-Svc
	Expect-Callback	Ascend-Expect-Callback
	Force-56kbps	Ascend-Force-56
	Transit-Number	Ascend-Transit-Number
Connection > UsrRad-Options	Acct-Type	Ascend-User-Acct-Type
	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
External-Auth	Acct-Type	Ascend-User-Acct-Type
External-Auth > Rad-Auth-Client	Acct-Id-Base	Ascend-User-Acct-Base

Table B-1. Parameters and analogous attributes (continued)

Profile > Subprofile	Parameter	Analogous attribute
	Acct-Server-1 Acct-Server-2 Acct-Server-3	Ascend-User-Acct-Host
	Acct-Key	Ascend-User-Acct-Key
	Acct-Port	Ascend-User-Acct-Port
	Acct-Timeout	Ascend-User-Acct-Time
	Auth-Rsp-Required	Ascend-Require-Auth
	Send-Auth-Mode	Ascend-Send-Auth
IP-Interface	IP-Address Netmask	NAS-Identifier
	Multicast-Allowed	Ascend-Multicast-Client
	Multicast-Rate-Limit	Ascend-Multicast-Rate-Limit
IP-Route	IP-Route parameters	Framed-Route
	Metric	Ascend-Metric
T1 > Line-Interface > Channel-Config	Trunk-Group	Ascend-Group
Terminal Server > Immediate-Mode-Options	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

Attributes and parameters in numerical order

Table B-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 B-2. Attributes and analogous parameters in numerical order

Attribute number	Attribute name	Attribute values	Analogous parameter
1	User-Name	Text string	Station
2	Password (User-Password)	Text string	Recv-Password
3	Challenge-Response	Text string	None
4	NAS-Identifier	IP address	IP-Address Netmask Local-Address Netmask-Local
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)	None
7	Framed-Protocol	PPP (1) SLIP (2) MPP (256) EURAW (257) EUUI (258) FR (261) FR-CIR (263)	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
12	Framed-MTU	Integer	MRU

Table B-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
23	Framed-IPX-Network	Integer	None
25	Class	Text string	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
46	Acct-Session-Time	Integer	None
47	Acct-Input-Packets	Integer	None

Table B-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
48	Acct-Output-Packets	Integer	None
61	NAS-Port-Type	NAS_Port_Type_Sync NAS_Port_Type_Async	None
125	Ascend-Maximum-Call-Duration	Integer	None
128	Ascend-Shared-Profile-Enable	Shared-Profile-No (0) Shared-Profile-Yes (1)	Shared-Prof
129	Ascend-Primary-Home-Agent	IP address or hostname	None
130	Ascend-Secondary-Home-Agent	IP address or hostname	None
131	Ascend-Dialout-Allowed	Dialout-Not-Allowed (0) Dialout-Allowed (1)	None
132	Ascend-Client-Gateway	IP address	Client-Default-Gateway
133	Ascend-BACP-Enable	BACP-No (0) BACP-Yes (1)	None
134	Ascend-DHCP-Maximum-Leases	Integer	None
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
147	Ascend-DHCP-Reply	DHCP-Reply-No (0) DHCP-Reply-Yes (1)	None
148	Ascend-DHCP-Pool-Number	Integer	None

Table B-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
149	Ascend-Expect-Callback	Expect-Callback-No (0) Expect-Callback-Yes (1)	Expect-Callback
150	Ascend-Event-Type	Ascend-Coldstart (1) Ascend-Session-Event (2)	None
151	Ascend-Session-Svr-Key	Text string	None
152	Ascend-Multicast-Client	Multicast-No (0) Multicast-Yes (1)	Multicast-Allowed
153	Ascend-Multicast-Rate-Limit	Integer	Multicast-Rate-Limit
154	Ascend-IF-Netmask	IP address	None
155	Ascend-Remote-Addr	IP address	None
156	Ascend-FR-Circuit-Name	Text string	None
157	Ascend-FR-LinkUp	Ascend-LinkUp-Default (0) Ascend-LinkUp-AlwaysUp (1)	None
158	Ascend-FR-Nailed-Grp	Integer	None
159	Ascend-FR-Type	Ascend-FR-DTE (0) Ascend-FR-DCE (1) Ascend-FR-NNI (2)	None
160	Ascend-FR-Link-Mgt	Ascend-FR-No-Link-Mgt (0) Ascend-FR-T1-617D (1) Ascend-FR-Q-933A (2)	None
161	Ascend-FR-N391	Integer	None
162	Ascend-FR-DCE-N392	Integer	None
163	Ascend-FR-DTE-N392	Integer	None
164	Ascend-FR-DCE-N393	Integer	None
165	Ascend-FR-DTE-N393	Integer	None
166	Ascend-FR-T391	Integer	None
167	Ascend-FR-T392	Integer	None
168	Ascend-Bridge-Address	***MAC_address*** ***profile_name*** ***IP_address***	None

Table B-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
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
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***]	None
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 between 16 and 991	None
180	Ascend-FR-Profile-Name	Text string	None
181	Ascend-Ara-PW	Text string	None
182	Ascend-IPX-Node-Addr	12-digit ASCII string	None
184	Ascend-Home-Agent-Password	Text string	None
185	Ascend-Home-Network-Name	Text string	None
186	Ascend-Home-Agent-UDP-Port	Integer	None
187	Ascend-Multilink-ID	Integer	None

Table B-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
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
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
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

Table B-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
214	Ascend-Send-Secret	Text string	Send-Password
215	Ascend-Receive-Secret	Text string	Recv-Password
216	Ascend-IPX-Peer-Mode	IPX-Peer-Router (0) IPX-Peer-Dialin (1)	None
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)	None
220	Ascend-FR-Direct-Profile	Text string	None
221	Ascend-FR-Direct-DLCI	Integer	None
222	Ascend-Handle-IPX	Handle-IPX-None (0) Handle-IPX-Client (1) Handle-IPX-Server (2)	None
223	Ascend-Netware-timeout	Integer	None
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)	None
230	Ascend-Bridge	Bridge-No (0) Bridge-Yes (1)	Bridge
231	Ascend-Send-Auth	Send-Auth-None (0) Send-Auth-PAP (1) Send-Auth-CHAP (2)	Send-Auth-Mode

Table B-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
232	Ascend-Send-Passwd	Text string	Send-Password
233	Ascend-Link-Compression	Link-Comp-None (0) Link-Comp-Stac (1)	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
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	Filter specification	None
243	Ascend-Call-Filter	Filter specification	None
244	Ascend-Idle-Limit	Integer	Idle-Timer
245	Ascend-Preempt-Limit	Integer	None
246	Ascend-Callback	Callback-No (0) Callback-Yes (1)	Callback

Table B-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
247	Ascend-Data-Svc	Switched-Voice-Bearer (0) Switched-56KR (1) Switched-64K (2) Switched-64KR (3) Switched-56K (4) Nailed-56KR (1) Nailed-64K (2) Switched-384KR (5) Switched-384K (6) Switched-1536K (7) Switched-1536KR (8) Switched-128K (9) Switched-192K (10) Switched-256K (11) Switched-320K (12) Switched-384K-MR (13) Switched-448K (14) Switched-512K (15) Switched-576K (16) Switched-640K (17) Switched-704K (18) Switched-768K (19) Switched-832K (20) Switched-896K (21) Switched-960K (22) Switched-1024K (23) Switched-1088K (24) Switched-1152K (25) Switched-1216K (26) Switched-1280K (27) Switched-1344K (28) Switched-1408K (29) Switched-1472K (30) Switched-1600K (31) Switched-1664K (32) Switched-1728K (33) Switched-1792K (34) Switched-1856K (35) Switched-1920K (36) Switched-inherited (37) Switched-restricted-bearer-x30 (38) Switched-clear-bearer-v110 (39) Switched-restricted-64-x30 (40) Switched-clear-56-v110 (41) Switched-modem (42)	Data-Service

Table B-2. Attributes and analogous parameters in numerical order (continued)

Attribute number	Attribute name	Attribute values	Analogous parameter
248	Ascend-Force-56	Force-56-No (0) Force-56-Yes (1)	Force-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	None
254	Ascend-MPP-Idle-Percent	Integer	None

Attributes and parameters in alphabetical order

Table B-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 B-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
Ascend-Add-Seconds	240	Integer	Add-Persistence

Table B-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-Ara-PW	181	Text string	None
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-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-Bridge	230	Bridge-No (0) Bridge-Yes (1)	Bridge
Ascend-Bridge-Address	168	***MAC_address*** ***profile_name*** ***IP_address***	None
Ascend-Callback	246	Callback-No (0) Callback-Yes (1)	Callback
Ascend-Call-By-Call	250	Integer	Call-By-Call
Ascend-Call-Filter	243	Filter specification	None
Ascend-Call-Type	177	Nailed (1) Nailed/Mpp (2) Perm/Switched (3)	Call-Type
Ascend-Client-Gateway	132	IP address	Client-Default-Gateway
Ascend-Connect-Progress	196	Integer	None
Ascend-Data-Filter	242	Filter specification	None
Ascend-Data-Rate	197	Integer	None

Table B-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-Data-Svc	247	Switched-Voice-Bearer (0) Switched-56KR (1) Switched-64K (2) Switched-64KR (3) Switched-56K (4) Nailed-56KR (1) Nailed-64K (2) Switched-384KR (5) Switched-384K (6) Switched-1536K (7) Switched-1536KR (8) Switched-128K (9) Switched-192K (10) Switched-256K (11) Switched-320K (12) Switched-384K-MR (13) Switched-448K (14) Switched-512K (15) Switched-576K (16) Switched-640K (17) Switched-704K (18) Switched-768K (19) Switched-832K (20) Switched-896K (21) Switched-960K (22) Switched-1024K (23) Switched-1088K (24) Switched-1152K (25) Switched-1216K (26) Switched-1280K (27) Switched-1344K (28) Switched-1408K (29) Switched-1472K (30) Switched-1600K (31) Switched-1664K (32) Switched-1728K (33) Switched-1792K (34) Switched-1856K (35) Switched-1920K (36) Switched-inherited (37) Switched-restricted-bearer-x30 (38) Switched-clear-bearer-v110 (39) Switched-restricted-64-x30 (40) Switched-clear-56-v110 (41) Switched-modem (42)	Data-Service

Table B-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-DBA-Monitor	171	DBA-Transmit (0) DBA-Transmit-Recv (1) DBA-None (2)	Bandwidth-Monitor-Direction
Ascend-Dec-Channel-Count	237	Integer	Decrement-Channel-Count
Ascend-DHCP-Maximum-Leases	134	Integer	None
Ascend-DHCP-Pool-Number	148	Integer	None
Ascend-DHCP-Reply	147	DHCP-Reply-No (0) DHCP-Reply-Yes (1)	None
Ascend-Dial-Number	227	Text string	Dial-Number
Ascend-Dialout-Allowed	131	Dialout-Not-Allowed (0) Dialout-Allowed (1)	None
Ascend-Disconnect-Cause	195	Integer	None
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-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	None
Ascend-FR-DCE-N392	162	Integer	None
Ascend-FR-DCE-N393	164	Integer	None
Ascend-FR-DTE-N392	163	Integer	None
Ascend-FR-DTE-N393	165	Integer	None
Ascend-FR-Direct	219	FR-Direct-No (0) FR-Direct-Yes (1)	None
Ascend-FR-Direct-DLCI	221	Integer	None
Ascend-FR-Direct-Profile	220	Text string	None
Ascend-FR-DLCI	179	Integer between 16 and 991	None

Table B-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-FR-Link-Mgt	160	Ascend-FR-No-Link-Mgt (0) Ascend-FR-T1-617D (1) Ascend-FR-Q-933A (2)	None
Ascend-FR-LinkUp	157	Ascend-LinkUp-Default (0) Ascend-LinkUp-AlwaysUp (1)	None
Ascend-FR-N391	161	Integer	None
Ascend-FR-Nailed-Grp	158	Integer	None
Ascend-FR-Profile-Name	180	Text string	None
Ascend-FR-T391	166	Integer	None
Ascend-FR-T392	167	Integer	None
Ascend-FR-Type	159	Ascend-FR-DTE (0) Ascend-FR-DCE (1) Ascend-FR-NNI (2)	None
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-Handle-IPX	222	Handle-IPX-None (0) Handle-IPX-Client (1) Handle-IPX-Server (2)	None
Ascend-History-Weigh-Type	239	History-Constant (0) History-Linear (1) History-Quadratic (2)	Dynamic-Algorithm
Ascend-Home-Agent-Password	184	Text string	None
Ascend-Home-Agent-UDP-Port	186	Integer	None
Ascend-Home-Network-Name	185	Text string	None
Ascend-Host-Info	252	Text string	Host-*n* Text-*n*
Ascend-Idle-Limit	244	Integer	Idle-Timer
Ascend-IF-Addr		IP address	
Ascend-IF-Netmask	154	IP address	None

Table B-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
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-IPX-Alias	224	Text string	None
Ascend-IPX-Node-Addr	182	12-digit ASCII string	None
Ascend-IPX-Peer-Mode	216	IPX-Peer-Router (0) IPX-Peer-Dialin (1)	None
Ascend-IPX-Route	174	***profile_name*** ***network#*** [***node#***] [***socket#***] [***server_type***] [***hop_count***] [***tick_count***] [***name***]	None
Ascend-Link-Compression	233	Link-Comp-None (0) Link-Comp-Stac (1)	Link-Compression
Ascend-Maximum-Call-Duration	125	Integer	None
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-MPP-Idle-Percent	254	Integer	None
Ascend-Multicast-Client	152	Multicast-No (0) Multicast-Yes (1)	Multicast-Allowed
Ascend-Multicast-Rate-Limit	153	Integer	Multicast-Rate-Limit
Ascend-Multilink-ID	187	Integer	None

Table B-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-Netware-timeout	223	Integer	None
Ascend-Number-Sessions	202	Text string	None
Ascend-Num-In-Multilink	188	Integer	None
Ascend-PPP-Address	253	IP address	None
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-Primary-Home-Agent	129	IP address or hostname	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-PW-Expiration	21	Date	None
Ascend-PW-Lifetime	208	Integer	None
Ascend-Receive-Secret	215	Text string	Recv-Password
Ascend-Remote-Addr	155	IP address	None
Ascend-Remove-Seconds	241	Integer	Sub-Persistence
Ascend-Require-Auth	201	Not-Require-Auth (0) Require-Auth (1)	Auth-Rsp-Required
Ascend-Route-IP	228	Route-IP-No (0) Route-IP-Yes (1)	IP-Touting-Enabled

Table B-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-Route-IPX	229	Route-IPX-No (0) Route-IPX-Yes (1)	None
Ascend-Secondary-Home-Agent	130	IP address or hostname	None
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-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
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

Table B-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Ascend-User-Acct-Type	138	Ascend-User-Acct-None (0) Ascend-User-Acct-User (1) Ascend-User-Acct-User-Default (2)	Acct-Type
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
Framed-Address	8	IP address	Remote-Address
Framed-Compression	13	Van-Jacobson-TCP-IP (1) (No other values supported)	VJ-Header-Prediction
Framed-IPX-Network	23	Integer	None
Framed-MTU	12	Integer	MRU
Framed-Netmask	9	IP address	Netmask-Remote
Framed-Protocol	7	PPP (1) SLIP (2) MPP (256) EURAW (257) EUUI (258) FR (261) FR-CIR (263)	Encapsulation-Protocol
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
Login-Host	14	IP address	Host

Table B-3. Attributes and analogous parameters in alphabetical order (continued)

Attribute name	Attribute number	Attribute values	Analogous parameter
Login-Service	15	Telnet (0) Rlogin (1) TCP-Clear (2)	Service
Login-TCP-Port	16	Integer	Port
NAS-Identifier	4	IP address	IP-Address Netmask Local-Address Netmask-Local
NAS-Port	5	Zero-based, bit encoded number	None
NAS-Port-Type	61	NAS_Port_Type_Sync NAS_Port_Type_Async	None
Password (User-Password)	2	Text string	Recv-Password
Reply-Message	18	Text string	Banner (terminal-server users only)
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)	None

Attribute and Packet Cross Reference

C

This appendix contains a list of packets and their RADIUS attributes associated with authentication, connection setup, and user sessions. The appendix consists of the following sections:

For information about attributes associated with accounting, see “Understanding accounting records” on page 13-10.

Access-Request attributes

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 C-1.

Table C-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)	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 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 MAX TNT.	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, such as for the purpose of 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 network port on which the MAX TNT received a call.	Specified in the `/etc/services` file
NAS-Port-Type (61)	Specifies the type of service in use for the established session.	Async
Password (2)	Specifies the user's password for an incoming or outgoing call.	Null
User-Name (1)	Specifies the user's name.	Null

Table C-1. Access-Request attributes (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. 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 attributes

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 C-2 lists the RADIUS attributes defined in IETF RFC 2058 and supported by the Ascend RADIUS daemon.

Table C-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, such as for the purpose of 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

Table C-2. RFC 2058 Access-Accept attributes supported by Ascend (continued)

Attribute	Description	Default value
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+, Frame Relay, EU-UI, or EU-RAW link.	1524
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-IPX-Network (23)	Specifies a virtual IPX network required for the home agent to route IPX packets to the mobile node.	Null
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.
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
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
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

Table C-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 C-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-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-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
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-Bridge (230)	Enables or disables protocol-independent bridging for the link.	Disable bridging.
Ascend-Bridge-Address (168)	Specifies a bridge entry.	*MAC_address*=000000000000 *profile_name*=null *IP_address*=0.0.0.0
Ascend-Callback (246)	Enables or disables callback.	Disable callback.

Table C-3. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default value
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-Gateway (132)	Specifies the default route for IP packets coming from the user on this connection.	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
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-DHCP-Maximum-Leases (134)	Specifies the maximum number of dynamic addresses to assign to Network Address Translation (NAT) clients using a connection	4
Ascend-DHCP-Pool-Number (148)	Specifies the address pool to use for allocating an IP address to a Dynamic Host Configuration Protocol (DHCP) client or a Network Address Translation (NAT) client during a connection.	0 (zero)
Ascend-DHCP-Reply (147)	Specifies whether the MAX TNT processes Dynamic Host Configuration Protocol (DHCP) packets and acts as a DHCP server during a connection.	DHCP-Reply-No (Disable DHCP functionality.)
Ascend-Dial-Number (227)	Specifies the phone number the MAX TNT dials to reach the bridge, 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

Table C-3. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default value
Ascend-Expect-Callback (149)	Specifies whether a user calling out should expect the remote end to call back.	Expect-Callback-No
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.)
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 gateway connection or a redirect connection.	FR-Direct-No
Ascend-FR-Direct-DLCI (221)	Identifies the user profile to the Frame Relay switch as a logical link on a physical circuit for a redirect connection.	16
Ascend-FR-Direct-Profile (220)	Specifies the name of the Frame Relay profile that carries the redirect connection to the Frame Relay switch.	Null
Ascend-FR-DLCI (179)	Specifies the Data Link Connection Indicator that identifies the RADIUS user profile to the Frame Relay switch as a logical link on a physical circuit in a gateway connection.	16
Ascend-FR-DTE-N392 (163)	Specifies the number of errors, occurring during Ascend-FR-DTE-N393-monitored events, that cause the network side to declare the user side's procedures inactive.	3

Table C-3. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default value
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-LinkUp (157)	Specifies whether a link comes up automatically.	Link does not come up automatically.
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 the MAX TNT uses to build a gateway connection.	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 type of Frame Relay connection.	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-AIM or 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-Handle-IPX (222)	Specifies how the MAX TNT handles NCP watchdog requests on behalf of IPX clients during IPX bridging.	Handle-IPX-None (Do not handle NCP watchdog requests.)
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

Table C-3. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default value
Ascend-Home-Agent-Password (184)	Specifies the password that the foreign agent sends to the home agent during ATMP operation.	Null
Ascend-Home-Agent-UDP-Port (186)	Specifies the UDP port number to use when the foreign agent sends ATMP packets to the home agent.	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 node during ATMP operation.	Null
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-Addr	Specifies the IP address of the local numbered interface to the WAN.	0.0.0.0
Ascend-IF-Netmask (154)	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-IPX-Alias (224)	Specifies an IPX network number to use when connecting to IPX routers that require numbered interfaces.	00000000
Ascend-IPX-Node-Addr (182)	Specifies a unique IPX node address on the Framed-IPX-Network. This value completes the IPX address of a mobile node.	000000000001
Ascend-IPX-Peer-Mode (216)	Specifies whether the caller is an Ethernet client with its own IPX network address or a dial-in PPP client.	IPX-Peer-Router (Ethernet client with its own IPX network address)

Table C-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 an incoming call can remain connected.	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 length of time, in seconds, allowed for any session.	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 (152)	Specifies whether the user is a multicast client of the MAX TNT.	Multicast-No
Ascend-Multicast-Rate-Limit (153)	Specifies how many seconds the MAX TNT waits before accepting another packet from a multicast client.	100

Table C-3. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default value
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-Netware-timeout (223)	Specifies the number of minutes the MAX TNT responds to NCP watchdog requests on behalf of IPX clients on the other side of an offline IPX bridging or routing connection.	0 (zero)
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 the MAX TNT reports to the calling unit during PPP IPCP negotiations.	Always negotiated
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)	Instructs the MAX TNT whether to use the 0037h value for the VJ compression type.	VJ compression type 002dh
Ascend-PPP-VJ-Slot-Comp (210)	Instructs the MAX TNT whether to 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.	None (Attribute does not appear in a user profile.)
Ascend-Pre-Input-Packets (192)	Specifies the number of input packets before authentication.	None (Attribute does not appear in a user profile.)
Ascend-Pre-Output-Octets (191)	Specifies the number of output octets before authentication.	None (Attribute does not appear in a user profile.)
Ascend-Pre-Output-Packets (193)	Records the number of output packets before authentication.	None (Attribute does not appear in a user profile.)

Table C-3. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default value
Ascend-Primary-Home-Agent (129)	Specifies the first home agent the foreign agent tries to reach when setting up an ATMP tunnel, and indicates the UDP port the foreign agent uses for the link.	0.0.0.0 (IP address) 5150 (UDP port)
Ascend-PRI-Number-Type (226)	Specifies the type of phone number the MAX TNT dials.	National-Number
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-Receive-Secret (215)	Specifies a value received from a dial-in user to verify an encrypted password.	Null
Ascend-Remote-Addr (155)	Specifies the IP address of the link's remote interface to the WAN.	0.0.0.0
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-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-Secondary-Home-Agent (130)	Specifies the secondary home agent the foreign agent tries to reach when the primary home agent (Ascend-Primary-Home-Agent) is unavailable. Also indicates the UDP port the foreign agent uses for the link.	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

Table C-3. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default value
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
Ascend-Shared-Profile-Enable (128)	Specifies whether multiple incoming callers can share a single RADIUS user profile.	Shared-Profile-No
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

Table C-3. Ascend RADIUS Access-Accept attributes (continued)

Attribute	Description	Default value
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 the value of the Ascend-TS-Idle-Limit attribute.)

Access-Reject attributes

If the attribute values submitted to RADIUS do not match the attribute values in the user profile, the RADIUS server does not authenticates the call. It returns an Access-Reject packet containing one or more of the values listed in Table C-4.

Table C-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-Terminate-Session attributes

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. This attribute carries message text from the RADIUS server to RADIUS clients such as the MAX TNT.

Ascend-Access-Event-Request attributes

The MAX TNT can report the number of sessions by class to the RADIUS authentication server when Auth-Type=RADIUS-Logout in the Rad-Auth-Client subprofile of the External-Auth profile. In addition, the MAX TNT can report on sessions 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 (for authentication requests)
- Acct-Sess-Interval in the Rad-Acct-Client subprofile of the External-Auth profile (for accounting requests).

Table C-5 lists the attributes in an Ascend-Access-Event-Request packet.

Table C-5. Ascend-Access-Event-Request attributes

Attribute	Description	Default value
NAS-Identifier (4) (for both authentication and accounting requests)	Specifies the IP address of the MAX TNT.	0.0.0.0/0
Password (2) (for authentication requests only)	Specifies the user's password for an incoming or outgoing call.	Null
Ascend-Event-Type (150) (for both 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) (for both authentication and accounting requests)	Specifies the number of active user sessions of a given class (as indicated by the Class attribute). In the case of multi-channel calls, such as MP+ calls, each separate connection counts as a session.	0 (zero)

Ascend-Access-Event-Response attributes

Table C-6 lists the attributes in an Ascend-Access-Event-Response packet.

Table C-6. Ascend-Access-Event-Response attributes

Attribute	Description	Default value
NAS-Identifier (4) (for both authentication and accounting responses)	Specifies the IP address of the MAX TNT.	0.0.0.0/0
Ascend-Event-Type (150) (for both 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) (for both 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 multi-channel calls, such as MP+ calls, each separate connection counts as a session.	0 (zero)

Index

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W