MAX T1/PRI
Security Supplement

Ascend Communications

Pipeline, Multiband, and Multiband Bandwidth-on-Demand are trademarks of Ascend Communications, Inc. Other trademarks and trade names mentioned in this publication belong to their respective owners.

Copyright © 1996, Ascend Communications, Inc. All Rights Reserved.

This document contains information that is the property of Ascend Communications, Inc. This document may not be copied, reproduced, reduced to any electronic medium or machine readable form, or otherwise duplicated, and the information herein may not be used, disseminated or otherwise disclosed, except with the prior written consent of Ascend Communications, Inc.

Part Number 7820-0404-002 January 25, 1996

Ascend Customer Service

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

- The product name and model
- The software and hardware options
- The software version
- The SPIDs (Service Profile Identifiers) associated with your product
- The type of telco switch and mode, such as AT&T 5ESS Custom or Northern Telecom DMS-100 National ISDN 1
- Whether you are routing or bridging with your Ascend product
- The type of computer you are using
- A description of the problem

How to contact Ascend Customer Service

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

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

Ascend Communications
1275 Harbor Bay Parkway
Alameda, CA 94502

Need information on new features and products?

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

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

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

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

  `ftp.ascend.com`

Table of Contents

About This Supplement

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

1 MAX System Security

Introduction to system security 1-2
Setting up security profiles. 1-3
    Parameters in a Security Profile 1-3
    Modifying the Default Profile. 1-4
    Assigning a password to the Full Access Profile 1-5
    Activating the Full Access security level 1-6
Restricting operator access. 1-7
    Disabling remote management access 1-8
    Password-protecting SNMP 1-8
    Password-protecting Telnet access 1-8
    Restricting the terminal server environment. 1-9
        Assigning a password for dial-in sessions. 1-9
        Protecting the command-line interface 1-10
        Restricting Telnet in the terminal server 1-10

2 Connection Security

Introduction to connection security 2-2
Authenticating calls 2-3
    Using CLID authentication. 2-4
    Using callback security. 2-5
    Requiring a Connection Profile 2-5
    PPP authentication using PAP or CHAP 2-5
    Combinet authentication. 2-7
    Terminal server call authentication. 2-8
Integrating the MAX with third-party servers 2-8
    RADIUS servers. 2-9
    TACACS servers 2-9
    Configuring the MAX to communicate with RADIUS or TACACS. 2-9
    Password aging and expired RADIUS passwords 2-10

3 Security Card Authentication

How security cards work 3-2
Supporting incoming security card calls 3-3
    Configuring the MAX for incoming security card calls. 3-3
    Setting RADIUS attributes for security card authentication. 3-3
        RADIUS attributes for token passwords 3-3
        Setting an authentication mode in the users file 3-4

Sample RADIUS user profiles. 3-5
Supporting outbound security card calls 3-6
Setting up a dial-out connection to a secure site. 3-6
Requesting PAP-TOKEN mode 3-6
Requesting PAP-TOKEN-CHAP mode 3-7
Requesting CACHE-TOKEN 3-7
Configuring a connection with a local APP Server utility 3-8
Invoking password mode in the terminal server. 3-8
Using the APP Server on a UNIX host. 3-9
Using the APP Server utility on a DOS or Windows host 3-10
Installing the APP Server utility for DOS 3-11
Installing the APP Server utility for Windows 3-12

About This Supplement

This Supplement explains security issues related to local and wide-area networking. It focuses only on security and in many cases it refers to the *MAX ISP and Telecommuting Configuration Guide* and the *MAX RADIUS Supplemen*t for details on how to set up specific configurations.

What is in this supplement?

This Supplement contains these chapters:

- Chapter 1, "MAX System Security," shows you how to restrict access to the operations of the MAX. It describes security profiles and includes information about preventing unauthorized operations from Telnet sessions, SNMP, and other access methods.
- Chapter 2, "Connection Security," shows you how to control who can access your local network through the MAX. It explains call authentication, security protocols, callback, and other connection security features. It also explains how to configure the MAX to forward authentication requests to a RADIUS or TACACS server.
- Chapter 3, "Security Card Authentication," explains how to support security card authentication and set up users to respond to password challenges. It includes information about Ascend's APP Server utility and password mode in a terminal server session.

What you should know

This Supplement is intended for the person who is setting up security in the MAX. It does not discuss general network security issues or provide guidelines about the extent to which you should protect your network and local hosts.

If you would like some background about security, we recommend the following publication, which is available in book stores:

- *Firewalls and Internet Security*, William R. Cheswick and Steven M. Bellovin

Documentation conventions

This section shows the documentation conventions used in this guide.

Convention	Meaning
`Monospace text`	Monospace text represents information that you enter exactly as shown, and it identifies onscreen text, such as, statistical information.
italics	Italics represent variable information. Do not enter the words themselves in the command; enter the information they represent.

Convention	Meaning
Note:	A note signifies important additional information.
 **Caution:**	A caution means that a failure to follow the recommended procedure could result in a loss of data or damage to equipment.
 **Warning:**	A warning means that a failure to take appropriate safety precautions could result in physical injury.

MAX System Security

1

This chapter covers these topics:

Introduction to system security 1-2

Setting up security profiles. 1-3

Restricting operator access. 1-7

Introduction to system security

System security protects the MAX itself from unauthorized access. The following configuration parameters are related to system security:

Table 1-1. System security parameters

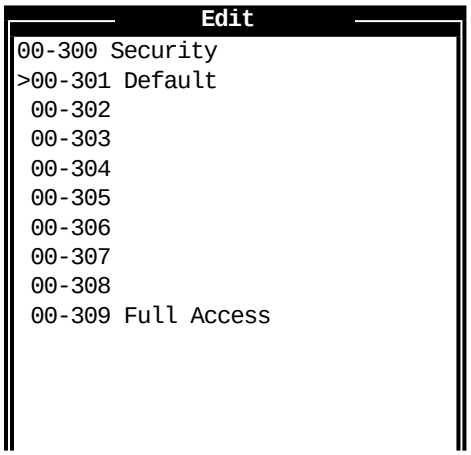
Location	Parameter with default value
System→Sys Config	Remote Mgmt=Yes
System→Security→*any profile*	Name=[] Passwd=[] Operations=Yes Edit Security=Yes Edit System=Yes Edit Line=Yes Edit All Ports=Yes Edit Own Port=N/A Edit All Calls=Yes Edit Com Call=N/A Edit Own Call=N/A Edit Cur Call=N/A Sys Diag=Yes All Port Diag=Yes Own Port Diag=N/A Download=Yes Upload=Yes Field Service=Yes
Ethernet→Mod Config→SNMP options...	Read Comm=public R/W Comm=write
Ethernet→Mod Config→TServ options...	TS Enabled=Yes Passwd=[] Telnet=Yes Initial Scrn=Cmd Toggle Scrn=No Security=None Host #*n* Addr=0.0.0.0 Host #*n* Text=[] Immed Telnet-0.0.0.0
Ethernet→Mod Config	Telnet PW=[]

For details on each of these parameters, see Table 1-2 on page 1-3 and the *MAX Reference Guide*. For information about RADIUS attributes, see the *MAX RADIUS Supplement*.

Note: All passwords are initially null except for the Full Access Profile password, which has the default password “Ascend”, and the SNMP community strings. We recommend that you change these defaults as soon as possible. See *MAX ISP and Telecommuting Configuration Guide* for related information about saving and restoring configurations.

Setting up security profiles

The MAX has up to nine security levels, which are defined in Security Profiles. Security Profiles are located below System→Security in the MAX configuration menus.



When the MAX is shipped from the factory, all levels are set with full privileges. A profile must have a name to be activated, so only the Default and Full Access Profiles can be activated initially.

Note: We strongly recommend that you follow the instructions in "Modifying the Default Profile" on page 1-4 and "Assigning a password to the Full Access Profile" on page 1-5. These instructions result in two security levels, one that is totally restrictive (Default) and one that is totally open (Full Access). If you need additional security levels, you can define them in the remaining Security Profiles.

Parameters in a Security Profile

The parameters in a Security Profile are listed below. For more details on each of these parameters, see the *MAX Reference Guide*.

Table 1-2. Parameters in a Security Profile

Parameter	Description
Name	A Security Profile name can be up to 16 characters. Initially, only two of the Security Profiles have a name (Default and Full Access). A profile must have a name for users to select it.
Passwd	A password can be up to 20 characters. The Default profile has no password. The default password for the Full Access Profile is "Ascend".
Operations	When set to Yes, an operator can view configuration profiles and change the value of any parameter that is not restricted by other settings. Setting this to No sets all other privileges in the profile to N/A. In addition, when this privilege is set to No, an operator cannot access most DO commands. Only DO Esc, DO Close Telnet, and DO password are available to them.

Table 1-2. Parameters in a Security Profile (continued)

Parameter	Description
Edit Security	When set to Yes, an operator can edit Security Profiles and access all other operations by enabling them in his or her active Security Profile. This is the most powerful privilege, because it enables users to modify their own privileges.
Edit System	When set to Yes, an operator can edit the System Profile, the SNMP Read Comm and R/W Comm passwords, and the IP routing table (in the terminal server interface). If Edit System=No, an operator cannot edit the System Profile, the SNMP password parameters, or the IP routing table.
Edit Line	When set to Yes, an operator can edit Line Profiles.
Edit All Ports	When set to Yes, an operator can edit all Port Profiles.
Edit Own Port	When set to Yes, an operator can use AIM remote management to edit the Port Profile for the port that has been called.
Edit All Calls	When set to Yes, an operator can edit all parameters in all Call Profiles and Connection Profiles.
Edit Com Call	When set to Yes, an operator can edit common Call Profiles.
Edit Own Call	When set to Yes, an operator can use AIM or MP+ remote management to edit the Call Profiles for the port that has been called.
Edit Cur Call	When set to Yes, an operator can edit all parameters in the current Call Profile.
Sys Diag	When set to Yes, an operator can use any of the commands in the Sys Diag menu.
All Port Diag	When set to Yes, an operator can perform all serial host port diagnostics. A serial host port is the V.35, RS-499, or X.21 port on the MAX.
Own Port Diag	When set to Yes, an operator can perform port diagnostics for his or her own serial host port.
Download	When set to Yes, an operator can download the configuration of the MAX using the Save Cfg command.
Upload	When set to Yes, an operator can upload a configuration using the Restore Cfg command.
Field Service	When set to Yes, an operator can perform Ascend-provided field service operations, such as uploading new system software.

Modifying the Default Profile

The first profile in the Security menu is named Default. The password assigned to this profile is null, and the profile's name and password cannot be changed. The MAX activates this profile whenever it is powered on or reset, and for every new login session.

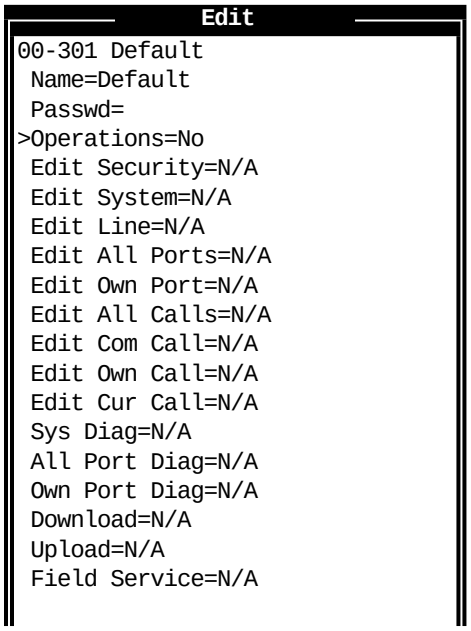
Note: Although the Default Profile is set initially with full privileges, it is intended to be very restrictive, because every user who logs in via Telnet, the Control port, or remote management, is granted the privileges specified there.

To edit the Default Profile to make it appropriately restrictive, follow these steps:

1. Open the Default Profile.

   The first two parameters in the Default Profile cannot be changed—the name is always Default and the password is always null.

2. Set Operations to No.



   All other parameters are set to N/A when Operations=No.

   Operators will be able to view settings but will not be able to change anything, and all passwords (including the null password) will be hidden by the string *SECURE* in the MAX user interface.

3. Exit the Default Profile, saving your changes.

Assigning a password to the Full Access Profile

The last profile in the Security menu is named Full Access. The default password assigned to this profile is “Ascend”.

The Full Access Profile is intended to remain totally open, with all privileges set to Yes. It is important to change the default password as soon as possible. It is also important *not* to turn off the Edit Security privilege in the Full Access Profile, or you will be unable to edit privileges when Full Access has been activated.

To assign a password protecting the Full Access Profile, follow these steps:

1. Open the Full Access Profile.
2. When you are prompted for the password, type:

   Ascend

   Passwords are case sensitive. You must enter the password exactly as shown.

3. Select the Passwd parameter and press Enter to open a text field.
4. Type a new password for this profile.

```
Edit
00-309 Full Access
 Name=Full Access
>Passwd=*SECURE*
 Operations=Yes
 Edit Security=Yes
 Edit System=Yes
 Edit Line=Yes
 Edit All Ports=Yes
 Edit Own Port=N/A
 Edit All Calls=Yes
 Edit Com Call=N/A
 Edit Own Call=N/A
 Edit Cur Call=N/A
 Sys Diag=Yes
 All Port Diag=Yes
 Own Port Diag=N/A
 Download=Yes
 Upload=Yes
 Field Service=Yes
```

5. Leave all other privileges enabled.

   Do not turn off the Edit Security privilege!
6. Exit the Full Access Profile, saving your changes.

Although the MAX does not prevent you from turning off privileges in the Full Access Profile, most sites leave all privileges enabled in this profile and define additional Security Profiles to handle slightly more restrictive privileges.

Activating the Full Access security level

To activate the Full Access Profile, follow these steps:

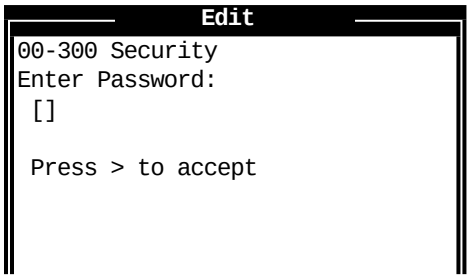
1. Press Ctrl-D to open the DO menu, and then press P (or select P=Password).

```
Edit
00-300 Security
DO...
>0=ESC
 P=Password
```

2. In the list of Security Profiles that opens, select Full Access.

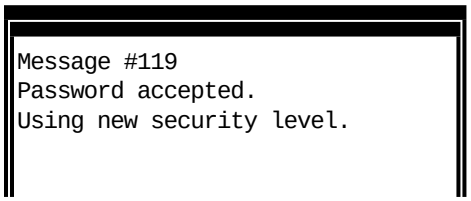
   (After you have defined privileges in additional Security Profiles, you can select any profile with the security level you need.)

   The MAX then prompts for that profile's password.



3. Type the password assigned to the profile and press Enter to accept it.

   If you enter the right password, a message states that the password was accepted and the MAX is using the new security level.



If the password you enter is incorrect, you are prompted again to enter the password.

Restricting operator access

There are several access methods that enable an operator to log into the MAX or to access information about it. Each of these access methods must be considered when you're setting up system security in the MAX.

Note: An operator is assigned the default security level at login. Without a password to the Full Access Profile or another "open" Security Profile, the operator can view information but cannot change anything.

This section describes how to restrict these access methods:

- AIM or MP+ remote management access from a remote Ascend unit

  An operator of a remote Ascend unit can use the DO menu (DO-8) to begin a remote management session on an AIM or MP+ call.

- Telnet login from any Telnet workstation

  A user can log into the MAX from a local or remote host.

- Access from an SNMP manager on any IP host

  A user who has access to an SNMP manager application can access information stored in the MAX, including its routing table and other data you may want to restrict.

- Terminal server login

  A user can start a terminal server session from a computer in terminal emulation mode connected to the MAX Control port (a serial connection) or from a remote computer via Telnet or TCP. See the chapter on Configuring the MAX as a Terminal Server in the *MAX ISP and Telecommuting Configuration Guide* for details about terminal server sessions.

Disabling remote management access

To prevent an operator from accessing the MAX from a remote Ascend unit using AIM or MP+ remote management, open the System Profile and set the Remote Mgmt parameter to No.

Table 1-3. Remote management parameter

Location	Parameter
System→Sys Config	Remote Mgmt=No

For related information on remote management, see the chapter on System Administration in the *MAX ISP and Telecommuting Configuration Guide*.

Password-protecting SNMP

You can assign passwords that restrict operators from accessing the MAX from an SNMP manager on any IP host by assigning keywords to the community strings.

Table 1-4. SNMP passwords

Location	Parameter
Ethernet→Mod Config→SNMP options...	Read Comm=*SECURE* (a keyword) R/W Comm=*SECURE* (a keyword)

An SNMP manager application residing on a workstation on the local or remote network can access management information, set alarm thresholds, and change some settings on the MAX. To password-protect this type of network access, assign Read and Read/Write SNMP community string. Each string can be up to 16 characters.

- Read Comm

  The Read community string authenticates an SNMP manager accessing the MAX to perform read commands (GET and GET NEXT). The GET command requests information. The GET NEXT command is used to obtain a table of information, such as a routing table. After you enter a string in the Ethernet Profile, users must supply it to use those SNMP commands.

- R/W Comm

  The Write community string authenticates an SNMP manager accessing the MAX to perform read and write commands (GET, GET NEXT, and SET). The SET command is issued to change information maintained by the MAX. After you enter a string in the Ethernet Profile, users must supply it to use those SNMP commands.

Note: There is no way to turn SNMP Write off, so it is important to set a secret R/W Comm string. The default R/W Comm string is set to “write,” which means that anyone who has used an Ascend product probably knows this default string.

Password-protecting Telnet access

You can restrict operators from accessing the MAX across the network from a remote PC running Telnet by assigning a Telnet password.

Table 1-5. Telnet password

Location	Parameter
Ethernet→Mod Config	Telnet PW=*SECURE* (a password)

The Telnet password you supply in the Ethernet Profile (Mod Config menu) may be up to 20 characters in length. Any user who initiates an incoming Telnet session to the MAX will be prompted to supply this password before the Telnet session is established.

If the Telnet session is initiated from the WAN, the connection must be authenticated as specified in a Connection Profile first. See Chapter 2, "Connection Security."

See “Restricting Telnet in the terminal server” on page 1-10 for additional information about restricting Telnet in the terminal server interface.

Restricting the terminal server environment

For details about how the MAX authenticates terminal server calls, see “Authenticating calls” on page 2-3. Table 1-6 shows the parameters you can use to restrict the terminal server environment.

Table 1-6. Terminal server security parameters

Location	Parameter
Ethernet→Mod Config→TServ options...	TS Enabled=Yes Passwd=*SECURE* Telnet=Yes Initial Scrn=Cmd Toggle Scrn=No Security=None Host #*n* Addr=0.0.0.0 Host #*n* Text=[] Immed Telnet-0.0.0.0

Note: If you edit the terminal server banner or the list of Telnet hosts in the RADIUS files, use the Upd Rem Cfg command in the Sys Diag menu to update these fields in the MAX.

Assigning a password for dial-in sessions

The first two parameters in the TServ Options submenu of the Ethernet Profile enable terminal server sessions and assign a password that may be required from remote users.

- TS Enabled

  If you set this parameter to No, no one can access the terminal server interface.

- Passwd

  If you specify a password here, users logging into the terminal server via modem, V.120, or V.110 will be prompted to supply it before gaining admission to the terminal server. It does not apply to remote sessions authenticated by RADIUS or to a local terminal server session. Users who are authenticated by RADIUS supply a password that matches their User-Password in the RADIUS database.

Protecting the command-line interface

The remaining terminal server security parameters shown in Table 1-6 are related to keeping dial-in users from accessing the command-line interface in a terminal server session. The command-line interface enables users to see routes, addresses, and statistics about the local network. You can prevent users from accessing those commands by setting the screen to the menu-driven interface, or by redirecting the terminal server session into a host other than the MAX via “immediate Telnet.”

By default, terminal server sessions present users with a command-line interface. You can change this default and prevent users from toggling to the command-line interface, or require that they enter the terminal server password to toggle to that interface.

- Initial Scrn and Toggle Scrn

  The Initial Scr parameter specifies the type of user interface that appears at the beginning of a remote terminal server session, the standard command-line interface or a menu-driven interface. To prevent users from accessing the command-line interface, set this parameter to Menu.

  You also must set the Toggle Scrn parameter to No, to prevent users from switching to the command-line interface.

- Security

  This parameter specifies the type of security that the MAX uses with a remote terminal server session.

  – None (the default) specifies that the user sees the initial terminal server screen and can change between menu-driven mode and command-line mode without entering the local terminal server password specified by Passwd, and without being remotely authenticated.

  – Partial specifies that the user sees the initial terminal server screen without entering the local terminal server password specified by Passwd, and without being remotely authenticated.

    However, the user must enter a terminal server password when changing between menu-driven mode and command-line mode if Initial Scrn=Cmd or Toggle Scrn=Yes.

  – Full specifies that the user sees the initial terminal server screen by entering the local terminal server password specified by Passwd, or by entering the remote authentication server name and password; in addition, the user must enter a password when changing between menu-driven mode and command-line mode.

Restricting Telnet in the terminal server

The Telnet parameters have two implications for security. One is for the security of the command-line interface itself, the other is for the security of other hosts on your local network.

- Telnet

  If you want to stop users from invoking Telnet sessions in the terminal server environment, set Telnet to No.

- Host #n Addr and Host #n Text

  These parameters specify the IP addresses and names of the first, second, third, and fourth hosts to which an operator can Telnet, as listed in the terminal server menu-driven interface.

- Immed Telnet

  This parameter specifies the IP address or hostname of a device to which remote terminal server users Telnet immediately after the terminal server banner appears. If you specify an address here, the users will never see the MAX interface, they will instead immediately be connected to the specified host via Telnet.

Connection Security

2

This chapter covers these topics:

Introduction to connection security 2-2

Authenticating calls 2-3

Integrating the MAX with third-party servers 2-8

Introduction to connection security

The MAX includes several security mechanisms for controlling dial-in access, including the following features:

- Authentication protocols for PPP (point-to-point protocol) encapsulated calls

  The MAX supports both PAP (password authentication protocol) and CHAP (challenge handshake authentication protocol).

- CLID (calling-line ID) authentication

  Calling Line ID or Caller ID is the phone number of the user placing the call. If you configure the MAX for CLID authentication, it adds this information to the authentication process.

- Callback

  When callback is enabled in a profile and an incoming call matches that profile, the MAX hangs up and dials back using the dial number specified in the profile. Callback security provides the highest level of control in assuring that incoming calls are coming from a known network.

- Rejecting unknown callers

  When password authentication is not in use, you can configure the MAX to reject all incoming bridging or routing calls for which a matching profile is not found.

- Filters

  Filtering can provide a robust form of security available in a dial-up internetworking environment. You can tailor a filter on a per-connection basis to allow or deny packets from any combination source and destination address, protocol discriminator, source and destination port, and TCP sessions.

  For details on filter security, see the chapter on Using Filters in the *MAX ISP and Telecommuting Configuration Guide*.

- Integration with RADIUS or TACACS authentication servers

  As communities of dial-in sites grow, it becomes impractical to store all relevant security and access parameters in a single piece of equipment. The MAX can access a third-party database such as RADIUS or TACACS instead, which makes it easier to centrally control, manage, and audit security.

- Integration with ACE or SAFEWORD servers using personal security cards

  A security card is a hand-held device the shape and size of a credit card, such as those provided by Enigma Logic or Security Dynamics. You can configure the MAX to present dial-in users with password challenges that require passwords obtained from such a card.

This chapter does not describe the details of how IP addresses are validated or assigned to incoming callers dynamically, although that process may be part of caller authentication. For details on that topic, see the chapter on Configuring the MAX as an IP Router in the *MAX ISP and Telecommuting Configuration Guide*.

This chapter does not describe how to configure the MAX to work with ACE or SAFEWORD servers. For details on that topic, see Chapter 3, "Security Card Authentication."

The configuration parameters shown in Table 2-1 are related to connection authentication:

Table 2-1. Connection authentication parameters

Location	Parameter with default value
System→Sys Config	Name=[]
Ethernet→Connections→*any profile*	Station=[] Calling #=[] Dial #=[]
Ethernet→Connections→*any profile*→ IP options...	LAN Adrs=0.0.0.0
Ethernet→Connections→*any profile*→ Encaps options...	Recv PW=[] Send Auth=None Send PW=[] Aux Send PW=N/A
Ethernet→Connections→*any profile*→ Telco options...	Callback=No AnsOrig=Both
Ethernet→Answer	Profile Reqd=No CLID Auth=Ignore
Ethernet→Answer→PPP options...	Recv Auth=None
Ethernet→Answer→COMB options...	Password Reqd=No
Ethernet→Mod Config→TServ options...	TS Enabled=Yes Passwd=[] Initial Scrn=Cmd Security=Full
Ethernet→Mod Config→Auth...	Auth=None Auth Host #1=N/A Auth Host #2=N/A Auth Host #3=N/A Auth Port=N/A Auth Timeout=N/A Auth Key=N/A Auth Pool=N/A Auth Req=No

Authenticating calls

The MAX authenticates incoming calls based on the type of call and the authentication settings related to that call type. These are the basic types of incoming call:

- PPP and MP+ calls

  Most sites require PAP or CHAP authentication of PPP calls. If the incoming PPP call does not include a source IP address, PAP or CHAP authentication is required.

- Combinet calls

  Combinet calls are authenticated based on the physical address of the calling device. Most sites also require a password to authenticate Combinet calls.

- Terminal server calls

  Terminal server calls can be authenticated before the connection is accepted by assigning a password to the terminal server interface and setting Security to Full.

You can use CLID authentication, callback, or both to increase the security of your local network against intrusion based on any type of incoming call.

For information about configuring these authentication methods in a RADIUS users file, see the *MAX RADIUS Supplement.*

Using CLID authentication

CLID is the calling line ID—the phone number of the calling device. You can require CLID authentication to ensure that the incoming call originates at a known location.

When CLID authentication is configured, the MAX hangs up if the number specified in the Calling # parameter does not match the caller's number. CLID authentication occurs first, before any name-password comparisons.

Note: If the call matches a RADIUS profile in which Ascend-Require-Auth=Require-Auth, the session parameters set by CLID authentication may change during subsequent name-password authentication. See the description of the Auth Req parameter in "Configuring the MAX to communicate with RADIUS or TACACS" on page 2-9 for related information.

To set CLID authentication, use the parameters shown in Table 2-2. Or, see the *MAX RADIUS Supplement* to configure it in the users file.

Table 2-2. CLID authentication parameters

Location	Parameter
Ethernet→Connections→*any profile*	Calling #=555-1213
Ethernet→Answer	CLID Auth=Required (or Prefer)

In some installations, the WAN provider might not be able deliver CLIDs, or individual callers might choose to keep their CLIDs private; in addition, CLID is not available without end-to-end ISDN service on the call and ANI (Automatic Number Identification) from your WAN provider. Ask your WAN provider whether the calling-party number is conveyed by the network to the receiving party. In some cases, the network does not deliver the calling-party number, such as when the MAX is behind one or more PBXs.

The CLID Auth parameter in the Answer Profile can be set to these values:

- CLID Auth=Ignore

  Ignore indicates that calling-party information is not required for authentication.

- CLID Auth=Prefer

  Prefer specifies that whenever CLID is available, the calling-party's phone number must match the Calling # parameter before answering the call. If the CLID is not available or if the MAX cannot find a match to a calling number, the MAX applies authentication using the Recv Auth or Password Reqd parameters.

- CLID Auth=Required

  Required indicates that the calling-party's phone number must match the value of the Calling # parameter before the MAX can answer the call. If the CLID is not available, the MAX does not answer the call.

Using callback security

Callback security instructs the MAX to hang up and call back when it receives an incoming call. You can require callback to ensure that the connection is made with the number specified in the Dial # parameter.

Note: The Callback parameter is N/A for leased lines (if Call Type=Nailed).

To set callback security, use the parameters shown in Table 2-3. Or, see the *MAX RADIUS Supplement* to configure it in the users file.

Table 2-3. Callback parameters

Location	Parameter
Ethernet→Connections→*any profile*	Dial #=555-1415
Ethernet→Connections→*any profile*→ Telco options...	Callback=Yes AnsOrig=Both

If you set Callback=Yes, you must also set AnsOrig=Both, because the Connection Profile must both answer the call and call back the device requesting access. Similarly, the calling device must be able to both dial out to and accept incoming calls from the MAX.

Requiring a Connection Profile

The Profile Reqd parameter in the Answer Profile affects how the MAX handles bridging and routing calls for which it could find no Connection Profile or third-party authentication profile. This parameter does not affect terminal server calls. The Profile Reqd parameter is shown in Table 2-4.

Table 2-4. Profile required parameter

Location	Parameter
Ethernet→Answer	Profile Reqd=Yes

If the MAX doesn't find a matching Connection Profile or third-party authentication profile for the incoming call, it checks the Answer Profile.

If the call is PPP-encapsulated and Recv Auth is *not* set to None, or if it is a Combinet call and Passwd Reqd=Yes, the call is rejected.

If the call is PPP-encapsulated and both Recv Auth=None and Profile Reqd=No, or if it is a Combinet call and both Passwd Reqd=No and Profile Reqd=No, the MAX attempts to set up the parameters of the session using the information specified in the Answer Profile.

PPP authentication using PAP or CHAP

PPP and MP+ calls can use PAP or CHAP authentication provided that both sides of the connection support the same protocol (PAP, CHAP, or both).

PAP provides a simple way for a peer to establish its identity in a two-way handshake when initially establishing a link. It sends passwords in the clear, so it is not a very strong

authentication method. PAP provides baseline security when your system interoperates with non-Ascend equipment.

CHAP is a stronger authentication method than PAP. During the establishing of the initial link, CHAP verifies the identity of a peer through a three-way handshake. It sends passwords encrypted by means of a one-way hash function. CHAP's use of an incrementally changing identifier and a variable challenge value protects against playback attack.

Table 2-5 lists the parameters related to authentication of incoming PPP calls in a Connection Profile, See the *MAX RADIUS Supplement* for information on configuring these parameters in a users file.

Table 2-5. Authentication parameters for incoming PPP or MP+ calls

Location	Parameter
Ethernet→Connections→*any profile*	Station=[] Encaps=PPP or MP+
Ethernet→Connections→*any profile*→ IP options...	LAN Adrs=0.0.0.0
Ethernet→Connections→*any profile*→ Encaps options...	Recv PW=[]
Ethernet→Connections→*any profile*→ Telco options...	AnsOrig=Both (or Ans Only)
Ethernet→Answer	Profile Reqd=Yes
Ethernet→Answer→PPP options...	Recv Auth=Either (or PAP or CHAP)

For an incoming PPP or MP+ call, the MAX attempts to match the caller's name and password to the Station and Recv PW parameters in a Connection Profile. If it does not find a matching profile, it checks the caller's source IP address and attempts to match it to the LAN Adrs parameter in a Connection Profile.

If Recv Auth is set to PAP or to CHAP, the MAX tries to authenticate the call using the specified protocol. It completes the initial handshake for that protocol, compares the password to the Recv PW parameter, and hangs up if authentication fails. If Recv Auth=Either, the MAX first tries to use CHAP and if the far end of the connection doesn't support CHAP, the MAX uses PAP instead.

Note: RADIUS servers allow CHAP. CHAP is not supported in TACACS.

The AnsOrig parameter specifies whether the MAX can initiate calls, receive them, or both. The MAX will not accept an incoming call if this parameter is set to Call Only.

Table 2-6 lists the parameters related to authentication in outbound PPP calls. See the *MAX RADIUS Supplement* for information on configuring these parameters in a users file.

Table 2-6. Authentication parameters for outbound PPP or MP+ calls

Location	Parameter
System→Sys Config	Name=[]
Ethernet→Connections→*any profile*	Encaps=PPP or MP+

Table 2-6. Authentication parameters for outbound PPP or MP+ calls

Location	Parameter
Ethernet→Connections→*any profile*→ Encaps options...	Send Auth=PAP (or CHAP) Send PW=[] Aux Send PW=N/A
Ethernet→Connections→*any profile*→ Telco options...	AnsOrig=Both (or Call Only)

The strings specified in the Name and Send PW parameters are the name and password used to authenticate the call. These strings must match the Station and Recv PW parameters on the answering device.

The AnsOrig parameter specifies whether the device can initiate calls, receive them, or both. If this parameter is set to Ans Only, no outbound calls will be made.

Combinet authentication

Combinet bridging uses a physical MAC (Media Access Control) address and a password to authenticate calls.

Table 2-7 shows the parameters related to Combinet authentication. See the MAX RADIUS Supplement for information about configuring Combinet authentication in a users file.

Table 2-7. Combinet authentication parameters

Location	Parameter
System→Sys Config	Name=[]
Ethernet→Connections→*any profile*	Station=[] Encaps=COMB Bridge=Yes
Ethernet→Connections→*any profile*→ Encaps options...	Recv PW=*SECURE*
Ethernet→Answer	Profile Reqd=Yes
Ethernet→Answer→Encaps...	COMB=Yes
Ethernet→Answer→COMB options...	Password Reqd=Yes
Ethernet→Mod Config	Bridging=Yes

To authenticate Combinet calls, the MAX first checks the Answer Profile parameters. If COMB=Yes in the Encaps submenu of the Answer Profile, it allows Combinet encapsulation. The MAX then checks the Passwd Reqd parameter in the COMB Options submenu of the Answer Profile.

If the Answer Profile has Passwd Reqd=Yes, the MAX compares the caller's MAC address and password to the Station and Recv PW parameters in a profile. If it finds a match, it accepts the call. If Passwd Reqd=No, it accepts the call based only upon the matching MAC address.

Terminal server call authentication

The MAX can act as a terminal server across serial connections as well as SLIP (Serial Line IP), raw TCP, asynchronous PPP, immediate Telnet, or MAX Link Client connections. This section describes how the MAX authenticates terminal server sessions that are initiated remotely. For information about terminal server sessions initiated locally, see Chapter 1, "MAX System Security."

Authentication of remote terminal server calls uses the parameters shown in Table 2-8.

Table 2-8. Terminal server authentication parameters

Location	Parameter
Ethernet→Connections→*any profile*	Station=[]
Ethernet→Connections→*any profile*→ Encaps options...	Recv PW=[]
Ethernet→Connections→*any profile*→ Telco options...	AnsOrig=Both (or Ans Only)
Ethernet→Mod Config→TServ options...	TS Enabled=Yes Passwd=*SECURE* (a password) Initial Scrn=Cmd Security=Full

Terminal server authentication is two-tiered. The first level is the Passwd parameter in the TServ Options submenu of the Ethernet Profile (Mod Config menu). The second level is the name and password specified in the caller's Connection Profile.

When the caller initiates a terminal server session, the MAX checks the Security parameter in the TServ Options submenu of the Ethernet Profile. If Security=None or if Security=Partial and Initial Scrn=Menu, the MAX skips the first level of authentication and attempts to verify the caller by using the Connection Profile information.

If Security=Full or if Security=Partial and Initial Scrn=Cmd, the MAX compares the password to the Passwd parameter in the TServ Options submenu. If the caller enters the wrong password, the MAX hangs up. If the caller enters the proper password or if no password is assigned to the Passwd parameter, the MAX attempts to verify the caller by using the Connection Profile information.

If the incoming call is PPP-encapsulated, the MAX authenticates the call as described in "PPP authentication using PAP or CHAP" on page 2-5. Terminal server authentication does not apply to PPP or MP+ calls.

Integrating the MAX with third-party servers

The MAX can communicate with RADIUS or TACACS authentication databases on a local or remote IP network. These third-party authentication methods provide a way to vastly increase the number of authentication entries that can be supported within the MAX. Without RADIUS or TACACs, the number of authentication entries is limited by the number of Connection Profiles supported in the MAX.

When it interacts with a third-party server, the MAX is a NAS (network access server). The NAS is the device that requests a RADIUS or TACACS service, such as authenticating a user.

In this context, a user attempting to open a connection to your MAX is a client of your MAX, your MAX is a client of the third-party server.

For Ascend specifics related to RADIUS servers, see the *MAX RADIUS Supplement*.

RADIUS servers

RADIUS is a protocol that enables access to secure networks through a centrally managed server. The same information stored in Connection Profiles can be stored instead in a flat ASCII or indexed (DBM) database served by a RADIUS daemon.

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

Your MAX can use the data from the RADIUS database not only to authenticate incoming calls but also to create and advertise static routes and to place outbound calls.

RADIUS provides standard access to these external authentication servers:

- Security Dynamics ACE server
- Enigma Logic SAFEWORD server
- UNIX host password database

Note: Although call authentication alone can be configured using most RADIUS daemons, many features, such as logout accounting, are available only when the Ascend version of the RADIUS daemon is running. We strongly recommend that you download and install the Ascend version of the RADIUS daemon, as well as its required dictionary file, if you intend to use RADIUS authentication for connections managed by the MAX.

TACACS servers

TACACS is a simple query/response protocol that enables the MAX to check a user's password and enable or prevent access. TACACS supports PAP (Password Authentication Protocol), Combinet name and password validation, and terminal server validation.

Note: TACACS does not support CHAP.

Configuring the MAX to communicate with RADIUS or TACACS

To configure the MAX to communicate with a RADIUS or TACACS server, you must set the parameters shown in Table 2-9.

Table 2-9. RADIUS or TACACS parameters

Location	Parameter
Ethernet→Mod Config→Auth...	Auth=RADIUS Auth Host #1=10.0.0.*x* Auth Host #2=10.0.0.*x* Auth Host #3=10.0.0.*x* Auth Port=800 Auth Timeout=1 Auth Key=[] (RADIUS only) Auth Pool=No (RADIUS only) Auth Req=Yes (RADIUS only)

The Auth parameter specifies the type of authentication server. If it is set to None, (the default) no authentication servers are supported. The other options are TACACS, RADIUS, and RADIUS/LOGOUT (which is RADIUS with logout accounting).

If you select TACACS, RADIUS, or RADIUS/LOGOUT, you must specify at least one server using the Auth Host parameters for your selection to have an effect.

You can specify up to three server addresses, or specify one address in all three parameters to enable the MAX to retry failed requests. The MAX first tries to connect to Auth Host #1. If it does not receive a response within the time specified by Auth Timeout, it retries that address three times. If it receives no response, the MAX sends the authentication request to Auth Host #2 (provided that an address is configured for that host), retrying if necessary. If it fails again to receive a response in the specified timeout period, it sends the request to Auth Host #3 and follows the same procedure there.

The MAX uses the specified UDP Port (Auth Port) to communicate with the Auth Host addresses. The default port for the RADIUS daemon appears in the /etc/services file on the UNIX host on which the daemon is running. The default value for the TACACS daemon is 49.

The Auth Key parameter specifies a RADIUS client password. If the RADIUS server requires a password to answer authentication requests, enter that password here, exactly as it appears in the RADIUS client file. The password is case sensitive.

The Auth Pool parameter determines whether or not the MAX sends the IP address derived from its pool #1 to the RADIUS server when it requests authentication. Auth Pool also determines whether the RADIUS server can change this IP address. For details on dynamic IP address assignment with RADIUS, see the chapter on Configuring the MAX as an IP Router in the *MAX ISP and Telecommuting Configuration Guide*.

The Auth Req parameter specifies whether a response is required from the RADIUS server. It is set to Yes by default. It is intended to for use with CLID authentication, where the MAX must be able to compare the caller's ID before accepting the call. If the MAX makes a request to the RADIUS server for the caller's profile and the request times out, the CLID-authenticated call is rejected. However, if you set Auth Req=No and the RADIUS query times out, the MAX will accept the connection even though CLID Auth=Required and the caller's ID has not been verified. (It is assumed that a second level of authentication will be performed.) If the call is not CLID-authenticated (if CLID Auth=Prefer or Ignore), this parameter is ignored.

Password aging and expired RADIUS passwords

The Ascend RADIUS daemon supports password aging and expiration as well as a method for enabling dial-in users to replace expired passwords under certain conditions. For details on

specifying password aging and expiration in a user profile, see the section on Passwords in the Getting Started chapter of the *MAX RADIUS Supplement*.

Note: Do not attempt to reset expired passwords with the Livingston radpass utility, which is incompatible with the Ascend RADIUS daemon. Only the Ascend RADIUS daemon or another daemon that supports Ascend password-expiration specifications enables dial-in users to replace expired passwords. The Livingston daemon or other daemons that do *not* support Ascend password-expiration specifications usually cannot even report password expiration; instead the notification reports password failure. Some RADIUS daemons that report password expiration still do not support the Ascend method of replacing passwords.

When the server is running the Ascend RADIUS daemon and has been configured for expired passwords, a dial-in user can replace expired passwords under these conditions:

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

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

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

If the incoming call meets these conditions, this is what happens when the user attempts to establish a terminal server connection associated with an expired password:

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

   If the new password is null or matches the old password, the prompt repeats.

   If the new password is valid (if it does not have too many characters), the MAX asks the user to re-enter the password for confirmation. If the two entries do not match, the MAX prompts again for a new password.
3. After receiving a valid confirmation of the new password, the MAX contacts the RADIUS server for acceptance of the new password.

   If the RADIUS server allows 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 may reject the password change for any of these reasons:

   – The RADIUS daemon was not invoked with the -p option to allow password change.

   – The file system in which the RADIUS users file resides is full so the entry cannot be updated.

   – The RADIUS users file is locked against writing.

   – The RADIUS daemon is running in DBM mode (through a database engine).

     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 is allowed only after you rebuild the RADIUS database with the modified users file containing the new password.

Security Card Authentication

3

This chapter covers these topics:

How security cards work 3-2

Supporting incoming security card calls 3-3

Supporting outbound security card calls 3-6

How security cards work

A secure network site can be set up to change its password very frequently, many times a day. For these secure sites, the MAX is a NAS (network access server). The NAS is the device that requests a RADIUS service, such as authenticating a user. In the context of a security card environment, a user attempting to open a connection to your MAX is a client of your MAX, your MAX is a client of the RADIUS server, and the RADIUS server is a client of an external authentication server, such as a Security Dynamics (ACE) or Enigma Logic (SAFEWORD) server.

The ACE or SAFEWORD server syncs up with hand-held personal security cards (devices the size and shape of a credit card) to provide users with the current password in real-time. The LCD on the users' security cards displays the current, one-time-only password required to gain access at that moment to the secure network.

An example security card environment is shown in Figure 3-1. It includes a calling unit, such as an Ascend Pipeline, a NAS (the MAX), a RADIUS server, and an ACE or SAFEWORD server.

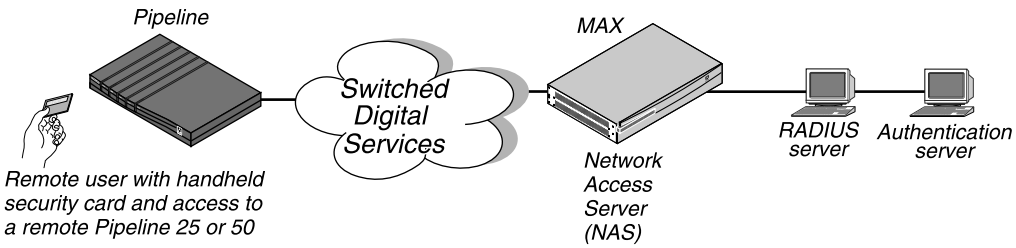


Figure 3-1 Security card environment

This is how security-card passwords are authenticated:

1. A connection is initiated from a calling unit, such as an Ascend Pipeline, to a NAS (the MAX).
2. The NAS requests authentication of the call from the RADIUS server.
3. The RADIUS server forwards the request to the ACE or SAFEWORD server.
4. The ACE or SAFEWORD server sends a challenge message (which may confirm a null challenge) back through the RADIUS server and the NAS to the Pipeline that's dialing in.
5. A user on the dialing network, who may be at the Pipeline console in a terminal server session or using the APP Server utility at a UNIX or Windows host, sees the challenge message and obtains the current password from his or her security card.
6. The user enters the current password obtained from the security card in response to the challenge message.

   If 60 seconds or more pass without a response, the call is dropped.

   If the user enters the correct password, network access is established.

   If the user enters an incorrect password, the ACE or SAFEWORD server returns another challenge (a maximum of three challenges is possible) and the user has another 60 seconds to enter the correct password. After three incorrect entries, or if 60 or more seconds pass per challenge without a response, the call is terminated.

Note: See "Supporting outbound security card calls" on page 3-6 for details on how users with security cards respond to password authentication challenges.

Supporting incoming security card calls

This section describes how to configure the MAX as a NAS to support security card authentication for incoming calls from dial-in users. It also includes an overview of the RADIUS attributes that directly affect how security cards are handled. It does not describe how to configure an ACE or SAFEWORD server.

Configuring the MAX for incoming security card calls

To handle incoming security card passwords from dial-in users, the MAX must forward those authentication requests to RADIUS, which in turn forwards them to an ACE or SAFEWORD server. So, you must configure the MAX to communicate with the RADIUS server. For example, to communicate with a RADIUS server running on the IP host 10.23.45.1, the configuration in the Auth submenu of the Ethernet Profile would look similar to this:

```
Edit
90-900 Mod Config
 Auth...
 >Auth=RADIUS
  Auth Host #1=10.23.45.1
  Auth Host #2=10.23.45.1
  Auth Host #3=10.23.45.1
  Auth Port=800
  Auth Timeout=1
  Auth Key=
  Auth Pool=No
  Auth Req=Yes
```

See "RADIUS servers" on page 2-9 of this Supplement for more details.

In addition, the caller who has a security card must have a valid RADIUS profile in the users file. See the next section for more information.

Setting RADIUS attributes for security card authentication

The first step in setting up RADIUS for security card authentication is to make sure the server is running the most recent version of the Ascend RADIUS daemon. We strongly recommend that you download and install the latest version of the RADIUS daemon *and its dictionary file* from ftp.ascend.com. The RADIUS archive is located within the Software Releases directory.

For background information on configuring attributes in a RADIUS users file, see the *MAX RADIUS Supplement*.

RADIUS attributes for token passwords

These are the relevant RADIUS attributes:

- Password

  The profile must specify the reserved password from an ACE or SAFEWORD server.

  For an Enigma Logic server, the reserved password is SAFEWORD.

  For a Security Dynamics server, the reserved password is ACE.

- Ascend-Token-Expiry

  This attribute sets the lifetime of a cached token—that is, the lifetime of the hand-held security card authentication.

  When the cached token is still alive, subsequent CACHE-TOKEN authentication requests from the same user (for example, when a channel is added to the call) are authenticated by CHAP using the cached token. When the cached token has expired, CACHE-TOKEN authentication requests are authenticated through the ACE or SAFEWORD server.

  See Ascend-Token-Idle, next, for related information.

- Ascend-Token-Idle

  This attribute sets the maximum length of time in minutes a cached token can remain alive between authentications. If this attribute is not specified, the cached token remains alive until Ascend-Token-Expiry causes it to expire.

  This attribute is useful for enforcing authentication when a connection is brought up again after an idle period.

- Ascend-Token-Immediate

  This attribute establishes how RADIUS treats the password received from a login-user when the user's profile specifies an ACE or SAFEWORD server.

  If it is set to zero (No), the initial password received from the user is ignored.

  Choose this value for ACE or SAFEWORD servers that issue a challenge that must be entered by the user in his or her security card before deriving a password.

  If it is set to one (Yes), the initial password received from the user is sent to the ACE or SAFEWORD server for authentication.

Setting an authentication mode in the users file

The calling unit is configured to support one of three authentication modes, but it is the RADIUS profile and daemon that determine which mode will actually be used. See "Setting up a dial-out connection to a secure site" on page 3-6 for information about the dial-in configurations. See the *MAX RADIUS Supplement* for more details about RADIUS options and configurations.

- PAP-TOKEN

  PAP-TOKEN mode is the default. The RADIUS profile must have a password of ACE or SAFEWORD, as shown immediately below in an example profile for a device named "ascend3."

  ```
  ascend3 Password="ACE",
  User-Service=Framed-User,
  Framed-Protocol=MPP,
  Framed-Address=10.0.3.2,
  Framed-Netmask=255.255.255.0
  ```

  See "Requesting PAP-TOKEN mode" on page 3-6 for more information.

- PAP-TOKEN-CHAP

  When the call requests PAP-TOKEN-CHAP, the RADIUS profile must have a password of ACE or SAFEWORD, and the Ascend-Receive-Secret attribute must be set to the same password as the Aux Send PW parameter in the calling profile ("b5XSAM" in the example below).

  The following example shows a profile for a device named "ascend7". It uses a SAFEWORD server and allows PAP-TOKEN-CHAP authentication. The incoming call is assigned the IP address 10.0.200.1 with the netmask 255.255.255.0.

```
ascend7 Password="SAFEWORD"
User-Service=Framed-User,
Framed-Protocol=MPP,
Framed-Address=10.0.200.1,
Framed-Netmask=255.255.255.0
Ascend-Receive-Secret=b5XSAM
```

See "Requesting PAP-TOKEN-CHAP mode" on page 3-7 for related information.

- CACHE-TOKEN

  CACHE-TOKEN uses 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.

  The RADIUS profile must have a password of ACE or SAFEWORD.

  In addition, the Ascend-Receive-Secret attribute must set to the same password as the Send PW parameter in the calling profile ("shared-secret" in the example below) and the Ascend-Token-Expiry attribute must set to a value other than zero (90 minutes in the example below),

  The following example shows a user profile for a device named "ascend5". It allows CACHE-TOKEN authentication with a 90-minute token cache, and uses an ACE server.

  ```
  ascend5 Password="ACE", Ascend-Token-Expiry=90
  Ascend-Receive-Secret="shared-secret",
  User-Service=Framed-User,
  Framed-Protocol=MPP,
  Framed-Address=10.0.3.2,
  Framed-Netmask=255.255.255.0
  ```

  Notice that the Ascend-Token-Expiry attribute must be placed on the first line of the entry, along with the user-name and ACE or SAFEWORD password. If an ACE or SAFEWORD entry exists but the value of Send PW in the calling profile does not match Ascend-Receive-Secret, the call is rejected. Similarly, if the Ascend-Token-Expiry is not in the users file entry or is set to 0, the call is rejected.

  See "Requesting CACHE-TOKEN" on page 3-7 for related information.

Sample RADIUS user profiles

The following RADIUS profile provides authentication through a SAFEWORD server:

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

This profile provides authentication using a SAFEWORD server with token caching for 90 minutes:

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

The following example profile provides authentication using an ACE server with token caching for 540 minutes (9 hours) and an idle time of 80 minutes. ("Idle" means without a new call authentication, *not* without a call being up.) This example caches tokens all day and allows a lunch break as long as it doesn't exceed 80 minutes:

```
ascend5 Password = "ACE", Ascend-Token-Expiry = 540,
Ascend-Token-Idle = 80
Ascend-Receive-Secret = "shared secret", User-Service = Framed-User,
Framed-Protocol = PPP,
Framed-Address = 10.0.3.1,
Framed-Netmask = 255.255.255.0
```

The next profile provides authentication using an ACE server with no challenge. The dynamic password is entered in place of the usual “static” password (which means that the profile is useful only for modem dial-in calls).

```
ascend6 Password = "ACE", Ascend-Token-Immediate = Tok-Imm-Yes
User-Service = Login-User,
Login-Service = Telnet,
Login-Host = 10.0.4.1
```

Supporting outbound security card calls

Most sites use the MAX as a NAS for incoming security card calls. However, you can also configure the MAX as the calling unit, to allow security card users on the local network to call out to a NAS at a secure site.

The instructions in this section explain how to configure the MAX to place calls to a remote NAS and to handle password challenges when they are returned from the NAS.

There are two ways for a user to respond to the password challenges presented by the NAS from an ACE or SAFEWORD server. (1) A user can enter the security-card token from a terminal server session using password mode, or (2) a user can enter the token from a Windows or UNIX host running the APP Server utility. In either case, the idea is the same. One session window on the calling side displays password challenges and allows the user to type in the appropriate response. Only one host on the network can run the APP Server utility.

Setting up a dial-out connection to a secure site

For the MAX to place calls to a NAS at a secure site, it needs the appropriate Connection Profile specifying a token-based authentication mode.

The authentication mode configured in the calling unit affects how the token passwords are transmitted and how the dial-in user is affected by channels being added to an established session.

The calling unit requests the authentication mode with which it is configured, but the RADIUS daemon and user profile accessed by the answering NAS determine which mode will actually be used. See “Setting an authentication mode in the users file” on page 3-4 for related information.

Requesting PAP-TOKEN mode

PAP-TOKEN is the default authentication mode used when the RADIUS profile has a password of ACE or SAFEWORD. It is an extension of PAP authentication.

When PAP-TOKEN mode is in use, the dynamic password supplied by a user is sent in the clear (via PAP), but because it’s a one-time-only password, this is not a serious security risk.

The response to the initial password challenge authenticates the base channel of the call. If bandwidth requirements cause another channel to come up, the user is challenged for a password whenever a channel is added to a call.

These are the parameters to configure in the calling unit for PAP-TOKEN:

Table 3-1. PAP-TOKEN parameters

Location	Parameter
Ethernet→Connections→*any profile* → Encaps options...	Send Auth=PAP-TOKEN Send PW=*SECURE* (a password)

The Send Auth parameter specifies the authentication mode requested by the caller (PAP-TOKEN). The Send PW password is sent as part of the initial session negotiation. If the session then presents a password challenge, the user types in their current one-time-only password obtained from the security card in response to that challenge.

Requesting PAP-TOKEN-CHAP mode

If PAP-TOKEN-CHAP is specified in the calling unit, but the RADIUS profile at the far end is not set up for PAP-TOKEN-CHAP, PAP-TOKEN will be used instead.

PAP-TOKEN-CHAP authenticates additional channels using CHAP.

The dynamic password supplied by a user is used to authenticate the base channel of the call. It is sent in the clear (via PAP). When the MAX adds additional channels to the base channel of the call, PAP-TOKEN-CHAP uses CHAP authentication for the new channels. CHAP sends encrypted passwords, so it can take the auxiliary password from the Aux Send PW parameter and transmit it securely.

These are the parameters to configure in the calling unit:

Table 3-2. PAP-TOKEN-CHAP parameters

Location	Parameter
Ethernet→Connections→*any profile* → Encaps options...	Send Auth=PAP-TOKEN-CHAP Send PW=*SECURE* (a password) Aux Send PW=*SECURE* (a password)

The Send Auth parameter specifies the authentication mode requested by the caller (PAP-TOKEN-CHAP in this case). The Send PW password is sent as part of the initial session negotiation. If the session then presents a password challenge, the user types in their current one-time-only password obtained from the security card in response to that challenge.

The Aux Send PW parameter is sent via CHAP for authenticating additional channels.

Requesting CACHE-TOKEN

CACHE-TOKEN uses CHAP and caches the initial password for re-use in authenticating channels as they are added to the call. The RADIUS profile at the far end must be set up with appropriate attributes that specify how long the token will be cached.

These are the parameters to be configured in the calling unit:

Table 3-3. CACHE-TOKEN parameters

Location	Parameter
Ethernet→Connections→*any profile* → Encaps options...	Send Auth=CACHE-TOKEN Send PW=*SECURE* (a password)

The Send Auth parameter specifies the authentication mode requested by the caller (CACHE-TOKEN). The Send PW password is sent as part of the initial session negotiation. Then, the user is prompted for a token password to authenticate the base channel of the call via CHAP. If the RADIUS server has been configured correctly, it caches that encrypted password for the specified period, or for the specified amount of idle time during the connection. When channels are added to the call or when a new call is made, it uses the cached password to authenticate them.

Configuring a connection with a local APP Server utility

To allow users to supply token passwords from a PC or UNIX host on the local network, you must configure the MAX to communicate with the APP Server utility on that host. APP is a UDP protocol whose default port is 7001. The communication between the MAX and the host running the APP Server may be unicast (when both the MAX and the host have an IP address) or broadcast (when the host may not have an IP address).

The APP parameters are shown in Table 3-4.

Table 3-4. APP Server-specific parameters

Location	Parameter
Ethernet→Mod Config→Auth...	APP Server=Yes APP Host=10.65.212.1 APP Port=7001

- APP Server

  Set this parameter to yes to enable the MAX to communicate password challenges to the host running the APP Server utility.

- APP Host

  Specify the IP address of the host running the APP Server utility on the local IP network. 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 in this parameter (255.255.255.255).

- APP Port

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

Invoking password mode in the terminal server

A user can bring up a connection to the secure site in the usual way: by invoking a program that requires a connection to a host on that remote network, by using the DO menu in the MAX, or by dialing the remote NAS via modem.

Note: If the connection is brought up by modem, the process of responding to password challenges begins at Step 2, below.

Users can invoke password mode in a terminal server session by following these steps:

1. At the terminal server prompt, the user types:

   ```
   set password
   ```

   The following message is displayed:

   ```
   Entering Password Mode...
   ```

   The prompt changes to the following:

   ```
   [^C to exit] Password Mode>
   ```

2. The user brings up the connection.
3. While the connection is being negotiated, the remote NAS returns a challenge prompt that looks like this:

   ```
   From: hostname
   0-Challenge: challenge
   Enter next password:
   ```

4. The user enters the password obtained from his or her security card at the challenge prompt.

   A user has 60 seconds to enter the password correctly. If the password is entered correctly, the connection is established to the secure network. If the password is not entered within 60 seconds, the login attempt times out. If the password is entered incorrectly, the challenge prompt is displayed again up to three times.

   hostname is the name of the NAS called, such as the MAX, and it is optional on some systems. If the Send Auth parameter is configured incorrectly, no challenge prompt appears, or the user sees and error message such as this:

   ```
   From: hostname
   Received unexpected PAP Challenge!... check PPP Auth Mode
   ```

5. To return to normal terminal server operations, the user presses CTRL-C at the Password Mode prompt.

Using the APP Server on a UNIX host

The APP Server utility for UNIX enables a user to respond to token password challenges received from a remote NAS. You can download this utility from ftp.ascend.com.

This section describes how to install and run the APP Server utility on a UNIX host. When a user on the LAN starts an application that requires a connection to a host on a secure network, the MAX initiates a call transparently (as usual). After the initial session negotiation, the remote NAS returns a password challenge that looks similar to this:

```
From: hostname
0-Challenge: challenge (or null challenge, depending on your setup)
Enter next password:
```

This prompt is displayed in the APP Server screen on the UNIX host. A user has 60 seconds to obtain the current dynamic password from the security card and enter it correctly. If the password is entered correctly, the connection is established to the secure network. If the password is not entered within 60 seconds, the login attempt times out. If the password is entered incorrectly, the challenge prompt is displayed again up to three times.

To install and run the APP Server utility on a UNIX host, follow these steps:

1. Download the APP Server files from ftp.ascend.com to the UNIX host.
2. Decompress (gunzip) and separate (tar) the files.
3. Edit the Makefile appropriately for your operating system and compiler.
4. Compile the appsrvr source file (make).
5. Add a line to /etc/services assigning UDP port 7001 to the appServer.

   If you can use the default port 7001 (if it is not already assigned), add this line to /etc/services to document that the port is now in use:

   appServer<tab>7001/udp

   If port 7001 is already assigned to a different purpose, you can use a different port for the APP Server utility by adding a line such as this to the services file:

   appServer<tab>*nnn*/udp

   where *nnn* is the port number to be used. Make sure that the MAX configuration agrees with this number (see "Configuring a connection with a local APP Server utility" on page 3-8).
6. If the UNIX host has an IP address, you can run the utility in unicast mode by typing this command at the UNIX prompt:

   ./appsvr

   When you run the utility in unicast mode, it transmits packets on the specified UDP port with the source address set to its own IP address. When the MAX receives those packets on the specified UDP port, it returns packets to that IP address.
7. If the UNIX host does *not* have an IP address (for example, if it obtains its address from a BOOTP or DHCP server), run the utility in broadcast mode instead by typing this command:

   ./appsrvr –b

   The –b option sets a socket option to allow broadcast transmissions and inhibits the utility's complaints about receiving invalid APP frame types when it receives when it receives its own transmissions.

Note: On some UNIX systems, you need root privileges to run the APP Server utility in broadcast mode. (Some hosts disallow broadcast transmissions without root privileges.) If you are running the utility in broadcast mode, make sure that the MAX is configured with the broadcast address in the APP Host parameter (APP Host=255.255.255.255).

Using the APP Server utility on a DOS or Windows host

The APP Server utility for Windows or DOS enables a user to respond to token password challenges received from a remote NAS. You can download the utility from ftp.ascend.com.

This section describes how to install and run the APP Server utility on a PC running Windows or DOS. When a user on the LAN starts an application that requires a connection to a host on the secure network, the MAX initiates a call transparently (as usual). After the initial session negotiation, the remote NAS returns a password challenge.

If the PC is running DOS, the password challenge looks similar to this:

```
Ascend Password Server Module vX.X
Requester: hostname
Request: challenge (or null challenge, depending on your setup)
Enter password:
```

If the PC is running Windows, the challenge is displayed in the AppServer window. It has the same fields as the DOS prompt shown immediately above, but it is in a graphic format.

Two APP Server executables are available for PC-compatible systems:

- APPSRVR1.EXE

  This program provides a "one-shot" authentication mechanism that occurs only when the PC is booted. It does not require an IP address or TCP/IP stack in the DOS system.

  APPSRVR1.EXE is executed from AUTOEXEC.BAT as part of system startup. It can be used to authenticate a connection that has begun transparently or it can bring up a connection to the remote NAS.

  APPSRVR1.EXE builds an IP header and sends broadcast packets via the ODI driver to the MAX, passing it the name and IP address of a Connection Profile. The MAX must be configured with the broadcast address in the APP Host parameter (APP Host= 255.255.255.255).

- APPSRVR2.EXE

  This program is a Windows application. It can be used to authenticate a connection that has begun transparently or it can bring up a connection to the remote NAS.

  APPSRVR2.EXE is typically launched at system startup and remains open on the Windows system. You can launch it manually by double-clicking its icon, or include it in the Startup group. It has a Connect button for initiating a connection, and will prompt for a password when it is needed.

Installing the APP Server utility for DOS

To provide authentication from a DOS system, install only APPSRVR1.EXE. Users must reboot the PC to initiate a connection to the secure network.

Note: APPSRVR1.EXE does not require an IP stack or IP address, but it does require an ODI driver.

1. Create an \ASCEND directory below the root directory.
2. Copy APPSRVR1.EXE into that directory.
3. Open AUTOEXEC.BAT and add a command line invoking APPSRVR1.EXE.

   The command line for APPSRVR1.EXE must be positioned after the line invoking the network ODI driver and *before* the network protocol stack (TCIP or IPX or other supported protocol). For example:

   ```
   C:\NOVELL\LSL.COM
   C:\NOVELL\XXXODI.COM
   C:\ASCEND\APPSRVR1.EXE
   REM Protocol Stack is loaded next
   ```

The APPSRVR1.EXE command line can include the options shown in Table 3-5.

Table 3-5. Options for the APPSRVR1.EXE command line

Option	Effect
`/tss`	Set seconds between connection attempts, where *ss*=number of seconds (example: t135; default: 20 secs.)
`/ykk`	Set number of times the PC attempts to connect before timeout, where *kk*=number of attempts (example: y4)
`/mxx`	Set host MAC address in decimal format, where *xx*=MAC address in decimal format of the PC running appsrv1 (default: zero)

Table 3-5. Options for the APPSRVR1.EXE command line

Option	Effect
`/pmm`	Set UDP port number (mm—default: 7001). See the note below.
`/bnn`	Set UDP port number (nn) broadcast at startup (default: same port as APPSRVR1.EXE). See the note below.
`/cyy`	Sets name of Connection Profile called on startup. If the Connection Profile is not specified in AUTOEXEC.BAT by using this option, the utility prompts the user for the name of the profile.
`/f`	Suppress call on startup (default: force call on startup)
`/d`	Disconnect call
`/?`	Display APPSRVR1.EXE help screen.

Note: The PC sends a broadcast UDP packet that has the destination and the source port 7001 unless you specify otherwise with the /p or /b options. If you specify a number other than 7001 in the APP Port parameter, you must use one of these options to specify the same port.

Installing the APP Server utility for Windows

To provide authentication under Windows, you can install one or both of the APPSRVR utilities.

- Install APPSRVR1.EXE…

  If the Windows PC does not have a TCP/IP stack, install only APPSRVR1.EXE. Do not install APPSRVR2.EXE, which requires IP.

  You may want to install APPSRVR1.EXE even if the PC has a stack, to enable a user to authenticate a call before Windows has been started.

- Install APPSRVR2.EXE…

  Install this program if the Windows PC has a TCP/IP stack.

To install both programs on the Windows PC, follow these steps:

1. Create an \ASCEND directory below the root directory.
2. Copy APPSRVR1.EXE, APPSRVR2.EXE, and CTL3D.DLL into that directory.

   If you have decided not to install APPSRVR1.EXE, don't copy it into the directory and skip the next step.
3. Open AUTOEXEC.BAT and add a command line invoking APPSRVR1.EXE.

   See "Installing the APP Server utility for DOS" on page 3-11 for details.
4. Create a new program group in your Program Manager.

   Choose File→New→Program Group and type "Ascend".
5. Create an icon for APPSRVR2.EXE in your Program Manager.

   Choose File→New→Program Item.
6. To launch the APP Server utility when you start Windows, place the APPSRVR2.EXE icon in your Startup group.

   If you prefer not to add the APP Server utility to your Startup group, you can launch the utility manually by double-clicking its icon.

A

Answer Profile
- CLID Auth parameter in 2-4
- Combinet authentication in 2-7

APP Server utility 3-8, 3-9
Ascend-Receive-Secret 3-4
Ascend-Token-Expiry 3-4
Ascend-Token-Idle 3-4
Ascend-Token-Immediate 3-4
attributes, RADIUS 3-3
Auth Host parameter 2-10
Auth Key parameter 2-10
Auth parameter 2-10
Auth Pool parameter 2-10
Auth Port parameter 2-10
Auth Req parameter 2-10
Auth Timeout value 2-10
authentication
- CACHE-TOKEN 3-7
- Combinet call 2-7
- for outbound security-card calls 3-6
- PAP/CHAP 2-5
- PAP-TOKEN 3-6
- PAP-TOKEN-CHAP 3-7
- terminal server 2-8

Aux Send PW parameter 3-7

C

CACHE-TOKEN authentication, for incoming calls 3-5
Callback parameters 2-5
Calling Line ID 2-4
calls
- authenticating Combinet 2-7
- authenticating incoming 2-3
- authenticating outbound 3-6
- authenticating terminal server 2-8
- authenticating using PAP and CHAP 2-5
- incoming security card 3-3
- password mode in terminal server 3-8
- rejecting unknown incoming 2-5

CHAP authentication 2-6
Combinet authentication 2-7
command-line interface 1-10
configuration
- for APP Server utility 3-8
- for APP Server utility on DOS 3-11
- for APP Server utility on UNIX 3-10
- for APP Server utility on Windows 3-12
- for incoming security card calls 3-3

Connection Profile 2-5
connection security 2-2

D

DBM authentication database 2-9, 2-11
Default Profile 1-4
dial-in sessions 1-9
DOS, configuring APP server utility for 3-11

E

editing default profile 1-5
expired passwords 2-10

F

Full Access Profile 1-5

I

incoming calls
- authenticating 2-3
- configuring for security card 3-3
- rejecting unknown 2-5
- See also calls

Initial Scrn parameter 1-10
interface protection 1-9
IP addresses, sent to RADIUS server 2-10

L

Livingston daemon 2-11
Livingston radpass utility 2-11

M

MAX
- integrating third-party servers with 2-8
- system security function in 1-2

modifying default profile 1-5

O

outbound call authentication 3-6
- *See also* calls

P

PAP authentication protocol 2-5
PAP-TOKEN authentication
- for incoming calls 3-4
- for outbound calls 3-6

PAP-TOKEN-CHAP authentication
- for incoming calls 3-4
- for outbound calls 3-7

parameters
- AnsOrig 2-6
- APP Server-specific 3-8
- Auth Req 2-10
- Aux Send PW 3-7
- Callback 2-5

parameters (*continued*)
Calling # 2-4
CLID Auth 2-4
COMB 2-7
connection security 2-3
Dial # 2-5
Initial Scrn 1-10, 2-8
Name 2-7
Passwd Reqd 2-7
Profile Reqd 2-5
RADIUS/TACACS authentication 2-9
Recv Auth 2-6
Recv PW 2-6
Remote Mgmt 1-8
Security 2-8
Security Profile 1-3
Send Auth 3-7
Send PW 2-7, 3-7
Station 2-6
system security 1-2
terminal server authentication 2-8
terminal server security 1-9
Toggle Scrn 1-10
Password attribute 3-3
passwords
aging/expiration of 2-11
dial-in sessions 1-9
how verified 2-6
RADIUS Client 2-10
SNMP 1-8
Telnet 1-8
terminal server 2-8
PPP-encapsulated call authentication 2-6
Profile Reqd parameter 2-5
profiles
callback in Connection 2-5
modifying Default 1-5
password to Full Access 1-5
setting up security 1-3

R

RADIUS attributes for token passwords 3-3
RADIUS client password 2-10
RADIUS daemon
and password expiration 2-10
obtaining latest Ascend version 2-9
version for security card authentication 3-3
RADIUS servers, integration with 2-9
remote management access 1-8
Remote Mgmt parameter 1-8

S

security cards
configuring for incoming calls 3-3
supporting local users 3-6
Token immediate feature for 3-4
using 3-2
Security Profiles
activating new 1-6
parameters in 1-3
Send Auth parameter 3-7
Send PW parameter 3-7
servers
and expired passwords 2-11
integration with RADIUS 2-9
integration with TACACS 2-9
integration with third-party authentication 2-8
password mode for terminal 3-8
security parameters for terminal 1-9
sessions
password for dial-in 1-9
starting terminal server 1-7
SNMP passwords 1-8
system security
activating levels in 1-6
for Telnet 1-9, 1-10
parameters for 1-2
setting up profiles 1-3

T

TACACS server integration 2-9
Telnet
passwords for 1-9
security for 1-10
Terminal server calls
authentication for 2-8
See also calls
terminal servers
security parameters for 1-9
See also servers
using password mode 3-9
third-party servers 2-8
See also servers
Toggle Scrn parameter 1-10
token
lifetime 3-4
lifetime on idle connections 3-4
Token immediate feature 3-4

U

UDP port for APP Server 3-8, 3-10, 3-12
UNIX system 3-9
unknown incoming calls 2-5