MAX 200Plus Security Supplement

Ascend Communications

Part Number 7820-0422-002 July 2, 1997

Contents

Figures

Tables

About This Supplement

What this supplement contains

This supplement is intended for the person setting up security on the MAX. It explains how to set up different kinds of security options using the MAX configuration interface, and contains the following chapters:

- Chapter 1, “Getting Started with Basic Security,” details recommended changes to default security settings to protect the MAX from unauthorized access.
- Chapter 2, “Setting Up Security Profiles,” describes security levels for the MAX and explains the privileges you can set in Security profiles.
- Chapter 3, “Setting Up User Authentication,” explains how to identify and permit access to users dialing in over both analog and digital lines.
- Chapter 4, “Creating Data Filters,” details how to set up data filters and call filters.
- Chapter 5, “Setting Up Security-Card Authentication,” describes how the MAX supports dynamic password challenges sent from an external authentication server at a secure site.
- Chapter 6, “Setting Up User Authorization,” describes how to limit user access to network devices, resources, and services.

This supplement also contains an index.

What this supplement does not contain

This supplement does not describe how to set up security in RADIUS, how to use the Access Control product, or how to set up the MAX to work with firewalls and the Secure Access product. Further, it does not discuss general network security issues or provide guidelines about the extent to which you should protect your network and local hosts. For pointers to information about these products and topics, consult Table 1.

Table 1 Where to go for additional security information

Topic	**Publication**
RADIUS	MAX *RADIUS Configuration Guide*
Access Control	*Access Control User’s Guide*
Firewalls and Secure Access	*Secure Access Manager User’s Guide*
Detailed discussion of security issues	We recommend Firewalls and Internet Security by William R. Cheswick and Steven M. Bellovin

What you should know

This supplement is intended for the person who will be setting up security in the MAX. It does not discuss general network security issues, or provide guidelines for protecting your network and local hosts. To use this book effectively, however, you should be familiar with network security. For background information about security, we recommend the following publication, which is available in bookstores:

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

RADIUS and other external servers offer additional methods for handling security. For more information about RADIUS, see the *RADIUS Supplement*.

Ascend's Access Control is a software program that provides authentication, authorization, and accounting services for users who request network connections. For more information about Access Control, see the *Access Control User's Guide*, available from Ascend.

Documentation conventions

This guide uses the following documentation conventions:

Table 2 Documentation conventions

Convention	Meaning
`Monospace text`	Represents text that appears on your computer's screen. Signifies a command or file name in some manuals. In most Ascend manuals, command and file names are simply capitalized, just like any other name. But if your manual includes names that are case sensitive on some platforms, they are not capitalized. Instead, they are shown in a monospace typeface.
`Boldface mono-space text`	Represents characters that you enter exactly as shown (unless the characters are also in ***`italics`***—see *Italics*, below).
`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 and to show emphasis.
[ ]	Square brackets indicate an optional attribute that you append to a command. To include an attribute, type only the information inside the brackets. Do not type the brackets unless they appear in bold type.
|	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 the parameter that precedes the angle bracket is selected.

Table 2 Documentation conventions (continued)

Convention	Meaning
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.

Related publications

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

Here are some related publications that you might find useful:

- *Firewalls and Internet Security*, William R. Cheswick and Steven M. Bellovin
- *The Guide to T1 Networking*, William A. Flanagan
- *TCP/IP Illustrated*, W. Richard Stevens

Getting Started with Basic Security

1

This chapter describes how to set up basic security on the MAX, and covers these topics:

Introducing Security profiles

A Security profile consists of parameters you can set to control access to the MAX. All Security profiles are located below the Security menu of the System profile in the MAX configuration interface.

```
00-300 Security
>00-301 Default
 00-302
 00-303
 00-304
 00-305
 00-306
 00-307
 00-308
 00-309 Full Access
```

Two profiles are provided on all MAX units:

- Full Access

  The Full Access Security profile provides full access to the MAX unit. It is the "super-user" profile that enables you to configure your system, dial remote locations, reset the unit, and upgrade system software.

  A user who knows the password for the Full Access profile can perform any operation on the MAX. The default Full Access password is "Ascend". You should change the Full Access password as soon as possible. For details, see "Changing the Full Access password" on page 1-3.

- Default

  The MAX assigns the Default profile to every user who logs in via Telnet, the Control port, and remote management. The MAX activates the Default profile whenever the MAX powers on or resets. The privileges set in the Default profile are available to all users. You cannot change the name of the Default profile or assign a password to it. However, you can change its settings to make the profile more restrictive. For details, see "Setting the Default profile for read-only access" on page 1-4.

Note: We strongly recommend that you follow the instructions in "Changing the Full Access password" on page 1-3 and "Setting the Default profile for read-only access" on page 1-4. These instructions result in two security levels, one that is totally open (Full Access) and one that is totally restrictive (Default).

If you are the only user who must configure the MAX or perform administrative tasks, you do not need to create any Security profiles in addition to the ones provided. However, many sites choose to define additional security levels and enable certain users to perform a subset of administrative functions. You can create up to seven additional Security profiles. For more information on these tasks, see Chapter 2, "Setting Up Security Profiles."

Understanding basic security measures

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. Their default security settings enable you to configure and set up the MAX without any restrictions. Before you make the MAX generally accessible, you should change these default security settings to protect the configured unit from unauthorized access. These are the steps you must carry out:

1. Change the Full Access password.
2. Activate the Full Access profile
3. Set the Default profile for read-only access.
4. Change the SNMP read-write community string.
5. Assign a Telnet password.
6. Require profiles for incoming connections.
7. Turn off ICMP redirects.

Each section that follows describes each of these steps.

Changing the Full Access password

The Full Access Security profile is the "super-user" profile that enables you to configure your system, dial remote locations, reset the unit, and upgrade system software. This profile is intended to remain totally open, with all privileges set to Yes. The default password assigned to the profile is "Ascend". A user who knows the password for the Full Access profile can perform any operation on the MAX.

Change the default password as soon as possible. D*o not* turn off the Edit Security privilege in the Full Access profile, or you will be unable to edit privileges when you activate Full Access.

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

1. Open the System > Security menu.
2. Open the Full Access profile.
3. When prompted, enter the default password:
   `Ascend`
   Passwords are case-sensitive. You must enter the password exactly as shown.
4. Select the Passwd parameter and press Enter to open a text field.
5. Type a new password for the profile.
6. Press Enter.
   The string "*SECURE*" replaces the letters you typed:

```
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
 Field Service=Yes
```

7 Leave all other privileges enabled.

Caution: Do not turn off the Edit Security privilege!

8 Exit the Full Access profile, saving your changes.

Activating the Full Access profile

You must activate the Full Access profile for your own use in performing the rest of the basic security measures. 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).

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

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

The MAX prompts you for the Full Access password:

```
00-300 Security
Enter Password:
 []

 Press > to accept
```

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

When you enter the correct password, the MAX displays a message informing you that the password was accepted and that the MAX is using the new security level

```
Message #119
Password accepted.
Using new security level.
```

If the password you enter is incorrect, the MAX prompts you again for the password.

Setting the Default profile for read-only access

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 you power on or reset the unit, and whenever a user begins a new login session.

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

To make the Default profile appropriately restrictive, follow these steps:

1 Open the System>Security menu.

2 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.

3 Set Operations=No.

```
00-301 Default
 Name=Default
 Passwd=
>Operations=No
 Edit Security=N/A
 Edit System=N/A
 Edit Line=N/A
 Edit All Ports=N/A
 Edit Own Port=N/A
 Edit All Calls=N/A
 Field Service=N/A
```

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

From now on, users who access the MAX terminal server cannot make any changes to its configuration or to perform restricted operations. For all users with the Default security level, passwords (including the null password) are hidden by the string *SECURE* in the MAX unit's user interface.

4 Exit the Default profile and save your changes.

Changing the SNMP read-write community string

An SNMP community string is an identifier that an SNMP manager application must specify before it can access the MIB (Management Information Base). The MAX has two community strings:

- Read Comm

  The read community string has the value "public" by default. It enables an SNMP manager to perform read commands (get and get next) in order to request specific information.

- R/W Comm

  The read-write community string has the value "write" by default. It enables an SNMP manager to perform both read and write commands (get, get next, and set). Using these commands, the application can access management information, set alarm thresholds, and change settings on the MAX.

You cannot turn off SNMP write, so you must change the default read-write string in order to secure the MAX against unauthorized SNMP access. To change the read-write community string, follow these steps:

1 Open the Ethernet > Mod Config > SNMP Options menu.

2 For the R/W Comm parameter, specify a text string containing up to 16 characters.

For example, you can specify this setting:

```
R/W Comm=unique-string
```

3 Close the SNMP Options menu and save your changes.

Assigning a Telnet password

Until you assign a Telnet password, any local user who knows the MAX unit's IP address can start a Telnet session with the MAX. When you assign a password, all users requesting incoming Telnet sessions, whether locally or from across the WAN, must enter the password.

To assign a Telnet password, follow these steps:

1. Open the Ethernet > Mod Config > Ether Options menu.
2. For the Telnet PW parameter, specify a password containing up to 20 characters.
   For example, you might enter this setting:
   `Telnet PW=telnet-pwd`
3. Close the Ether Options menu and save your changes.

Requiring profiles for incoming connections

You can use the MAX unit's Answer profile to build connections that do not require a name and password. Although some sites allow such connections, most sites impose much tighter restrictions. You should strongly consider limiting incoming connections to those that have a configured Connection profile, Password profile, or RADIUS user profile.

Chapter 3, "Setting Up User Authentication," describes the types of authentication you can configure for incoming connections. At the most basic level, however, you can configure the MAX to reject all incoming connections for which it finds no matching profile.

To require configured profiles for all incoming connections, follow these steps:

1. Open the Ethernet > Answer menu.
2. To specify that a matching profile is required for incoming calls, set Profile Reqd=Yes.

   Note: If you support ARA (AppleTalk Remote Access) connections through the MAX, setting Profile Reqd=Yes disables Guest access to your network.
3. Close the Answer menu and save your changes.

Turning off ICMP redirects

ICMP enables a unit to find the most efficient IP route to a destination. ICMP Redirect packets are one of the oldest route discovery methods on the Internet and one of the least secure; it is possible to counterfeit ICMP Redirects and change the way a device routes packets. If the MAX is routing IP, we recommend that you turn off ICMP redirects.

To configure the MAX to ignore ICMP redirect packets, follow these steps:

1. Open the Ethernet>Mod Config menu.
2. Set ICMP Redirects=Ignore.
3. Close the Mod Config menu and save your changes.

Setting Up Security Profiles

2

This chapter covers these topics:

Understanding Security profile parameters

A Security profile consists of parameters you can set to control access to the MAX. All Security profiles are located below the Security menu of the System profile in the MAX configuration interface. Table 2-1 lists the parameters in a Security profile.

Table 2-1. Security profile parameters

Parameter	Description	Possible values
Name	Specifies a name for the profile.	Text string containing up to 16 characters. The default value is null.
Passwd	Specifies a password.	Text string containing up to 20 characters. The default value is null.
Operations	Enables or disables read-only security.	Yes No The default value is Yes.
Edit Security	Grants or restricts privileges to edit Security profiles.	Yes No The default value is Yes. Do not set this parameter to No for all nine Security profiles. If you do, you cannot edit any of them.
Edit System	Grants or restricts privileges to edt the System profile and the Read Comm and R/W Comm parameters in the Ethernet profile.	Yes No The default value is Yes.
Edit All Calls	Indicates whether an operator can edit all the parameters in all Call profiles and Connection profiles.	Yes No The default value is Yes. No specifies that an operator can edit only the Dial # and Base Ch Count parameters in the current Call profile. To disable editing of the Dial # and Base Ch Count parameters, you must set Edit All Calls=No and Edit Cur Call=No.
Field Service	Grants or restricts privileges to perform Ascend-provided field service operations, such as uploading new system software.	Yes No The default value is Yes.

Configuring a Security profile

To configure a new Security profile, follow these steps:

1. Open the System > Security menu.
2. Open an unnamed profile.
3. For the Name parameter, specify a name for the profile.

   You can enter up to 16 characters. For example, you might specify this setting:

   `Name=Calabasas`
4. For the Passwd parameter, specify a password containing up to 20 characters.

   As soon as you press Enter, the MAX hides the password string you specified by displaying the string `"*SECURE*"`.
5. To enable or disable read-only security, set the Operations parameter.

   Yes enables a user to view MAX profiles and to change the value of any parameter. The default value is Yes.

   No permits a user to view MAX profiles, but not to change the value of any parameter. If you specify No, a user cannot access DO commands other than DO Esc, DO Close Telnet, and DO password.
6. To grant or restrict privileges to edit Security profiles, set the Edit Security parameter.

   Yes grants privileges. When you specify Yes, a user can edit Security profiles, and can access all other operations by enabling them in his or her active Security profile. In addition, all passwords in Security profiles are visible as text. This privilege is the most powerful one you can assign, because it allows users to change their own privileges at will. The default value is Yes.

   No restricts privileges. When Edit Security=No, all passwords are hidden by the string `"*SECURE*."`

   

   Caution: Do not set the Edit Security parameter to No on all nine Security profiles; if you do, you cannot edit any of them.
7. To grant or restrict privileges to edt the System profile and the Ethernet profile, set the Edit System parameter.

   Yes grants privileges to edit the System profile, and to edit the Read Comm and R/W Comm parameters in the Ethernet profile. The default value is Yes.

   No restricts privileges.
8. To grant or restrict privileges to perform Ascend-provided field service operations, such as uploading new system software, set the Field Service parameter.

   Yes grants privileges. The default value is Yes.

   No restricts privileges. Selecting No does not disable access to any MAX operations. Field service operations are special diagnostic routines not available through MAX menus.
9. Close the new Security profile.

Activating a Security profile

When you log into the MAX, you can only view settings, because the Default profile is active. To make any changes or perform any administrative tasks, you must activate the Full Access profile or any other profile configured to allow setup or administrative tasks.

To activate a profile, follow these steps:

1. Press Ctrl-D to open the DO menu
2. Press P, or select P=Password.
3. In the list of Security profiles that opens, select the profile you want to activate.
   The MAX prompts you for the password.
4. Type the appropriate password, and press Enter.
   When you enter the correct password, the MAX displays a message informing you that the password was accepted and that the MAX is using the new security level. If the password you enter is incorrect, the MAX prompts you again for the password.

Using the Full Access profile

The Full Access Security profile is the “super-user” profile that enables you to configure your system, dial remote locations, reset the unit, and upgrade system software. This profile is intended to remain totally open, with all privileges set to Yes. The default password assigned to the profile is “Ascend”. A user who knows the password for the Full Access profile can perform any operation on the MAX.

You should change the default password as soon as possible.

Caution: Do not turn off the Edit Security privilege in the Full Access profile, or you will be unable to edit privileges when you activate Full Access.

These are the default settings for the Full Access profile:

```
Name=Full Access
Passwd=Ascend
Operations=Yes
Edit Security=Yes
Edit System=Yes
Field Service=Yes
```

Setting Up User Authentication

3

This chapter covers these topics:

Introducing user authentication

User authentication is a method of identifying and allowing access to specified remote users dialing in over both analog and digital lines.

For authentication not directly supported by the MAX, see the *MAX RADIUS Configuration Guide*.

What authentication methods does the MAX support?

You can choose from a wide array of authentication methods. The MAX supports the types of authentication described in the following sections.

Name and Password

You can configure the MAX to verify an incoming call based on the user's name and password; you can also specify a name and password for outgoing calls. Name and password authentication applies to these types of calls:

Callback

Callback security instructs the MAX to hang up on an incoming caller and then immediately initiate a call to that destination. For details on configuring the MAX to use callback security, see "Setting up callback security" on page 3-5.

Table 3-1. Call types authenticated by name and password requirements

PPP, MP, and MP+	You can specify PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), or MS-CHAP (Microsoft Challenge Authentication Protocol) authentication for name and password verification of incoming and outgoing PPP, MP, or MP+ calls. For details, see "Setting up authentication of PPP, MP, and MP+ calls" on page 3-7.
Terminal server	You can specify that users logging into the terminal server via a V.34, V.42, or V.120 connection must supply a username and password before gaining admission to the terminal server. See "Setting up remote terminal server authentication" on page 3-14.
ARA	You can specify name and password authentication for AppleTalk callers dialing in using a V.34, V.42, V.120, or X.75 connection. For details, see "Setting up ARA authentication" on page 3-18.
IP Address	You can specify that the MAX authenticate an incoming connection by checking the user's IP address; or, you can specify that the MAX assign an IP address to each incoming call. For details, see "Setting up IP addressing" on page 3-23.

How does user authentication work?

All authentication relies on the MAX finding a matching profile to verify information presented by the caller. The matching Connection profile or Name/Password profile may be resident locally; or, the profile might be managed by a third-party security server such as RADIUS or TACACS

By default, when you require a profile for authentication the MAX always checks for a Connection profile. If a Connection profile does not exist, the MAX checks for a remote RADIUS 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 first looks for a remote profile. If it cannot find one, the MAX looks for a local Connection profile.

This section describes how the MAX authenticates an incoming call. These events take place:

1 Before the MAX answers a call, it looks for a matching phone number in a RADIUS user profile. If it cannot find the correct phone number, the MAX hangs up.

2 If the MAX finds a matching phone number in a local Connection profile or RADIUS user profile, it answers the call.

3 The MAX routes the call.

4 The MAX checks its other Answer profile settings.

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

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

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

If Profile Reqd=Yes, the MAX must find a Connection profile, Name/Password profile, RADIUS user profile, or TACACS profile to authenticate the call. Setting up Profile Reqd configures user authentication for the following:

- unencapsulated calls
- calls using ARA or any other encapsulation listed in step Step 7

7 The MAX prompts the user for a login name and password. If the name and password match a local Connection profile or Name/Password profile, the call is authenticated. If no match is found and RADIUS or TACACS remote authentication has been enabled, the MAX requests authentication from the remote server. The MAX clears the call if authentication fails.

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

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

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

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

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

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

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

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

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

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

No matter which authentication method you choose, you can access authentication and user configuration data stored locally or remotely. These are your options:

- Local authentication using a Connection profile or a Name/Password profile.
- Remote authentication using a TACACS or RADIUS server.

  For details on configuring the MAX to use a TACACS server, see "Setting up an authentication server" on page 3-27. For details on configuring the MAX to use a RADIUS server, see the *MAX RADIUS Configuration Guide*.
- Remote authentication using a Digital Pathways Defender server.

  For details on configuring the MAX to use a Defender server, see "Configuring the MAX to use a Defender server" on page 3-30.
- Security-card authentication.

  You can set up your network site to require that users change passwords very frequently, many times per day. When you do so, you use an external authentication server, such as an ACE or SafeWord server. For details, see Chapter 5, "Setting Up Security-Card Authentication."

Setting up authentication using a name and password

Although you can configure local Connection profiles to authenticate using name and password, we recommend that you perform this function in RADIUS. For information, see the *MAX RADIUS Configuration Guide*.

The MAX does not support caller ID (CLID) or called-number authentication. See the *MAX RADIUS Configuration Guide*. for information on configuring authentication using these methods.

To require all callers to authenticate using name and password, follow these steps:

1 In the System > Sys Config menu, set the Name parameter to specify the name of the MAX.

2 In the Ethernet > Answer menu, set Profile Reqd=Yes.

3 In the Ethernet > Answer menu, set Id Auth=Prefer.

If the MAX cannot find a match to the calling party number, the MAX applies authentication using the Recv Auth or Password Reqd parameters in the Answer profile.

4 In the Ethernet > Answer > PPP Options menu, set the Recv Auth=PAP, CHAP, or Either (for PPP, MP, or MP+ calls only).

5 Open the Ethernet > Connections menu.

6 In the Connection profile, set the Station parameter to the name of the remote device.

7 In the Encaps Options submenu of the Connection profile, set the Recv PW parameter to specify the caller's password.

8 Save your changes.

Setting up callback security

Callback security instructs the MAX to hang up on an incoming caller and then immediately initiate a call to that destination. Callback ensures that the connection is made with a known destination.

You can configure the MAX to expect a callback from the machine that is called. This prevents problems that arise when CLID is set to Required on the machine that is expected to callback.

For example, in Figure 3-1 ping or Telnet is initiated through a MAX to a Pipeline and CLID is set to Required on the Pipeline (the side that doing the callback), the Pipeline rejects the incoming call before answering it. To the MAX (the initiating side), it appears as if the call never got through at all.

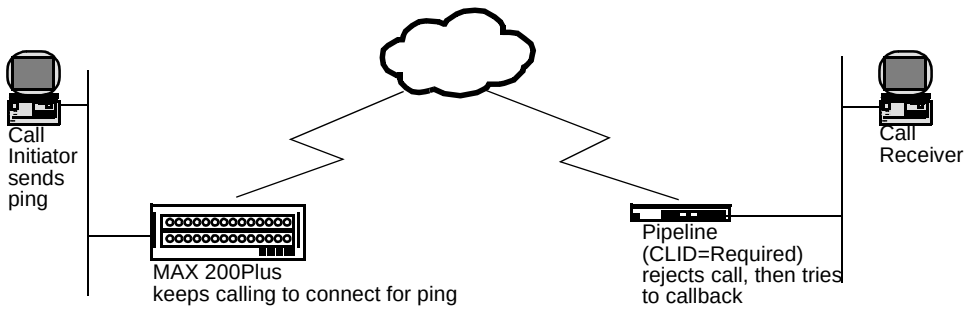

Figure 3-1. Callback connection failure

This is a special problem for ping and telnet, because these processes try continuously to open a connection and reject any callback because the process is already trying establish a connection.

When Exp Callback is set to Yes, calls that dialout and do not connect (for any reason) are put on a list that disallows any further calls to that destination for 90 seconds. This gives the far end an opportunity to complete the callback.

If a call fails for any reason, regardless of whether or not the called machine requires CLID and is attempting a callback, the call initiator must still wait 90 seconds before attempting the call the same number again if Exp Callback is set to Yes.

For information on how authentication works, "How does user authentication work?" on page 3-3.

Table 3-2 shows callback parameters on the MAX.

Table 3-2. Callback security parameters

Location	Parameters with sample values
Ethernet > Connections > *Any Connection profile*	Calling #=555-1213 Dial #=555-1213
Ethernet > Connections > *Any Connection profile* > Telco Options	Callback=Yes Exp Callback=Yes AnsOrig=Both

For information on setting up callback security in RADIUS, see the *MAX RADIUS Configuration Guide*.

To set callback security on the MAX, follow these steps:

1. Open the Ethernet > Connections menu.
2. Open a Connection profile.
3. Using the Dial # parameter, specify the number the MAX dials to reach the remote end of the connection.

   For example, you might enter this setting:

   ```
   Dial #=555-1213
   ```

4. Using the Calling # parameter, specify the number the remote device uses to call the MAX.

   For example, you might enter this setting:

   ```
   Calling #=555-1213
   ```

5. Open the Telco Options submenu of the Connection profile.
6. Turn on callback security by setting these parameters:

   ```
   Callback=Yes
   Exp Callback=Yes
   AnsOrig=Both
   ```

   Note: Callback does not apply to leased lines (if Call Type=Nailed).

   When 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 to and accept incoming calls from the MAX.

   To prevent a problem when CLID on the called machine is set to Required, set Exp Callback to Yes.
7. Save your changes.

Note: If the Pipeline is the calling device and callback is set up on the MAX, the Pipeline must set up Expect Callback.

Setting up authentication of PPP, MP, and MP+ calls

The answering unit always determines the authentication method to use for the call. You can specify PAP, CHAP, or MS-CHAP authentication for name and password verification of incoming PPP, MP, or MP+ calls.

For information on how PPP, MP, and MP+ authentication works, "How does user authentication work?" on page 3-3.

This section describes the following tasks:

- Setting up PAP, CHAP, and MS-CHAP authentication of incoming PPP, MP, and MP+ calls

  The only MS-CHAP format Ascend units support is the Windows NT version, DES and MD4 encryption. An Ascend unit can authenticate a Windows NT system and a Windows NT system can authenticate an Ascend unit. For more specific information on the MS-CHAP format, see Microsoft's Web site at:

  `ftp://ftp.microsoft.com/DEVELOPR/RFC/chapexts.txt`
- Requesting an authentication protocol for outgoing PPP, MP, and MP+ calls

For complete information on setting up PPP, MP, and MP+ calls on the MAX, see the *MAX ISP & Telecommuting Configuration Guide*. For complete information on setting up PPP, MP, and MP+ calls and authentication in RADIUS, see the *MAX RADIUS Configuration Guide*.

Understanding PPP, MP, and MP+

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

A PPP connection is usually a bridged or routed network connection initiated in PPP dialup software. Figure 3-2 shows the MAX with a PPP connection to a remote user running Windows 95 with the TCP/IP stack and PPP dialup software.

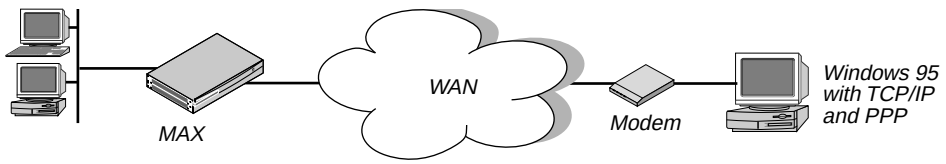

Figure 3-2. A PPP connection

Both MP and MP+ are enhancements to PPP for supporting multichannel links.

- MP supports multichannel links.

  The base channel count determines the number of calls to place, and the number of channels does not change. In addition, MP requires that all channels in the connection share the same phone number—that is, the channels on the answering side of the connection must be in a hunt group.
- MP+ enables the MAX to support multichannel links and Dynamic Bandwidth Allocation (DBA). DBA enables the MAX to increase bandwidth as needed and drop bandwidth

when it is no longer required. MP+ is the only PPP-based encapsulation method that supports DBA.

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

Figure 3-3 shows the MAX connected to a remote Pipeline 25 with an MP+ connection.

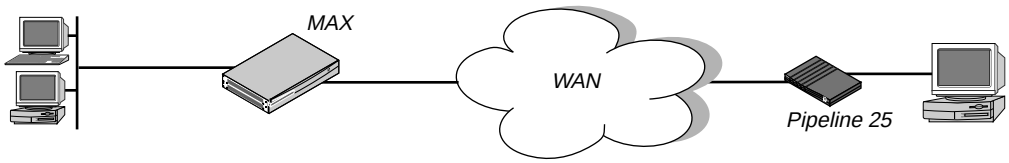

Figure 3-3. An MP+ connection

Understanding PAP, CHAP, and MS-CHAP

Keep this information in mind:

- If the incoming PPP call does not include a source IP address, PAP, CHAP, or MS-CHAP authentication is required.
- PAP and CHAP authentication is not available for ARA, V.34, V.42, or V.120 calls.

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

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

How PAP works

PAP is a PPP authentication protocol that provides a simple method for the MAX to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment, and does not use encryption. The remote device must support PAP.

For PAP authentication, these events take place:

1 The calling unit sends the remote secret in the clear to the MAX.

2 The MAX encrypts the remote secret using the NAS secret.

3 The RADIUS server decrypts the remote secret using the NAS secret.

4 The RADIUS server passes the clear copy of the remote secret to a UNIX or other password validation system.

How CHAP works

CHAP specifies a PPP authentication protocol that is more secure than PAP. It provides a way for the remote device to periodically verify the identity of the MAX using a three-way handshake and encryption. Authentication takes place upon initial link establishment; a device can repeat the authentication process any time after the connection is made. The remote device must support CHAP.

For CHAP authentication, these events take place:

1. The MAX sends a random, 128-bit challenge to the calling unit.
2. The calling unit calculates an MD5 digest using the remote secret, the challenge, and the PPP packet ID.
3. The calling unit sends the MD5 digest, the challenge, and the PPP packet ID (but not the remote secret) to the MAX; the MAX never has the remote secret.
4. The MAX forwards the digest, along with the original challenge and PPP packet ID to RADIUS.

   No encryption is necessary, because MD5 creates a one-way code that cannot be decoded. In addition, RADIUS cannot extract the remote secret. Therefore, it cannot provide a password to a UNIX password system; for this reason, CHAP and UNIX authentication cannot work together.
5. The RADIUS server looks up the remote secret from a local database, and calculates an MD5 digest using the local version of the remote secret, along with the challenge and the PPP packet ID it received from the MAX.
6. The RADIUS server compares the calculated MD5 digest with the digest it received from the MAX.

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

How MS-CHAP works

MS-CHAP is similar to CHAP with minor differences. For more information, see the Microsoft Website at

ftp://ftp.microsoft.com/DEVELOPR/RFC/chapexts.txt

Configuring PAP, CHAP, and MS-CHAP for PPP, MP, and MP+ calls

To configure connections using PAP, CHAP, and MS-CHAP, you must carry out these tasks:

- Set system-wide System, Answer, and Ethernet profile parameters.

  These parameters specify the name of the MAX, the types of encapsulation allowed, the kind of authentication required, and the contents of one or more IP address pools.
- Set up a Connection profile, Name/Password profile, or RADIUS user profile containing settings for each individual connection.

  Note: You only need to set up one of these profiles.

The parameters you can set are listed in Table 3-3.

Table 3-3. Parameters for connections using PAP, CHAP, or MS-CHAP

Location	Parameters with sample values
System > Sys Config	Name=mygw
Ethernet > Answer	Profile Reqd=Yes

Table 3-3. Parameters for connections using PAP, CHAP, or MS-CHAP (continued)

Location	Parameters with sample values
Ethernet > Answer > Encaps	PPP=Yes MP=Yes MPP=Yes
Ethernet > Answer > PPP Options	Recv Auth=PAP, CHAP, MS-CHAP, or Either
Ethernet > Mod Config > WAN Options	Pool#1 Start=10.0.0.20 Pool#1 Count=90 Pool Only=Yes
Ethernet > Connections > *Any Connection profile*	Station=dialgw Encaps=PPP, MP, or MPP
Ethernet > Connections > *Any Connection profile* > Encaps Options	Recv PW=*SECURE*
Ethernet > Names/Passwords > *Any Name/Password profile*	Name=Fred Recv PW=*SECURE*

Setting system-wide parameters

To set system-wide parameters for PAP, CHAP, or MS-CHAP authentication, follow these steps:

1 To specify the name of the MAX used when making outgoing calls, set the Name parameter in the System > Sys Config menu.

2 In the Ethernet > Answer menu, set Profile Reqd=Yes.

This setting specifies that the MAX rejects incoming calls for which it can find no Connection profile, no Name/Password profile, and no entry on a remote authentication server.

For an ARA connection, setting Profile Reqd=Yes prohibits Guest access.

3 In the Ethernet > Answer > Encaps menu, specify that the unit can receive any combination of PPP, MP, and MP+ calls.

Note: PAP, CHAP, and MS-CHAP authentication is available only if you choose MP, MPP, or PPP.

- To specify that the unit can receive PPP calls, set PPP=Yes.
- To specify that the unit can receive MP calls, set MP=Yes.
- To specify that the unit can receive MP+ calls, set MPP=Yes.

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

When you specify Either, the MAX allows authentication if the remote peer can authenticate using any of the designated authentication schemes. If you specify a protocol, the MAX allows authentication only if the remote peer uses that protocol for authentication.

5 If you are using a Name/Password profile for an IP routing connection, open the Ethernet > Mod Config > WAN Options menu to begin setting up one or more IP address pools.

Unlike Connection profiles and RADIUS user profiles, Name/Password profiles cannot specify an IP address for the calling station. When you use a Name/Password profile to authenticate an IP routing connection, the MAX automatically assigns the PPP caller a dynamic IP address as the connection is established. For a call configured in a Name/Password profile, the address assignment is always from the pool of addresses defined as Pool #1, if Pool #1 exists and has available addresses. If Pool #1 does not exist or does not have available addresses, the MAX assigns an address from Pool #2.

6 Set up address pools using the Pool #*n* Count and Pool #*n* Start parameters.

The Pool #*n* Count parameter specifies the number of IP addresses in the IP address pool. Specify a number between 0 and 254. The default value is 0 (zero).

The Pool #*n* Start parameter specifies the first IP address in the address pool. Specify an IP address in dotted decimal notation. The default value is 0.0.0.0.

You can also set up address pools using the Ascend-IP-Pool-Definition attribute. For details, see the *MAX RADIUS Configuration Guide.*

7 Set Pool Only=Yes.

The Pool Only parameter determines whether a caller can reject an IP address assignment and use his or her own IP address. To eliminate the possibility of a caller rejecting the automatic dynamic assignment and spoofing a local, trusted address, set Pool Only=Yes when using Name/Password profiles to authenticate IP routing connections.

For a call configured in a Name/Password profile, the address assignment is always from the pool of addresses defined as Pool #1, if Pool #1 exists and has available addresses. If Pool #1 does not exist or does not have available addresses, the MAX assigns an address from Pool #2.

If the calling station rejects the assignment, the MAX ends the call.

8 Save your changes.

Setting Connection profile parameters

Note: If you set up a Connection profile, you do not need to set up a Name/Password profile or a RADIUS user profile.

To set Connection profile parameters for PAP and CHAP authentication, follow these steps:

1 Open the Ethernet > Connections menu.

2 Open the Connection profile.

3 Set the Station parameter to the name of the user or device making the incoming call.

4 Set the Encaps parameter to the type of encapsulation used on the link.

- PPP specifies that Point-to-Point Protocol is used on the link.

  This setting ensures basic compatibility with non-Ascend devices. For this setting to work, both the dialing side and the answering side of the link must support PPP.

- MP specifies that Multilink Protocol is used on the link.

- MPP specifies that Multilink Protocol Plus (MP+)is used on the link.

  Both the dialing side and the answering side of the link must support MP+. If only one side supports MP+, the connection attempts to use MP. If MP is not available, the connection uses standard single-channel PPP.

5 Open the Encaps Options submenu of the Connection profile.

6 To specify the password that the remote end of the link must send, set the Recv PW parameter.

If the password specified by Recv PW does not match the remote end's value for Send PW (in a Connection profile), Ascend-Send-Passwd (in a RADIUS user profile), or Ascend-Send-Passwd (in a RADIUS user profile), the MAX disconnects the link.

7 Save your changes.

Setting Name/Password profile parameters

Note: If you set up a Name/Password profile, you do not need to set up a Connection profile or a RADIUS user profile.

The Name/Password profile applies only to ARA, PPP, MP, and MP+ calls and to terminal server users.

To set Name/Password profile parameters for PAP and CHAP authentication, follow these steps:

1 Open the Ethernet menu.

2 Open the Names/Passwords menu.

3 Open a Name/Password profile.

4 Set the Name parameter to the name of the user or device making the incoming call.

In a Name/Password profile, the Name parameter specifies the username associated with the profile; the name you specify also becomes the name of the profile.

5 To specify the password that the remote end of the link must send, set the Recv PW parameter.

If the password specified by Recv PW does not match the remote end's value for Send PW (in a Connection profile), Ascend-Send-Passwd (in a RADIUS user profile), or Ascend-Send-Passwd (in a RADIUS user profile), the MAX disconnects the link.

6 Set the value for Template Connection #.

- Use the default, Template Connection=#0 (the Answer profile), to specify that the Name/Password Profile use the Answer Profile as a template.

  This mode supports clients dialing in over PPP and ARA, but does not support a router dialing in.

- Specify a profile number between 1 and 31 to use the Connection Profile to which the number refers.

  In this mode the Name/Password Profile functions as an alias for the Connection Profile.

7 Set Active=Yes.

8 Save your changes.

When a user calls the MAX and Recv Auth has been set to a value other than None in the Answer profile, the MAX asks for a username and password. If the user enters the username specified by the Name parameter in the Name/Password profile, and the password specified by the Recv PW parameter in the Name/Password profile, the MAX uses the Answer profile parameters to establish the connection.

Disabling groups of dial-in calls with the Name/Password profile

You can specify a Connection profile to use as a template for the Name/Password profile, instead of the Answer profile, which is the default template for the Name/Password profile. You can specify a single Connection profile for a group of users, but have individual Name/Password profiles for each user by setting Template Connection # to a number that refers to a Connection profile. The MAX uses that Connection profile for authentication.

For example, you can set up a Connection Profile for the Sales group to use when dialing in, then set up a Name/Password Profile for each individual salesperson. To prevent a user (or users) from dialing in using one of the two following methods:

- De-activate the Name/Password profile for a single salesperson to prevent that salesperson from dialing in by setting the Name/Password Active flag for the user's Name/Password profile to No.
- De-activate the entire Sales group (by setting the Connection Profile Active flag for the Sales group to No).

Setting up a RADIUS user profile

If you set up a RADIUS user profile, you do not need to set up a Connection profile or a Name/Password profile. For information on setting RADIUS attributes for PAP and CHAP authentication, see the *MAX RADIUS Configuration Guide*.

Requesting PAP, CHAP, or MS-CHAP for outgoing calls

To request PAP, CHAP, or MS-CHAP authentication for an outgoing PPP, MP, or MP+ call, use the parameters listed in Table 3-4.

Table 3-4. Parameters for outgoing connections using PAP, CHAP, or MS-CHAP

Parameter	Parameters with sample values
System > Sys Config	Name=mygw
Ethernet > Connections > *Any Connection profile*	Encaps=PPP, MP, or MPP
Ethernet > Connections > *Any Connection profile* > Encaps Options	Send Auth=PAP, CHAP, or MS-CHAP Send PW=*SECURE*

To specify PAP, CHAP, MS-CHAP for an outgoing PPP, MP, or MP+ call, follow these steps:

1 To specify the name of the MAX, set the Name parameter in the System > Sys Config menu.

2 Open the Ethernet > Connections menu.

3 In the Connection profile, set the Encaps parameter to the type of encapsulation used on the link.

– PPP specifies that Point-to-Point Protocol is used on the link.

This setting ensures basic compatibility with non-Ascend devices. For this setting to work, both the dialing side and the answering side of the link must support PPP.

- MP specifies that Multilink Protocol is used on the link.
- MPP specifies that Multilink Protocol Plus is used on the link.

  Both the dialing side and the answering side of the link must support MP+. If only one side supports MP+, the connection attempts to use MP. If MP is not available, the connection uses standard single-channel PPP.

4 In the Encaps Options submenu of the Connection profile, set Send Auth=PAP, CHAP, or MS-CHAP.

This parameter specifies the authentication protocol that the MAX requests when initiating a connection using PPP, MP, or MP+ encapsulation. The MAX only continues authentication if the remote peer also supports the same protocol.

5 In the Encaps Options submenu, set the Send PW parameter to the password that the MAX sends to the remote end of a connection on outgoing calls.

If the password specified by Send PW does not match the remote end's value for Recv PW (in a Connection profile) or Ascend-Receive-Secret (in a RADIUS user profile), the remote end disconnects the link.

6 Save your changes.

For complete information on setting up an outgoing call in the MAX configuration interface, see the *MAX ISP & Telecommuting Configuration Guide*. For complete information on setting up an outgoing call and requesting authentication in RADIUS, see the *MAX RADIUS Configuration Guide*.

Setting up remote terminal server authentication

This section describes the authentication of users calling into the MAX from a terminal or other device that transmits and receives asynchronous data.These sessions are called "remote terminal server sessions" even if the user never sees the MAX terminal server commands or menu.

For information on how authentication works, "How does user authentication work?" on page 3-3.

A remote terminal server session uses one of these types of encapsulation:

Modem calls

Modem calls can originate from either analog or digital modems. The MAX receives incoming analog modem calls on the MAX unit's PCMCIA modems. The MAX receives incoming digital calls over BRI only.

An incoming modem call could be initiated from a PC running a communication program like Soft Comm, which causes the user's modem to dial into the MAX. The MAX directs the call to its modems, and then forwards the calls to its terminal server software. The terminal server either displays one of its interfaces to the caller or forwards the call to a Telnet or TCP host on the local network, depending on how it is configured.

A modem call may contain PPP encapsulation. For example, if the user is running Windows 95 with the TCP/IP stack and Netscape, Windows 95 could be configured to dial up the MAX whenever Netscape is started. In that case, Windows 95 would be running async PPP. After the call is forwarded to the terminal server software, if PPP encapsulation is detected, the call is forwarded to the bridge/router software for an async PPP session.

For users dialing in using modems, V.120, or V.110 devices to transport asynchronous PPP, see the section, "Setting up authentication of PPP, MP, and MP+ calls" on page 3-7. In these cases, none of the steps in "How terminal server authentication works" apply. Asynchronous PPP and synchronous PP sessions are treated identically by the MAX, except that asynchronous PPP sessions do not allow the user access to the MAX's terminal server menus or commands.

V.120 calls

Calls made with V.120 terminal adapters such as the BitSurfer (also known as ISDN modems) are asynchronous calls with CCITT V.120 encapsulation. The MAX handles V.120 encapsulation in software, so it does not require installed devices to process these calls. After removing the link encapsulation, it forwards these calls to its terminal server software. The terminal server either displays one of its interfaces to the caller or forwards the call to a Telnet or TCP host on the local network, depending on how it is configured. Or, if it detects PPP encapsulation, it can forward the call to the bridge/router software for an async PPP session.

Immediate Telnet service

You can specify that a remote terminal server user can establish a Telnet session immediately after the terminal server banner appears. To do this, set Immed Service=Telnet and Telnet Host Auth=Yes in Ethernet > Mod Config > TServ Options menu.

How terminal server authentication works

Terminal server authentication is two-tiered and makes use of these parameters and profiles:

- The Passwd parameter in the Ethernet > Mod Config > TServ Options menu
- Connection profile parameters

These events take place:

1 A caller initiates a terminal server session using a V.34, V.42, V.110, or V.120 connection.

2 If Security=Full or Partial and Initial Scrn=Cmd in the TServ Options menu, the MAX compares the password to the Passwd parameter.

3 If the caller enters the wrong password, the MAX hangs up.

4 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 Connection profile information.

5 If Security=None or Partial and Initial Scrn=Menu, the MAX skips the Passwd parameter and attempts to verify the caller by using the Connection profile information.

6 Terminal server sessions can require a system terminal server password in addition to the per-user password.Whether a system terminal server user password is required depends upon how the Security and Initial Scrn parameters in the Ethernet profile have been set.

– If Security=None, no authentication is performed.

- If Security=Partial, The MAX checks the value of the Profile Reqd parameter in the Answer profile.

  If Profile Reqd=Yes, the MAX must find a Connection profile, Name/Password profile, RADIUS user profile, or TACACS/TACACS+ profile to authenticate the call.
- If Security=Full, the MAX must find a Connection profile, Name/Password profile, RADIUS user profile, or TACACS/TACACS+ profile to authenticate the call, and then prompt the user for the correct name.

7 If the name matches a local Connection profile or Name/Password profile, the call is authenticated. If no match is found and RADIUS or TACACS remote authentication has been enabled, the MAX requests authentication from the remote server. The MAX clears the call if authentication fails.

Note: If Security=Partial or Security=Full, the user must supply the system terminal server password whenever changing from the menu mode to the command-line mode.

Configuring terminal server authentication

Table 3-5 lists the parameters you can use to set up terminal server password authentication.

Table 3-5. Terminal server s

Location	Parameters with sample values
Ethernet > Mod Config > TServ Options	TS Enabled=Yes Passwd=*SECURE* Security=Full Login Timeout=300 Login Prompt Password Prompt Toggle Scrn=No
Ethernet > Mod Config > Auth	Auth TS Secure=Yes

To set up password authentication for the terminal server interface, follow these steps:

1 Open the Ethernet > Mod Config > TServ Options menu.

2 Set TS Enabled=Yes.

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

3 For the Passwd parameter, specify the password a user must enter to begin a terminal server session.

You can enter up to 20 characters. The password is case sensitive.

4 Set Security=Full or Partial.

The Security parameter specifies whether a user must enter a password under different circumstances.

- Partial specifies that the user must enter the system terminal server password (in the Passwd parameter) before entering the terminal server command line mode, but the user is not prompted for a login name or password.

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 in the TServ Options menu.

- Full specifies that the user must enter the system terminal server password (in the Passwd parameter) before entering the terminal server command line mode. When making the initial connection, the user must enter a login name and password that match a local Connection profile or a RADIUS or TACACS profile.
- 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 in the TServ Options menu. For information on restricting the options available from the menu-driven interface, see "Restricting Telnet, raw TCP, and Rlogin access to the terminal server" on page 3-18.

5 Set the Login Timeout parameter.

Specify the number of seconds the MAX will wait for a user to complete logging in before disconnecting the user in the Login Timeout field.

You can enter any integer between 0 and 300 seconds. 300 seconds is the default.

The user has the total number of seconds indicated in the Login Timeout field to attempt a successful login. This means that the timer begins when the login prompt appears on the terminal server screen, and continues (is not reset) when the user makes unsuccessful login attempts. If the user has not logged in successfully by the time indicated by Login Timeout has elapsed, the MAX disconnects the call.

6 Set the Login Prompt parameter.

Specify the prompt the terminal server displays when asking the user for a login name.

A login prompt can contain up to 31 characters.

7 Set the Password Prompt parameter.

Specify the prompt the terminal server displays when asking the user for a password.

A login prompt can contain up to 31 characters.

8 If you are using RADIUS, open the Ethernet > Mod Config > Auth menu and set the Auth TS Secure parameter.

Set Auth TS Secure=No to specify that the MAX accept dial-in calls even though no login host is specified in the RADIUS user profile.

Auth TS Secure=Yes specifies that the MAX does not accept dial-in calls when there is no login host specified in the RADIUS user profile.

See the *MAX 200Plus Reference Guide* for more information.

Note: This applies only to dial-in calls where Login-Service=TCP-CLEAR or Login-Service=Telnet. It does not apply to PPP calls.

9 Save your changes.

Using an Answer or Connection profile as a template

When one of the users in the Name/Passwords Profile attempts to connect to the terminal server, the MAX uses a "template" profile constructed from the Answer or Connection profile and the name and password from the Name/Password Profile. For more information, see the *MAX 200Plus Reference Guide*.

If you prefer, you can authenticate a terminal server user with the name and password from a profile constructed a name and password from the Name/Password profile, with any additional

required parameter settings from the Answer or Connection profile. Since the Name/Password profile does not supply all the parameters a terminal server session might need, the MAX uses the settings from the Answer profile or Connection profile named in the Template parameter for these additional parameters.

Restricting Telnet, raw TCP, and Rlogin access to the terminal server

For the security of other hosts on your local network, you can carry these tasks:

- Give users a menu of specific hosts to which they can establish a Telnet, raw TCP, or Rlogin session.
- Specify that users establish a Telnet, raw TCP, or Rlogin session with a device immediately after login, bypassing the terminal server interface altogether.

To restrict Telnet, raw TCP, and Rlogin access to the terminal server, follow these steps:

1 Open the Ethernet > Mod Config > TServ Options menu.

2 To specify the hosts to which users can Telnet, set the Host #*n* Addr and Host #*n* Text parameters.

These parameters specify the IP addresses and descriptions of the first, second, third, and fourth hosts to which an operator can Telnet. The user sees a list of hosts only if he or she has access to the menu-driven interface. For details on granting this access, see “Restricting Telnet, raw TCP, and Rlogin access to the terminal server” on page 3-18.

For example, you might make these settings:

```
Host #1 Addr=10.2.3.1/24
Host #1 Text=host1.abc.com
Host #2 Addr=10.2.3.2/24
Host #2 Text=host2.abc.com
Host #3 Addr=10.2.3.3/24
Host #3 Text=host3.abc.com
Host #4 Addr=10.2.3.4/24
Host #4 Text=host4.abc.com
```

The MAX ignores the Host #*n* Addr parameter if a RADIUS server supplies the list of Telnet hosts—that is, if you set Remote Conf=Yes. For information on setting up a list of hosts in RADIUS, see the *MAX RADIUS Configuration Guide*.

Save your changes.

Setting up ARA authentication

ARA connections rely on AppleTalk; the MAX includes a minimal AppleTalk stack for ARA support. The minimal stack includes an NBP (Name Binding Protocol) network visible entity and an AEP (AppleTalk Echo Protocol) echo responder; you can therefore use standard AppleTalk management and diagnostic tools, such as InterPoll from Apple Computer, to obtain information.

For information on how authentication works, “How does user authentication work?” on page 3-3.

For a pure AppleTalk connection, a Macintosh user must have ARA Client software and an asynchronous modem. For a TCP/IP connection through ARA, the Macintosh must also be running TCP/IP software, such as MacTCP or Open Transport.

ARA is an asynchronous protocol. It supports V.34, V.42, V.120, and X.75 calls only. It does not support V.110 calls or synchronous connections.

Figure 3-4 shows a Macintosh with an internal modem dialing into the MAX. The Macintosh uses the ARA Client software to communicate with an IP host on the Ethernet.

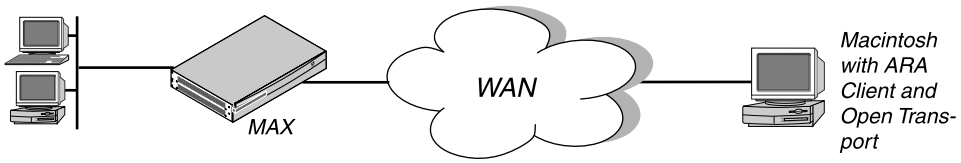

Figure 3-4. An ARA connection

Table 3-6 shows ARA authentication parameters on the MAX.

Table 3-6. ARA authentication parameters

Location	Parameters with sample values
System > Sys Config	Name=mygw
Ethernet > Answer	Profile Reqd=Yes
Ethernet > Answer > Encaps	ARA=Yes
Ethernet > Mod Config	Appletalk=Yes
Ethernet > Mod Config > AppleTalk	Zone Name=Berkeley
Ethernet > Mod Config > WAN Options	Pool#1 Start=10.0.0.20 Pool#1 Count=90 Pool Only=Yes Pool Summary=No
Ethernet > Connections > *Any Connection profile*	Station=Ted Encaps=ARA
Ethernet > Connections > *Any Connection profil*e > Encaps Options	Password=*SECURE*
Ethernet > Names/Passwords > *Any Password profile*	Name=Ted Recv PW=*SECURE*

This section describes how to set up ARA authentication in the MAX configuration interface. For complete information on setting up ARA calls on the MAX, see the *MAX ISP & Telecommuting Configuration Guide*. For complete information on setting up ARA calls and authentication in RADIUS, see the *MAX RADIUS Configuration Guide*.

Understanding ARA authentication tasks

To configure incoming connections using ARA authentication, you must carry out these tasks:

- Set system-wide System, Answer, and Ethernet profile parameters specifying the name of the MAX, the type of encapsulation allowed, the type of authentication in use, and the contents of one or more IP address pools.
- Set up a Connection profile, Password profile, or RADIUS user profile containing settings for each individual connection.

  Note: You only need to set up one of these profiles.

When the MAX receives an ARA call, it checks whether ARA encapsulation is enabled in the Answer profile and, if so, whether a profile is required. It then looks for a Connection profile that matches the caller's name and password. If it finds a match, it accepts the call.

If it cannot find a matching Connection profile, the MAX looks for a Name/Password profile. If it cannot find a matching Name/Password profile, the MAX looks for a RADIUS user profile or TACACS profile.

Setting system-wide parameters

To set system-wide parameters for ARA authentication, follow these steps:

1. In the System > Sys Config menu, set the Name parameter to the name of the MAX.
2. To disable Guest access via ARA, set Profile Reqd=Yes in the Ethernet > Answer menu.

   Note that ARA does not support PAP, CHAP, or MS-CHAP authentication.
3. To enable ARA encapsulation, set ARA=Yes in the Ethernet > Answer > Encaps menu.
4. Set Appletalk=Yes in the Ethernet > Mod Config menu.
5. If the local Ethernet supports an AppleTalk router with configured zones, set the Zone Name parameter in the Ethernet > Mod Config > AppleTalk menu.
6. If you are using a Name/Password profile for an IP routing connection, open the Ethernet > Mod Config > WAN Options menu to begin setting up one or more IP address pools.

   Unlike Connection profiles and RADIUS user profiles, Name/Password profiles cannot specify an IP address for the calling station. When you use a Name/Password profile to authenticate an IP routing connection, the MAX automatically assigns the PPP caller a dynamic IP address as the connection is established. For a call configured in a Name/Password profile, the address assignment is always from the pool of addresses defined as Pool #1, if Pool #1 exists and has available addresses. If Pool #1 does not exist or does not have available addresses, the MAX assigns an address from Pool #2.
7. Set up address pools using the Pool #*n* Count and Pool #*n* Start parameters.

   The Pool #*n* Count parameter specifies the number of IP addresses in the IP address pool. Specify a number between 0 and 254. The default value is 0 (zero).

   The Pool #*n* Start parameter specifies the first IP address in the address pool. Specify an IP address in dotted decimal notation. The default value is 0.0.0.0.

   You can also set up address pools using the Ascend-IP-Pool-Definition attribute. For details, see the *MAX RADIUS Configuration Guide.*
8. Set Pool Only=Yes.

The Pool Only parameter determines whether a caller can reject an IP address assignment and use his or her own IP address. To eliminate the possibility of a caller rejecting the automatic dynamic assignment and spoofing a local, trusted address, set Pool Only=Yes when using Name/Password profiles to authenticate IP routing connections.

For a call configured in a Name/Password profile, the address assignment is always from the pool of addresses defined as Pool #1, if Pool #1 exists and has available addresses. If Pool #1 does not exist or does not have available addresses, the MAX assigns an address from Pool #2.

If the calling station rejects the assignment, the MAX ends the call.

9 Save your changes.

Setting Connection profile parameters

Note: If you set up a Connection profile, you do not need to set up a Name/Password profile or a RADIUS user profile.

To set Connection profile parameters for ARA authentication, follow these steps:

1 Open the Ethernet > Connections menu.

2 Open the Connection profile.

3 Set the Station parameter to the name of the remote device.

4 Set Encaps=ARA.

5 Open the Encaps Options submenu of the Connection profile.

6 Set the Password parameter to specify the ARA password.

7 Save your changes.

Setting Name/Password profile parameters

Note: If you set up a Name/Password profile, you do not need to set up a Connection profile or a RADIUS user profile.

The Name/Password profile applies only to ARA (AppleTalk Remote Authentication) and PPP-encapsulated calls. It does not apply to terminal server users.

To set Name/Password profile parameters for ARA authentication, follow these steps:

1 Open the Ethernet menu

2 Open the Names/Passwords menu.

3 Open a Name/Password profile.

4 To specify the name of the remote device, set the Name parameter.

In a Name/Password profile, the Name parameter specifies the username associated with the profile; the name you specify also becomes the name of the profile.

5 To specify the password that the remote end of the link must send, set the Recv PW parameter.

If the password specified by Recv PW does not match the remote end's value for Send PW (in a Connection profile), Ascend-Send-Passwd (in a RADIUS user profile), or Ascend-Send-Secret (in a RADIUS user profile), the MAX disconnects the link.

6 Set the value for Template Connection #.

– Use the default, Template Connection=#0 (the Answer profile), to specify that the Name/Name/Password profile use the Answer Profile as a template.

  This mode supports clients dialing in over PPP and ARA, but does not support a router dialing in.

– Specify a profile number between 1 and 31 to use the Connection Profile to which the number refers.

7 Save your changes.

When a user calls the MAX and Recv Auth has been set to a value other than None in the Answer profile, the MAX asks for a username and password; if the user enters the username specified by the Name parameter in the Name/Password profile, and the password specified by the Recv PW parameter in the Name/Password profile, the MAX uses the Answer profile parameters to establish the connection.

Using a Connection profile with the Name/Password profile

You can specify a Connection profile to use as a template for the Name/Password profile, instead of the Answer profile, which is the default template for the Names/Password profile. You can specify a single Connection profile for a group of users, but have individual Names/Password profiles for each user by setting Template Connection # to a number that refers to a Connection profile. The MAX uses that Connection profile for authentication.

For example, you can set up a Connection Profile for the Sales group to use when dialing in, then set up a Name/Password Profile for each individual salesperson. To prevent a user (or users) from dialing in using one of the two following methods:

- De-activate the Name/Password profile for a single salesperson to prevent that salesperson from dialing in by setting the Name/Password Active flag for the user's Name/Password profile to No.
- De-activate the entire Sales group (by setting the Connection Profile Active flag for the Sales group to No).

Setting up a RADIUS user profile

If you set up a RADIUS user profile, you do not need to set up a Connection profile or a Name/Password profile. For information on setting RADIUS attributes for ARA authentication, see the *MAX RADIUS Configuration Guide*.

Setting up IP addressing

When a call comes in and password authentication is required, the MAX attempts to match the caller's name and password to a local Connection profile. If password authentication is not required, the MAX can match IP-routed PPP calls using the IP address specified by the Connection profile. The address can be a static address or a dynamic address.

- Static address

  A static address is specified by the LAN Adrs parameter in the Connection profile or by the Framed-Address attribute in the RADIUS user profile.

- Dynamic address

  A dynamic address comes from the pool of addresses set by the Pool #*n* Start and Pool #*n* Count parameters or by the Ascend-IP-Pool-Definition attribute.

  If the calling end accepts the IP address, the MAX sets the LAN Adrs parameter or Framed-Address attribute to the assigned address, depending on whether a Connection profile or RADIUS user profile is in use. If a static address is already set in a Connection profile or RADIUS user profile, it overrides any IP address from an IP address pool.

When an IP routing connection is being authenticated, the IP address is verified as part of the PPP negotiation before a call is established. Any of these scenarios can take place:

- If the caller's PPP software presents an IP address and the MAX does not require dynamic IP address assignment, the MAX must find a Connection profile or RADIUS user profile that matches that address.

  If the MAX finds a profile, it authenticates the connection using PAP, CHAP, or MS-CHAP, and then establishes the connection. If it does not find a matching profile, the MAX ends the call without completing PAP, CHAP, or MS-CHAP authentication.

- If the caller's PPP software specifies dynamic IP address assignment, the MAX must obtain an available IP address from pools defined in the Ethernet profile or in RADIUS.

  If the MAX successfully assigns an address, it authenticates the connection using PAP, CHAP, or MS-CHAP, and then establishes the connection. If no addresses are available, the MAX ends the call.

- If the caller's PPP software presents an IP address and the MAX requires dynamic IP address assignment, the calling station must accept the IP address

  If the calling station accepts the IP address, the MAX authenticates the connection using PAP, CHAP, or MS-CHAP, and then establishes the connection. If the calling station does not accept the IP address assignment, the MAX ends the call without completing PAP, CHAP, or MS-CHAP authentication.

  For more information on how authentication works on the MAX, see "How does user authentication work?" on page 3-3.

The parameters you can set for IP addressing are listed in Table 3-7.

Table 3-7. IP address parameters

Location	Parameters with sample values
Ethernet > Answer	Assign Adrs=Yes
Ethernet > Answer > PPP Options	Route IP=Yes
Ethernet > Connections > *Any Connection profile* > IP Options	LAN Adrs=10.5.6.7/24 (or) Pool=2
Ethernet > Mod Config > WAN Options	Pool #*n* Count=10 Pool #*n* Start=0.0.0.0 Pool Only=Yes

The sections that follow describe how to carry out these tasks:

- Specifying an IP address that must match a caller's IP address
- Assigning a dynamic IP address to a caller requesting one
- Requiring that a caller accept an IP address from the MAX
- Using Name/Password profiles to prevent IP spoofing

See the *MAX ISP & Telecommuting Configuration Guide* for related information on setting up IP routing connections in the MAX configuration interface. See the *MAX RADIUS Configuration Guide* for related information on setting up IP routing connections in RADIUS.

Specifying a static IP address

To set up a static IP address that must match a caller's IP address, follow these steps:

1 Open the Ethernet > Answer > PPP Options menu.

2 Set Route IP=Yes.

3 Open the Ethernet > Connections menu.

4 Open the Connection profile for the caller.

5 Open the IP Options submenu of the Connection profile.

6 To specify a static address, set the LAN Adrs parameter.

7 Save your changes.

Assigning a dynamic IP address to a caller requesting one

To configure the MAX to assign an IP address to a caller that requests one, follow these steps

1 Open the Ethernet > Answer menu.

2 Set Assign Adrs=Yes.

When you specify this setting, the MAX asks the device to accept an assigned address, choosing an address from the pool of addresses set by the Pool #*n* Start and Pool #*n* Count parameters or by the Ascend-IP-Pool-Definition attribute. If the calling end accepts the IP

address, the MAX sets the LAN Adrs parameter in the Connection profile to the assigned address.

Note: In some TCP/IP implementations, when the workstation needs the MAX to set the IP address, you must set the workstation's address to 0.0.0.0. Setting the address to any other value tells the workstation to use that value and notify the MAX.

3 Open the Ethernet > Answer > PPP Options menu.

4 Set Route IP=Yes.

5 Open the Ethernet > Mod Config > WAN Options menu.

6 Set up address pools using the Pool #*n* Count and Pool #*n* Start parameters.

The Pool #*n* Count parameter specifies the number of IP addresses in the IP address pool. Specify a number between 0 and 254. The default value is 0 (zero).

The Pool #*n* Start parameter specifies the first IP address in the address pool. Specify an IP address in dotted decimal notation. The default value is 0.0.0.0.

You can also set up address pools using the Ascend-IP-Pool-Definition attribute in RADIUS. For details, see the *MAX RADIUS Configuration Guide.*

7 Open the Ethernet > Connections menu.

8 Open a Connection profile.

9 In the Connection profile, set the Pool parameter to the number of the pool to use for the call.

10 Save your changes.

Requiring that a caller accept an IP address from the MAX

To require that a caller accept an IP address from the MAX, follow these steps:

1 Open the Ethernet > Answer menu.

2 Set Assign Adrs=Yes.

When you specify this setting, the MAX asks the device to accept an assigned address, choosing an address from the pool of addresses set by the Pool #*n* Start and Pool #*n* Count parameters or by the Ascend-IP-Pool-Definition attribute. If the calling end accepts the IP address, the MAX sets the LAN Adrs parameter in the Connection profile to the assigned address.

3 Open the Ethernet > Answer > PPP Options menu.

4 Set Route IP=Yes.

5 Open the Ethernet > Mod Config > WAN Options menu.

6 Set up address pools using the Pool #*n* Count and Pool #*n* Start parameters (optional).

The Pool #*n* Count parameter specifies the number of IP addresses in the IP address pool. Specify a number between 0 and 254. The default value is 0 (zero).

The Pool #*n* Start parameter specifies the first IP address in the address pool. Specify an IP address in dotted decimal notation. The default value is 0.0.0.0.

You can also set up address pools using the Ascend-IP-Pool-Definition attribute in RADIUS. For details, see the *MAX RADIUS Configuration Guide.*

7 To require a calling station to accept an IP address from the MAX, set Pool Only=Yes.

This setting requires the calling station to accept the static address specified in a Connection profile or RADIUS user profile, or a dynamic address. If the calling station rejects the assignment, the MAX ends the call.

If you set Pool Only=No, the MAX accepts the IP address specified by the caller.

8 Open the Ethernet > Connections menu.

9 Open a Connection profile.

10 In the Connection profile, set the LAN Adrs parameter to specify a static address, or set the Pool parameter to the number of the pool to use for assigning a dynamic IP address.

11 Save your changes.

Using Name/Password profiles to prevent IP address spoofing

IP address spoofing is a technique in which outside users pretend to be from the local network in order to obtain unauthorized access.

Unlike Connection profiles and RADIUS user profiles, Name/Password profiles cannot specify an IP address for the calling station. When you use a Name/Password profile to authenticate an IP routing connection, the MAX automatically assigns the PPP caller a dynamic IP address as the connection is established, ensuring that the user is not spoofing the address. Table 3-8 shows the relevant parameters on the MAX

Table 3-8. Name/Password profile address restriction parameters

Location	Parameters with sample values
Ethernet > Mod Config > WAN Options	Pool#1 Start=10.0.0.20 Pool#1 Count=90 Pool Only=Yes
Ethernet > Names/Passwords > *Any Name/Password profil*e	Name=Ted Recv PW=*SECURE*

Note: You also can set up data filters to prevent IP address spoofing. For details, see “A sample IP filter to prevent address spoofing” on page 4-10.

To set parameters to prevent IP spoofing, follow these steps:

1 Open the Ethernet menu.

2 Open the Names/Passwords menu.

3 Open a Name/Password profile.

4 Set the Name parameter to the name of the user or device making the incoming call.

In a Name/Password profile, the Name parameter specifies the username associated with the profile; the name you specify also becomes the name of the profile.

5 To specify the password that the remote end of the link must send, set the Recv PW parameter.

If the password specified by Recv PW does not match the remote end’s value for Send PW, the MAX disconnects the link.

6 Open the Ethernet > Mod Config > WAN Options menu.

7 Set up address pools using the Pool #*n* Count and Pool #*n* Start parameters.

The Pool #*n* Count parameter specifies the number of IP addresses in the IP address pool. Specify a number between 0 and 254. The default value is 0 (zero).

The Pool #*n* Start parameter specifies the first IP address in the address pool. Specify an IP address in dotted decimal notation. The default value is 0.0.0.0.

You can also set up address pools using the Ascend-IP-Pool-Definition attribute. For details, see the *MAX RADIUS Configuration Guide.*

8 Set Pool Only=Yes.

The Pool Only parameter determines whether a caller can reject an IP address assignment and use his or her own IP address. To eliminate the possibility of a caller rejecting the automatic dynamic assignment and spoofing a local, trusted address, set Pool Only=Yes when using Name/Password profiles to authenticate IP routing connections.

For a call configured in a Name/Password profile, the address assignment is always from the pool of addresses defined as Pool #1, if Pool #1 exists and has available addresses. If Pool #1 does not exist or does not have available addresses, the MAX assigns an address from Pool #2.

If the calling station rejects the assignment, the MAX ends the call.

9 Save your changes.

Setting up an authentication server

The MAX supports resident Connection profiles and Name/Password profiles for authenticating incoming connections, but the total number of supported profiles is limited by the amount of RAM in the unit. Many ISPs and other large sites use a third-party authentication server such as RADIUS (Remote Authentication Dial In User Service) or TACACS (Terminal Access Concentrator Access Control Server) to centrally control, manage, and audit security.

For information on how authentication works, “How does user authentication work?” on page 3-3.

Understanding authentication servers

When the MAX receives an incoming call, it first looks through its resident profiles (Connection and Name/Password profiles). If it doesn’t find a matching profile, it checks its Ethernet profile for an authentication server’s address. If it finds one, it accesses the authentication database in that server to search for a matching profile. The MAX supports these types of authentication servers:

- RADIUS

  The extensions to the RADIUS protocol provided by Ascend let you configure most of the features supported by the resident profiles. The information resides in a database on a PC or UNIX system; the RADIUS daemon on that system accesses the data.

  For complete information on installing and configuring a RADIUS server, and on setting up the MAX to operate with a RADIUS server, see the *MAX RADIUS Configuration Guide.*

- TACACS

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), and terminal server validation. It does not support CHAP authentication.

For details on setting up a TACACS server, see the documentation that came with your TACACS software. For information on setting up the MAX to operate with a TACACS server, see "Configuring the MAX to use a TACACS server" on page 3-28.

- Digital Pathways Defender

  The Defender is an authentication server developed by Digital Pathways. If an Ascend unit is configured to use Defender authentication, all authenticated users are given service according to the parameters of the TServ Options submenu in the Ethernet Profile. For information on configuring the MAX to use Defender authentication, see "Configuring direct Defender server authentication" on page 5-25.

- SecurID ACE

  The MAX can authenticate terminal server users by directly contacting an ACE server, developed by Security Dynamics. Although SecurID ACE authentication is also indirectly supported via RADIUS, direct support for the SecurID ACE server provides two advantages:

  – 1) For those installations where other RADIUS features are not required, having direct SecurID ACE support on the Ascend unit decreases the complexity of the system, making the system easier to configure and maintain.

  – The SecurID ACE support via RADIUS does not support the "New PIN Mode" feature, which allows a dial-in user to change the personal identifying number (PIN).

  Note: The MAX does not support ACE authentication for PPP dial-in users.

For information on setting up the MAX to use direct or indirect ACE/Server, see "Configuring direct SecurID ACE authentication" on page 5-18.

Configuring the MAX to use a TACACS server

This section describes how to configure the MAX to communicate with a TACACS server. Follow these steps:

1 Open the Ethernet > Mod Config > Auth menu.

```
X0-X00 Mod Config
 Auth...
 >Auth=TACACS
  Auth Host #1=10.23.45.11
  Auth Host #2=10.23.45.12
  Auth Host #3=10.23.45.13
  Auth Port=1645
  Auth Timeout=5
  Auth Key=N/A
  Auth Pool=N/A
  Auth Req=Yes
  Local Profile First=NYes
  APP Server=No
  APP Host=N/A
  APP Port=N/A
  SecurID DES encryption=N/A
```

```
SecurID host retries=N/A
SecurID NodeSecret=N/A
```

2 Set Auth=TACACS.

3 For each Auth Host parameter, specify the IP address of a TACACS host.

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

When it successfully connects to an authentication server, the MAX uses that machine until it fails to serve requests. The MAX does not use the first host until the second machine fails, even if the first host has come online while the second host is still servicing requests.

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

4 For the Auth Port parameter, enter the UDP port number used by the TACACS software.

For example, you might specify this setting:

`Auth Port=1645`

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

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

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

6 Specify whether to use remote authentication before local. The default is Yes.

If you enter No, remote authentication is tried first. The MAX waits for authentication to succeed or for the timeout specified in Auth Timeout to expire. This can take longer than the timeout specified for the connection and causes all connection attempts to fail.

To prevent this set the value for Auth Timeout low enough not to cause the line to be dropped, but still high enough to permit the unit to respond if it is able to. The recommended time is 3 seconds.

Some authentication methods do not work the same without a remote authenticator as they do with one. Table 3-9 shows authentication methods and the specific information you will need to consider if you use a particular method with Local Profile First=No.

Table 3-9. Remote authentication considerations

Method	Remote Authentication Considerations
PAP	None. Works the same with or without remote authentication.
CHAP	None. Works the same with or without remote authentication.
PAP-TOKEN	Works either way, but will not produce a challenge if there is a local profile. This defeats the security of using PAP-TOKEN.

Table 3-9. Remote authentication considerations (continued)

Method	Remote Authentication Considerations
PAP-TOKEN-CHAP	Brings up one channel, but all other channels fail.
CACHE-TOKEN	If the remote side has ever authenticated using a challenge, CACHE-TOKEN will not work with local profiles. If the remote side has not ever authenticated, there will be no problem with the local profiles.

7 Enter the port number for the source port for remote authentication requests.

Type a port number between 0 and 65535. The default value is 0 (zero); if you accept this value, the Ascend unit can use any port number between 1024 and 2000.

You can specify the same port for authentication and accounting requests.

8 Save your changes.

Configuring the MAX to use a Defender server

This section describes how to configure the MAX to communicate with a Defender server. Follow these steps:

1 Open the Ethernet > Mod Config > Auth menu:

```
X0-X00 Mod Config
 Auth
 >Auth=Defender
  Auth Host #1=137.175.80.24
  Auth Host #2=0.0.0.0
  Auth Host #3=0.0.0.0
  Auth Port=2626
  Auth Timeout=10
  Auth Key=****************
  Auth Pool=No
  APP Server=No
  APP Host=N/A
  APP Port=N/A
  SecurID DES encryption=N/A
  SecurID host retries=N/A
  SecurID NodeSecret=N/A
```

2 Set Auth to Defender.

Auth Host #2 and Auth Host #3 are not applicable, because the Ascend unit can support only one Defender authentication server at this time.

3 Set the value of Auth Port to the TCP port number of the Defender authentication server, usually 2626.

4 Set the value of Auth Key.

Auth Key is used as a DES secret key shared between the Ascend unit and the Defender authentication server. This key is also used for authentication by the Ascend unit in its role as a Defender authentication agent.

5 Set Auth Timeout to indicate the number of seconds the Ascend unit waits before assuming that the Defender server has become nonfunctional.

6 Enter the port number for the source port for remote authentication requests.

Type a port number between 0 and 65535. The default value is 0 (zero); if you accept this value, the Ascend unit can use any port number between 1024 and 2000.

You can specify the same port for authentication and accounting requests.

7 Save your changes.

Creating Data Filters

4

This chapter covers these topics:

Introduction to Ascend filters

Ascend filters define packet conditions. When a filter is in use, the MAX examines every packet in the packet stream and takes action if the defined filter rules are present. The action the MAX takes depends on the conditions you specify. You can indicate that a filter does not forward certain packets; or you can specify that a filter forwards *all* packets *except* those defined in the filter. The conditions also specify whether the MAX examines inbound packets, outbound packets, or both.

You can set up two types of filters:

- Call filters

  The forwarding action of a call filter does not affect which packets are sent across an active connection. In a call filter, the "forward" action determines which packets can either initiate a connection or reset the Idle timer for an established connection. The Idle timer is used to determine when to disconnect inactive sessions. Call filters are typically used to prevent unnecessary connections.

- Data filters

  The forwarding action of a data filter affects the actual data stream. The MAX drops or forwards certain packets as specified in the filter rules. Data filters most often apply to network security, but you need not limit them to that purpose.

  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.

  Data filters do not affect the Idle Timer, and a data filter applied to a Connection profile does not affect the answering process.

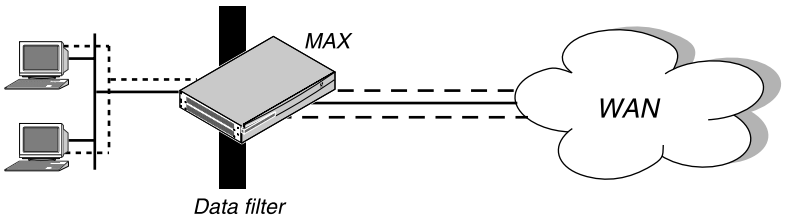

Figure 4-1. Data filters can drop or forward certain packets

When no filter is in use, the default action is to forward all packets and allow all packets to reset the Idle timer. Packets can pass through more than one filter. If both a data filter and call filter apply to an interface, the data filter is applied first.

Note: This chapter describes how to set up and use data filters only. For information on how to configure call filters, see the *MAX 200Plus ISP and Telecommuting Configuration Guide*. For information about IPX SAP filters, which affect which NetWare services the MAX adds to its service table, see the *MAX 200Plus ISP and Telecommuting Configuration Guide*.

Overview of Filter profiles

Figure 4-2 shows how filters are organized in the menu interface. The main menu is the Filters menu; all others are nested submenus below it.

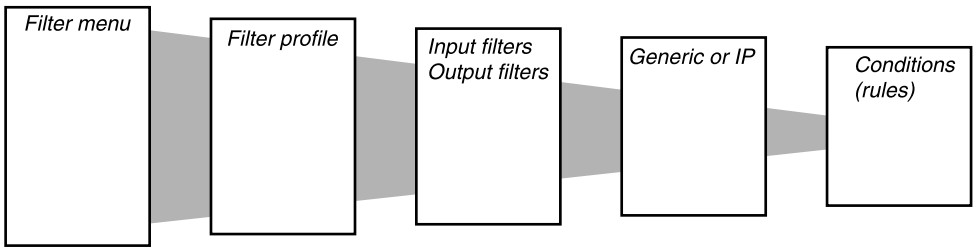

Figure 4-2. Filter terminology

- Filters menu

  The Filters menu contains a list of numbered profiles. When applying a filter, you identify it by the unique portion of its Filter profile number (for example, 1, 2, 3...). The MAX applies all filter rules within that profile.

- Filter profile

  A Filter profile is a set of filter rules.

- Input and output filters

  At the top level of a Filter profile are submenus labeled Input Filters and Output Filters. Each submenu contains a list of 12 filters. The MAX applies the conditions you define within the filters to the inbound or outbound packet stream in order, from 1 to 12. See “Filtering inbound and outbound packets” on page 4-3 for details.

- Generic or IP filters

  Each input filter or output filter can be one of two types: Generic or IP. Generic filter rules specify locations and values that can appear in any packet. IP filter rules specify IP-specific packet characteristics, such as address, mask, and port. Once you assign a type, you can open the corresponding submenu to define the packet-level filter rules. For details, see “Defining generic filter conditions” on page 4-5 and “Defining IP filter rules” on page 4-6.

- Filter rules

  Filter rules specify the actual packet characteristics that the MAX examines in the data stream.

Filtering inbound and outbound packets

To set up filters, you must carry out the following tasks:

- Specify and activate an input or output filter.
- Define generic filter conditions.
- Define IP filter conditions.
- Specify a filter in a profile.

The sections that follow describe how to perform each task.

Specifying and activating an input or output filter

To begin setting up filters for inbound and outbound packets, follow these steps:

1 Open the Filters menu.

2 Open a Filter profile.

3 For the Name parameter, specify the name of the profile.

```
50-401 IP Data
>Name=IP Data
 Input filters...
 Output filters...
```

4 Open the Input Filters or Output Filters submenu.

For an input filter, this menu appears:.

```
50-401 IP Data
 Input filters...
 >In filter 01
  In filter 02
  In filter 03
  In filter 04
  In filter 05
  In filter 06
  In filter 07
  In filter 08
  In filter 09
  In filter 10
  In filter 11
  In filter 12
```

For an output filter, this menu appears:

```
50-401 IP Data
 Input filters...
 >In filter 01
  In filter 02
  In filter 03
  In filter 04
  In filter 05
  In filter 06
  In filter 07
  In filter 08
  In filter 09
  In filter 10
  In filter 11
  In filter 12
```

You can specify up to 12 input filters and 12 output filters in a Filter profile. The MAX applies these filters in the order in which they appear; a filter must be activated for the MAX to apply it. Input filters cause the MAX to examine incoming packets. Output filters cause the MAX to examine outgoing packets.

If the MAX applies the filter as a data filter on Ethernet, it affects packets from the Ethernet *into* the MAX or from the MAX *out* to the Ethernet. If the MAX applies a data filter on a WAN interface defined in a Connection profile, the filter affects packets from that WAN interface *into* the MAX or from the MAX *out* to that interface.

The default action is to forward packets, so if a packet does not match any of the defined conditions, the MAX simply forwards it. If you define only input filters, the default action for output filters is to forward all packets. The same is true in the other direction; if you define only output filters, the default action for inbound packets is to forward them.

5 Select an "In filter" or an "Out filter" to configure.

When you open an "In filter," a menu like this one appears:

```
50-401 IP Data
 In filter 01
 >Valid=Yes
  Type=GENERIC
  Generic...
  IP...
```

When you open an "Out filter," a menu like this one appears:

```
50-401 IP Data
 Out filter 01
 >Valid=Yes
  Type=GENERIC
  Generic...
  IP...
```

6 To activate the filter, set Valid=Yes.

For the MAX to apply the filter, you must activate it.

7 To define a generic filter, set Type=Generic; to define an IP filter, set Type=IP.

A Generic filter defines bits and bytes within a packet, and specifies locations and values that can appear in any packet. An IP filter indicates IP-specific packet characteristics, such as address, mask, and port. IP filter rules relate only to TCP, IP, and UDP packets.

Defining generic filter conditions

If the Type=Generic, you can define generic filter rules. Table 4-1 shows the parameters you can set.

Table 4-1. Generic filter rules

Location	Parameters with sample values
Ethernet>Filters>Any Filter profile>Input filters> 01 to 12>Generic Ethernet>Filters>Any Filter profile>Output filters> 01 to 12>Generic	Forward=No Offset=14 Length=8 Mask=ffffffffffffffff Value=aaa030000000080f3 Compare=Equals More=No

To specify generic filter rules, follow these steps:

1 Set the Forward parameter.

The Forward setting determines which packets the MAX transmits and receives.

When you set Forward=Yes, the MAX forwards a packet if it meets the filter definition. When you set Forward=No, the MAX drops a packet it if meets the filter definition.

2 Set the Length, Offset, Mask, and Value parameters.

The Length parameter indicates the number of bytes in a packet. The Offset parameter specifies the starting position of the bytes the filter examines; the MAX ignores the portion of the packet that exceeds the Length specification. In other words, the Offset parameter hides the left-most bytes of data, while the Length parameter hides the right-most bytes of data.

The Mask value consists of the same number of bytes as the Length parameter. A mask hides the part of a number that appears behind the binary zeroes in the mask; for example, if Mask=ffff0000 in hexadecimal format, the MAX uses only the first 16 binary digits in the comparison, because f=1111 in binary format. The MAX applies the value of the Mask parameter before comparing the bytes to the setting of the Value parameter.

3 Set the Compare parameter.

This parameter specifies how the MAX compares a packet's contents to the Value specified in the filter. After applying the Offset, Mask, and Length values to reach the appropriate location in a packet, the MAX compares the contents of that location to the Value parameter.

- If you set Compare to Equals (the default) and the packet data is identical to the value specified by Value, the MAX applies the filter.
- If you set Compare to NotEquals, the MAX applies the filter if the packet data is not identical to the value specified by Value.

4 Set the More parameter.

This parameter specifies whether the current filter is linked to the one immediately following it. If More=Yes, the MAX can examine multiple non-contiguous bytes within a packet by "marrying" the current filter to the next one. The MAX applies the next filter before making a decision on whether to forward or drop the packet. The match occurs only if *both* sets of non-contiguous bytes contain the specified values. If More=No, the MAX bases its decision to forward or drop the packet based on whether the packet matches the definition in the present filter.

Defining IP filter rules

If Type=IP, you can define filter rules relevant only to TCP, IP, and UDP data packets, including bridged packets.

An IP filter can examine source address, destination address, and IP protocol type and port. Table 4-2 shows the filter rules you can specify in an IP filter.

Table 4-2. IP filter rules

Location	Parameters with sample values
Ethernet>Filters>Any Filter profile>Input filters> 01 to 12>Ip Ethernet>Filters>Any Filter profile>Output filters> 01 to 12>Ip	Forward=Yes Src Mask=255.255.255.192 Src Adrs=192.100.40.128 Dst Mask=0.0.0.0 Dst Adrs=0.0.0.0 Protocol=0 Src Port Cmp=None Src Port #=N/A Dst Port Cmp=None Dst Port #=N/A TCP Estab=N/A

To specify IP filter rules, follow these steps:

1 Set the Forward parameter.

The Forward setting determines which packets the MAX transmits and receives.

When you set Forward=Yes, the MAX forwards a packet if it meets the filter definition. When you set Forward=No, the MAX drops a packet it if meets the filter definition.

2 Set the Src Adrs parameter.

This parameter specifies the address to which the MAX compares a packet's source address. Enter the address in dotted decimal format. The null address (0.0.0.0) is the default. If you accept the default, the MAX does not use the source address as a filtering criterion.

3 Set the Src Mask parameter.

This parameter specifies the bits the MAX should mask when comparing a packet's source address to the value of the Src Adrs parameter. A mask hides the part of a number that appears behind each binary 0 (zero) in the mask; the MAX uses only the part of a number that appears behind each binary 1 for comparison. The MAX applies the mask to the address using a logical AND after the mask and address are both translated into binary format.

The value 0 (zero) hides all bits, because the decimal value 0 is the binary value 00000000; the value 255 does not mask any bits, because the decimal value 255 is the binary value 11111111. The null address (0.0.0.0) is the default; this setting indicates that the MAX masks all bits.

To specify a single source address, set Src Mask=255.255.255.255 and set Src Adrs to the IP address that the MAX uses for comparison.

4 Set the Dst Adrs parameter.

This parameter specifies the address to which the MAX compares a packet's destination address. Enter the address in dotted decimal format. The null address (0.0.0.0) is the default. If you accept the default, the MAX does not use the destination address as a filtering criterion.

5 Set the Dst Mask parameter.

This parameter specifies the bits the MAX should mask when comparing a packet's destination address to the value of the Dst Adrs parameter.

6 Set the Protocol parameter.

This parameter identifies a specific TCP/IP protocol; for example, 6 specifies a TCP packet. Common protocols are listed below, but protocol numbers are not limited to this list. For a complete list, see the section on Well-Known Port Numbers in RFC 1700, *Assigned Numbers*, by Reynolds, J. and Postel, J., October 1994.

- 1 — ICMP
- 5 — STREAM
- 8 — EGP
- 6 — TCP
- 9 — Any private interior gateway protocol (such as Cisco's IGRP)
- 11— Network Voice Protocol
- 17 — UDP
- 20 — Host Monitoring Protocol
- 22 — XNS IDP
- 27 — Reliable Data Protocol
- 28 — Internet Reliable Transport Protocol
- 29 — ISO Transport Protocol Class 4
- 30 — Bulk Data Transfer Protocol
- 61 — Any Host Internal Protocol

7 Set the Src Port # parameter.

This parameter specifies the port number to which the MAX compares the packet's source port number. The Src Port Cmp criterion determines how the MAX carries out the comparison.

You can enter a number between 0 and 65535. The default setting is 0 (zero). If you accept the default, the MAX does not use the source port number as a filtering criterion.

8 Set the Src Port Cmp parameter

This parameter specifies the type of comparison the MAX makes when using the Src Port # parameter. You can specify one of these settings:

- None specifies that the MAX does not compare the packet's source port to the value specified by Src Port #.

  None is the default.
- Less specifies that port numbers with a value less than the value specified by Src Port # match the filter.
- Eql specifies that port numbers equal to the value specified by Src Port # match the filter.
- Gtr specifies that port numbers with a value greater than the value specified by Src Port # match the filter.
- Neq specifies that port numbers not equal to the value specified by Src Port # match the filter.

This parameter works only for TCP and UDP packets. You must set Src Port Cmp=None if the Protocol parameter is not set to 6 (TCP) or 17 (UDP).

9 Set the Dst Port # parameter.

This parameter specifies the port number to which the MAX compares the packet's destination port number. The Dst Port Cmp criterion determines how the MAX carries out the comparison.

You can enter a number between 0 and 65535. The default setting is 0 (zero). If you accept the default, the MAX does not use the destination port number as a filtering criterion.

10 Set the Dst Port Cmp parameter.

This parameter specifies the type of comparison the MAX makes when using the Dst Port # parameter. You can specify any of the settings available for Src Port Cmp (as described in Step 8).

The Dst Port Cmp parameter works only for TCP and UDP packets. You must set Dst Port Cmp=None if the Protocol parameter is not set to 6 (TCP) or 17 (UDP).

11 Set the TCP Estab parameter.

This parameter specifies whether the filter should match only established TCP connections. You can specify one of these settings:

– Yes specifies that you want the filter to match only those TCP connections that are established.

– No specifies that you want the filter to match both initial and established TCP connections.

No is the default.

The TCP Estab parameter does not apply if the Protocol field is set to any value other than 6 (TCP).

Specifying a data filter in a profile

Using the Data Filter parameter, you can specify a data filter in an Answer profile, a Connection profile, or an Ethernet profile. Keep this information in mind:

- The Answer profile and Connection profile specify the packets that can cross the WAN interface.
- The Ethernet profile specifies the packets that can cross the local Ethernet interface.
- The MAX uses the Answer profile specification only if no Connection profile exists for the caller.
- If profile Reqd=Yes in the Answer profile, Data Filter does not apply in the Answer profile.

Specifying a data filter for the WAN interface

To define which packets can cross the WAN interface, follow these steps:

1 Open a Connection profile (under Ethernet > Connections) or the Ethernet > Answer menu.

2 Open the Session Options menu.

3 Using the Data Filter parameter, specify a data filter.

When you set Data Filter to 0 (zero), the MAX forwards all data packets.

The MAX applies a call filter after applying a data filter; only those packets that the data filter forwards can reach the call filter. If IPX client bridging is in use (Handle IPX=Client), set the Data Filter parameter to 0 (zero).

4 Close the Connection profile or Answer profile, saving your changes.

A filter applied to a Connection or Answer profile takes effect only when the connection goes from an offline state to a call-placed state.

Specifying a data filter for the local Ethernet interface

To define which packets can cross the local Ethernet interface, follow these steps:

1. Open the Ethernet > Mod Config > Ether Options menu.
2. Using the Filter parameter, specify a data filter.

   When you set Filter to 0 (zero), the MAX forwards all data packets.

   The MAX applies a call filter after applying a data filter; only those packets that the data filter forwards can reach the call filter. If IPX client bridging is in use (Handle IPX=Client), set the Filter parameter to 0 (zero).
3. Save your changes.

A filter applied to the Ethernet interface takes effect immediately. If you change the Filter profile definition, the new filters apply as soon as you save the Filter profile.

Sample filters

This section provides a step-by-step examples of creating Filter profiles and defining IP filters for network security purposes.

A sample IP filter to prevent address spoofing

IP address spoofing is a technique in which outside users pretend to be from the local network in order to obtain unauthorized access. This section shows how to define an IP data filter whose purpose is to prevent spoofing of local IP addresses. You can also use Password profiles to prevent IP address spoofing; for details, see “Using Name/Password profiles to prevent IP address spoofing” on page 3-26.

In this example, the filter first defines input filters that drop packets whose source address is on the local IP network or the loopback address (127.0.0.0). In effect, these filters say: “If you see an inbound packet with one of these source addresses, drop the packet.” The third input filter defines every other source address (0.0.0.0) and specifies “Forward everything else to the local network.”

The data filter then defines an output filter that specifies: “If an outbound packet has a source address on the local network, forward it; otherwise, drop it.” The MAX drops all outbound packets with a non-local source address.

This example assumes a local IP network address of 192.100.50.128, with a subnet mask of 255.255.255.192. Of course, you use your own local IP address and netmask when defining a Filter profile.

To define an IP data filter to prevent address spoofing, follow these steps:

1. Select an unnamed Filter profile in the Filters menu, and press Enter.

   For example, select 50-404.

```
50-400 Filters
50-401 IP Data
```

```
 50-402 NetWare Data
 50-403 AppleTalk Data
 >50-404
 50-405
 50-406
 50-407
 50-408
 50-409
 50-410
 50-411
 50-412
```

2 Assign a name to the Filter profile.

For example:

```
Name=no spoofing
50-404
>Name=no spoofing
 Input filters...
 Output filters...
```

3 Open the Input Filters submenu

4 Open In filter 01.

```
50-404
 In filter 01
 >Valid=Yes
  Type=IP
  Generic...
  IP...
```

5 Set Valid=Yes and Type=IP.

6 Open the IP submenu and specify the following conditions:

```
 Ip...
 >Forward=No
  Src Mask=255.255.255.192
  Src Adrs=192.100.50.128
  Dst Mask=0.0.0.0
  Dst Adrs=0.0.0.0
  Protocol=0
  Src Port Cmp=None
  Src Port #=N/A
  Dst Port Cmp=None
  Dst Port #=N/A
  TCP Estab=N/A
```

The Src Mask parameter specifies the local netmask The Src Adrs parameter specifies the local IP address. If an incoming packet has the local address, the MAX does not forward it onto the Ethernet.

7 Close In filter 01, and then open In filter 02.

8 Set Valid=Yes and Type=IP.

9 Open the IP submenu and specify the following conditions:

```
 Ip...
 >Forward=No
```

```
 Src Mask=255.0.0.0
 Src Adrs=127.0.0.0
 Dst Mask=0.0.0.0
 Dst Adrs=0.0.0.0
 Protocol=0
 Src Port Cmp=None
 Src Port #=N/A
 Dst Port Cmp=None
 Dst Port #=N/A
 TCP Estab=N/A
```

These conditions specify the loopback address in the Src Mask and Src Adrs fields. If an incoming packet has this address, the MAX does not forward it onto the Ethernet.

10 Close In filter 02, and then open In filter 03.

11 Set Valid=Yes and Type=IP.

12 Open the IP submenu and specify the following conditions:

```
Ip...
>Forward=Yes
 Src Mask=0.0.0.0
 Src Adrs=0.0.0.0
 Dst Mask=0.0.0.0
 Dst Adrs=0.0.0.0
 Protocol=0
 Src Port Cmp=None
 Src Port #=N/A
 Dst Port Cmp=None
 Dst Port #=N/A
 TCP Estab=N/A
```

These conditions specify every other source address (0.0.0.0) If an incoming packet has any non-local source address, the MAX does not forward it onto the Ethernet.

13 Close In filter 03, and then return to the top level of the “no spoofing” Filter profile.

14 Open the Output Filters submenu, and select Out filter 01.

15 Set Valid=Yes and Type=IP.

16 Open the IP submenu and specify the following conditions:

```
Ip...
>Forward=Yes
 Src Mask=255.255.255.192
 Src Adrs=192.100.40.128
 Dst Mask=0.0.0.0
 Dst Adrs=0.0.0.0
 Protocol=0
 Src Port Cmp=None
 Src Port #=N/A
 Dst Port Cmp=None
 Dst Port #=N/A
 TCP Estab=N/A
```

The Src Mask parameter specifies the local netmask The Src Adrs parameter specifies the local IP address. If an outgoing packet has a local source address, the MAX forwards it.

17 Close the Filter profile.

A sample IP filter for more complex security issues

This section illustrates some of the issues you may need to consider when writing your own IP filters. The sample filter presented here does not address the fine points of network security. You may want to use this sample filter as a starting point and augment it to address your security requirements.

In this example, the local network supports a Web server and the administrator needs to carry out these tasks:

- Provide dial-in access to the server's IP address .
- Restrict dial-in traffic to all other hosts on the local network.

However, many local IP hosts need to dial out to the Internet and use IP-based applications such as Telnet or FTP; therefore, their response packets need to be directed appropriately to the originating host. In this example, the Web server's IP address is 192.9.250.5.

The sample data filter appears in Connection profiles. Each input filter is defined in this way:

- In filter 01

  The first input filter specifies the Web server's IP address as the destination and sets IP forward to Yes. The MAX forwards all IP packets received with that destination address.

```
In filter 01...Ip...Forward=Yes
In filter 01...Ip...Src Mask=0.0.0.0
In filter 01...Ip...Src Adrs=0.0.0.0
In filter 01...Ip...Dst Mask=255.255.255.255
In filter 01...Ip...Dst Adrs=192.9.250.5
In filter 01...Ip...Protocol=6
In filter 01...Ip...Src Port Cmp=None
In filter 01...Ip...Src Port #=N/A
In filter 01...Ip...Dst Port Cmp=Eql
In filter 01...Ip...Dst Port #=80
In filter 01...Ip...TCP Estab=No
```

- In filter 02

  The second input filter specifies TCP packets (Protocol=6) *from* any address and *to* any address. The filter forwards them if the destination port is greater than the source port. For example, Telnet requests go out on port 23 and responses come back on some random port greater than port 1023. So, this filter defines packets coming back to respond to a user's request to Telnet to a remote host.

```
In filter 02...Ip...Forward=Yes
In filter 02...Ip...Src Mask=0.0.0.0
In filter 02...Ip...Src Adrs=0.0.0.0
In filter 02...Ip...Dst Mask=0.0.0.0
In filter 02...Ip...Dst Adrs=0.0.0.0
In filter 02...Ip...Protocol=6
In filter 02...Ip...Src Port Cmp=None
In filter 02...Ip...Src Port #=N/A
In filter 02...Ip...Dst Port Cmp=Gtr
In filter 02...Ip...Dst Port #=1023
In filter 02...Ip...TCP Estab=No
```

- In filter 03

The third input filter specifies UDP packets (Protocol=17) *from* any address and *to* any address. The filter forwards them if the destination port is greater than the source port. For example, suppose a RIP packet goes out as a UDP packet to destination port 520. The response to this request goes to a random destination port greater than 1023.

```
In filter 03...Ip...Forward=Yes
In filter 03...Ip...Src Mask=0.0.0.0
In filter 03...Ip...Src Adrs=0.0.0.0
In filter 03...Ip...Dst Mask=0.0.0.0
In filter 03...Ip...Dst Adrs=0.0.0.0
In filter 03...Ip...Protocol=17
In filter 03...Ip...Src Port Cmp=None
In filter 03...Ip...Src Port #=N/A
In filter 03...Ip...Dst Port Cmp=Gtr
In filter 03...Ip...Dst Port #=1023
In filter 03...Ip...TCP Estab=No
```

- In filter 04

  The fourth input filter specifies unrestricted pings and traceroutes. ICMP does not use ports like TCP and UDP, so a port comparison is unnecessary.

```
In filter 04...Ip...Forward=Yes
In filter 04...Ip...Src Mask=0.0.0.0
In filter 04...Ip...Src Adrs=0.0.0.0
In filter 04...Ip...Dst Mask=0.0.0.0
In filter 04...Ip...Dst Adrs=0.0.0.0
In filter 04...Ip...Protocol=1
In filter 04...Ip...Src Port Cmp=None
In filter 04...Ip...Src Port #=N/A
In filter 04...Ip...Dst Port Cmp=None
In filter 04...Ip...Dst Port #=N/A
In filter 04...Ip...TCP Estab=No
```

Setting Up Security-Card Authentication

5

This chapter covers these topics:

How security cards work

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

You can set up a remote authentication server using security cards to work with RADIUS or, in the case of the ACE/Server and Defender server, directly, without RADIUS. For information on how security card authentication using the SecurID ACE/Server without RADIUS works, see "Configuring direct SecurID ACE authentication" on page 5-18 and "Configuring direct Defender server authentication" on page 5-25.

Security-card authentication with RADIUS

Figure 5-1 illustrates an environment that includes an Ascend Pipeline as the calling unit, an NAS (the MAX), a RADIUS server, and an external authentication server.

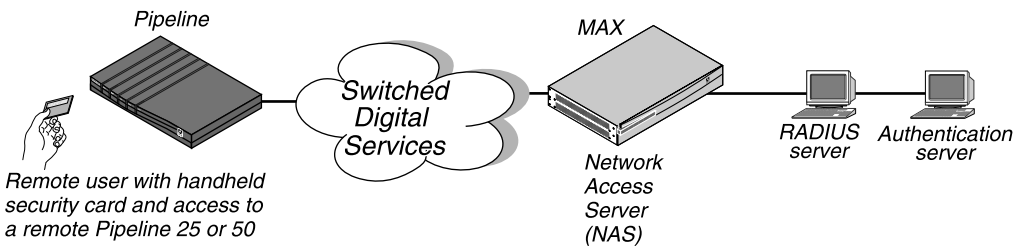

Figure 5-1. Using an external authentication server with RADIUS

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

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

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

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

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

The MAX is a client of the RADIUS server.

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

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

In this 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 to the user dialing in.

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

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

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

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

8 The user enters the current password obtained from the security card in response to the challenge message; this password travels back through the NAS and the RADIUS server to the authentication server.

9 The authentication server sends a response to the RADIUS server, specifying whether the user has entered the proper username 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 terminates the call.

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

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

Direct SecurID ACE authentication

You can also configure the MAX to use ACE/Server authentication without using RADIUS. The authentication process is different from authentication using the RADIUS server, and supports authentication of terminal server users only (not dial-in PPP users using the App Server). If your installation requires support for dial-in PPP users, you will need to configure it with RADIUS. See "Configuring the MAX to recognize the authentication server" on page 5-5.

This method is useful for installations where other RADIUS features are not required, since it decreases the complexity of the system, making it easier to configure and maintain. In addition, Direct ACE/Server authentication supports the New PIN Mode feature, which allows a dial-in user to change the personal identifying number (PIN). For information on the New PIN Mode feature, see "New PIN Mode" on page 5-17.

You can also configure ACE/Server authentication to use PAP-TOKEN-CHAP authentication. For more information, see "Configuring PAP-TOKEN-CHAP using direct ACE authentication" on page 5-24.

Understanding security-card authentication methods

You can set up SafeWord and ACE security-card authentication of incoming calls using PAP-TOKEN, CACHE-TOKEN, or PAP-TOKEN-CHAP authentication. You can also specify that users request one of these authentication types when dialing out through the MAX. This section provides an overview of token-based authentication.

- PAP-TOKEN

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

- CACHE-TOKEN

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

- PAP-TOKEN-CHAP

  PAP-TOKEN-CHAP 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 only the initial connection needs to be verified by a hand-held security card. Any additional channels are verified by CHAP only.

Setting up incoming security-card calls with RADIUS

You can configure all security-card calls to work with RADIUS. When the MAX receives an incoming security-card password from a user, it must forward the authentication request to RADIUS; the RADIUS server, in turn, forwards the request to an ACE or SafeWord server. If you are using RADIUS, the security-card caller must have a valid RADIUS user profile. Therefore, you must carry out both of these tasks:

- Configure the MAX to communicate with the RADIUS server.
- Configure a RADIUS user profile for the dial-in user.

For details on these tasks, see the *MAX RADIUS Configuration Guide*.

You can set up the SecurID ACE/Server for use without RADIUS. This method does not permit authentication of PPP dial-in users using the APP Server. To configure the Ace/Server to use PAP-TOKEN-CHAP authentication, see "Configuring PAP-TOKEN-CHAP using direct ACE authentication" on page 5-24.

If you are not using RADIUS see "Configuring direct Defender server authentication" on page 5-25.

Setting up outgoing security-card calls

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

To set up your site for outgoing security-card calls, you must complete these tasks:

1. Configure the MAX to recognize the security-card authentication server.
2. Configure the MAX to recognize the APP Server utility for each security-card user.

   The APP Server utility enables a user to respond to token password challenges received from an external authentication server, such as a Security Dynamics (ACE) or Enigma Logic (SafeWord) server. To allow users to supply token passwords from a host on the local network, you must configure the MAX to communicate with the APP Server utility on that host.
3. Set up dial-out connections in one or more Connection profiles.
4. Install the APP Server utility on each user's computer.
5. Dial a connection to the remote site.

Configuring the MAX to recognize the authentication server

For the MAX to communicate with the authentication server, you must set the parameters in Table 5-1.

Table 5-1. Authentication server parameters

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

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

- The MAX must request PAP-TOKEN authentication

  For details, see "Requesting PAP-TOKEN authentication" on page 5-7.
- You must have the APP Server utility running on a UNIX or Windows workstation on the local network.

  For details on installing the APP Server utility, see "Installing the APP Server utility" on page 5-9.

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

1. Open the Ethernet>Mod Config>DNS menu.
2. For the Password Host parameter, specify the IP address of the authentication server on the remote network.
3. Open the Ethernet>Mod Config>Auth menu.

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

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

5 Set Password Server=Yes.

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

6 Save your changes.

Configuring the MAXto recognize the APP Server utility

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

Table 5-2 lists the APP Server parameters.

Table 5-2. APP Server parameters

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

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

1 Open the Ethernet>Mod Config>Auth menu.

2 Set APP Server=Yes.

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

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

   For example, you must enter this setting:

   `APP Host=10.65.212.1`

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

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

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

5 Save your changes.

Setting up a dial-out connection to a secure site

For the MAX to place calls to an NAS at a secure site, it needs the appropriate Connection profile requesting a token-based authentication type. The authentication type configured in the calling unit affects

- How the MAX transmits the token passwords
- How the user must respond when the system adds channels to an established session

The calling unit requests an authentication type, but the RADIUS daemon and RADIUS user profile accessed by the answering NAS determine the access mode to use.

Requesting PAP-TOKEN authentication

When PAP-TOKEN authentication is in use, the MAX sends the dial-out user's password in the clear (via PAP); because the password is used for one time only, sending the password in the clear does not constitute 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 system challenges the user for a password whenever it adds a channel to a call.

To request PAP-TOKEN authentication for an outgoing call, use the parameters listed in Table 5-3.

Table 5-3. PAP-TOKEN parameters

Location	Parameters with sample values
Ethernet>Connections>Any Connection profile>Encaps Options	Send Auth=PAP-TOKEN Send PW=*SECURE*

To request PAP-TOKEN authentication in an outgoing Connection profile, follow these steps:

1. Open the Ethernet>Connections menu.
2. Open the Connection profile.
3. Open the Encaps Options submenu.
4. Set Send Auth=PAP-TOKEN.
   The Send Auth parameter specifies the authentication type requested by the caller.
5. For the Send PW parameter, specify a password.
   The MAX sends the value of the Send PW parameter as part of the initial session negotiation. If the session then presents a password challenge, the user types in the current one-time-only password displayed on the security card.
6. Save your changes.

Requesting CACHE-TOKEN authentication

CACHE-TOKEN uses CHAP and caches the initial password for re-use in authenticating additional channels. The RADIUS profile at the remote end must contains attributes specifying

how long the token remains cached. For complete information on setting up the RADIUS user profile at the remote end, see the *MAX RADIUS Configuration Guide*.

To request CACHE-TOKEN authentication for an outgoing call, use the parameters listed in Table 5-4.

Table 5-4. CACHE-TOKEN parameters

Location	Parameters with sample values
Ethernet>Connections>Any Connection profile>Encaps Options	Send Auth=CACHE-TOKEN Send PW=*SECURE*

To request CACHE-TOKEN authentication in an outgoing Connection profile, follow these steps:

1. Open the Ethernet>Connections menu.
2. Open the Connection profile.
3. Open the Encaps Options submenu.
4. Set Send Auth=CACHE-TOKEN.
   The Send Auth parameter specifies the authentication type requested by the caller.
5. For the Send PW parameter, specify a password.
   The MAX sends the value of the Send PW parameter as part of the initial session negotiation. The system prompts the user for a token password and uses this password to authenticate the base channel of the call via CHAP. The RADIUS server caches the encrypted password for the period specified by the Ascend-Token-Expiry attribute, or for the amount of idle time specified by the Ascend-Token-Idle attribute. When the system adds channels to a call or places a new call, it uses the cached password to authenticate the channels.
6. Save your changes.

Requesting PAP-TOKEN-CHAP authentication

In PAP-TOKEN-CHAP authentication, the remote NAS uses the dynamic password the user supplies to authenticate the base channel of the call. The MAX sends the dial-out user's password in the clear (via PAP). When the MAX adds additional channels to the base channel of the call, it uses CHAP authentication for the new channels. CHAP sends encrypted passwords, so it can take the auxiliary password specified by the Aux Send PW parameter and transmit it securely.

If the calling unit requests PAP-TOKEN-CHAP authentication, but the RADIUS user profile at the remote end is not set up for PAP-TOKEN-CHAP, the remote end uses PAP-TOKEN authentication instead.

To request PAP-TOKEN -CHAP authentication for an outgoing call, use the parameters listed in Table 5-5.

Table 5-5. PAP-TOKEN-CHAP parameters

Location	Parameters with sample values
Ethernet>Connections>Any Connection profile>Encaps Options	Send Auth=PAP-TOKEN-CHAP Send PW=*SECURE* Aux Send PW=*SECURE*

To request PAP-TOKEN-CHAP authentication in an outgoing Connection profile, follow these steps:

1. Open the Ethernet>Connections menu.
2. Open the Connection profile.
3. Open the Encaps Options submenu.
4. Set Send Auth=PAP-TOKEN-CHAP.

   The Send Auth parameter specifies the authentication type requested by the caller.
5. For the Send PW parameter, specify a password.

   The MAX sends the value of the Send PW parameter as part of the initial session negotiation. If the session then presents a password challenge, the user types in the current one-time-only password displayed on the security card.
6. For the Aux Send PW parameter, specify an auxiliary password.

   When the MAX adds additional channels to the base channel of the call, CHAP encrypts the auxiliary password specified by the Aux Send PW parameter and transmits it to the remote end.
7. Save your changes.

Installing the APP Server utility

The APP Server utility enables a user to respond to token password challenges from an external authentication server, such as a Security Dynamics (ACE) or Enigma Logic (SafeWord) server.

Previous versions of the APP Server utility enabled a single user to respond to password challenges from a remote ACE or SafeWord server. The current version supports multiple tokens—for a user name as well as the current password—so more than one user can use the APP Server to respond to password challenges.

Getting the right version of the utility

The APP Server utility is available for five platforms: DOS, Windows 3.1, Windows 95, Windows NT, and UNIX. The utility resides on ftp.ascend.com as a single tar archive that contains all five versions of the utility.

The tar file expands into five directories, one for each version of the utility:

- The DOS and Windows executable files are:
  - appsrvds.exe (for DOS)
  - appsrv31.exe (for Windows 3.1)

  - appsrv95.exe (for Windows 95)
  - appsrvnt.exe (for Windows NT)
- The directory contents for the Windows 95 and Windows NT versions are compressed.
- The UNIX utility is supplied as source files.

Creating banner text for the password prompt

This release incorporates a banner display facility. The banner text displays with the password prompt on the APP Server screen when you receive a challenge message. You can use the sample banner file included with this release. Or, you can specify the banner text in an ASCII file named appsrvr.ini. You can create the text file using any text editor; the file must reside in the directory in which the APP Server utility is located.

The banner can contain up to 200 characters and five lines of text. The first line of the file must contain the text "[BANNER]". For example, you might set up the file in this way:

```
[BANNER]
line1=The security password has changed. Please consult your
line2=card and enter the current password now.
line3=You have 60 seconds to enter the new password.
```

Installing the APP Server utility for DOS

To install the APP Server utility for DOS, follow these steps:

1. Create an \ascend directory below the root directory.
2. Copy appsrvds.exe into the \ascend directory.
3. If the appsrvr.ini file exists, copy the file into the \ascend directory.
   For more information on the appsrvr.ini file, see "Creating banner text for the password prompt" on page 5-10.
4. Open the autoexec.bat file and add a command line to start appsrvds.exe.
   The appsrvds.exe DOS utility does not require an IP stack or IP address, but it does require an ODI driver.
   You must put the command line for appsrvds.exe *after* the line that loads the network ODI driver and *before* the line that loads the network protocol stack (TCP/IP, IPX, or another supported protocol). For example:
   ```
   C:\novell\lsl.com
   C:\novell\xxxodi.com
   C:\ascend\appsrvds.exe
   REM Protocol Stack is loaded next
   ```
5. Close the autoexec.bat file.
6. Reboot your machine.

You can specify these options on the autoexec.bat command line:

- /t — Specifies a time delay between connection attempts (in seconds).
- /y — Specifies the number of cycle counts (attempts to connect) before timeout.
- /m —Specifies the MAC address (in decimal format) of the PC running the utility.
- /p — Specifies a UDP port number for communicating with the MAX.

- /b — Specifies a UDP port for broadcast messages.
- /f — Suppresses the call at startup.
- /d — Disconnects the call.
- /c — Specifies the name of the Connection profile to use to connect to the remote secure network.
- /? —Displays a 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 the /p or /b to specify the same port.

If you do not specify any command-line variables, the APP Server utility uses the following default values:

- Time delay between connection attempts = 20 seconds
- Number of cycles =3 (3 times 20 seconds)
- APP Server PC MAC address = none (zeros)
- UPD port to use = 7001
- Broadcast UDP port =communication UDP port
- APP Server will force a connection upon execution.

Note: A Connection profile is required to log into the remote secure network, so if the APP Server line in the autoexec.bat file does not specify which Connection profile to use, the system prompts you for a Connection profile name as the system boots.

For example, consider this command line:

```
C:\ascend\appsrvds.exe /cChicago /t20 /p7005
```

This line specifies a Connection profile named “Chicago,” assigns a 20-second time delay between connection attempts, and designates UDP port 7005 for communicating with the MAX.

Now, consider this command line:

```
C:\ascend\appsrvds.exe /cChicago /m00805110C7A44 /p7523 /t65 /
b7112
```

This line specifies a Connection profile named “Chicago,” specifies 00805110C7A44 as the MAC address of the PC running the utility, designates UDP port 7523 for communicating with the MAX, assigns a 65-second time delay between connection attempts, and designates port 7112 for sending broadcast messages (to initiate a call).

Installing the APP Server utility for Windows 3.1

To install the APP Server on a Windows 3.1 workstation, follow these steps:

1 Create an \ascend directory below the root directory.

2 Copy appsrv31.exe into the \ascend directory.

3 If the appsrv31.ini file exists, copy that file into the \ascend directory.

For details on the appsrvr.ini file, see “Creating banner text for the password prompt” on page 5-10.

4 Copy ctl3d.dll into the Windows \system directory.

We recommend adding the APP Server utility to the startup group (provided that you connect to the network as part of normal system startup). If you do not add the APP Server utility to your Startup group, you can launch the utility manually by double-clicking its icon.

To create an icon and add the APP Server to the startup group, follow these steps:

1 Create a new program group in your Program Manager.
Choose File>New>Program Group and type:
Ascend

2 Create an icon for appsrv31.exe in your Program Manager.
Choose File > New > Program Item.

3 To launch the APP Server utility when you start Windows, place the appsrv31.exe icon in your Startup group.

4 Reboot your machine.

Installing the APP Server utility for Windows 95

To install the APP Server on a Windows 95 workstation, follow these steps:

1 Copy the file xas-w95.exe into a temporary directory.
xas-w95.exe is a self-extracting zip file.

2 Execute the file from the DOS shell.
The zip file expands to several files that comprise the Windows 95 Setup program.

3 From the Start menu, run the Setup program in the temporary directory.

4 Follow the prompts, selecting the directory in which to install APP Server for Windows 95.

APP Server for Windows 95 starts automatically whenever the system reboots. You can close the APP Server utility in a session, but next time you reboot the system, the utility starts up again. To permanently remove or disable the APP Server utility, you must edit the Windows 95 Registry to remove the key that refers to appsrv95.exe.

Installing the APP Server utility for Windows NT

To install the APP Server on a Windows NT workstation, follow these steps:

1 Copy the file xas-nt.exe into a temporary directory.
xas-nt.exe is a self-extracting zip file.

2 Execute the file from the DOS shell.
The zip file expands to several files that comprise the Windows NT Setup program.

3 From the Start menu, run the Setup program in the temporary directory.

4 Follow the prompts, selecting the directory in which to install APP Server for Windows NT.

APP Server for Windows NT starts automatically whenever the system reboots. You can close the APP Server utility in a session, but next time you reboot the system, the utility starts up again.

There are three icons provided during installation that enable you to temporarily disable the APP Server, manually control when it runs, or remove it from the system.

- Activate service icon

  Running the activate service icon restarts the utility if it is running, or activates it for the first time.

- Remove service icon

  Running the remove service icon stops the utility if it is running and removes it from the service database. It no longer appears as a service in the Services applet on the Control Panel.

- Uninstall service icon

  Running the uninstall service icon causes the files, icons, program groups, and registry entries to be removed from the system.

Installing the APP Server utility for UNIX

To install the APP Server utility on a UNIX host:

1 Edit the Makefile appropriately for your operating system and compiler.

2 Compile the appsrvr source file (make).

3 Add a line to the /etc/services file assigning UDP port 7001 to the APP Server utility.

To use the default UDP port 7001, add this line to the /etc/services file to document that the port is now in use:

```
appServer  7001/udp
```

If port 7001 is already assigned for 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  port_num/udp
```

The *port_num* argument is the port number the utility uses. Make sure you specify the same number using the APP Port parameter on the MAX.

4 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 the specified IP address.

5 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 by typing this command:

```
./appsrvr –b
```

The –b argument sets a socket option to allow broadcast transmissions and inhibits the utility's complaints about receiving invalid APP frame types 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).

Dialing a connection to a secure site

This sections describes how to initiate a connection to a remote network from different types of platforms.

Connecting to a remote network from the terminal server

To make an outgoing call to a secure site from a terminal server session, follow the steps described in this section. For a modem connection, begin the process at Step 2.

1 At the terminal server prompt, enter this command:

```
set password
```

The following message displays:

```
Entering Password Mode...
The prompt changes to the display following text:
[^C to exit] Password Mode>
```

2 Bring up a connection to the secure site in one of these ways:

- Start a program that requires a connection to a host on the remote network.
- Use the DO menu on the MAX.
- Dial the remote NAS via modem

The remote NAS returns a challenge prompt that looks like this one:

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

hostname is the name of the NAS you are calling; it is optional on some systems.

If the Send Auth parameter is configured incorrectly, no challenge prompt appears, or you see an error message such as this one:

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

3 At the challenge prompt, enter the password obtained from your security card.

You have 60 seconds to enter the password correctly. When you enter the correct password, the MAX establishes the connection to the secure network. If you do not specify the correct password within 60 seconds, the login attempt times out. If you enter the password incorrectly, the challenge prompt displays again, up to three times.

4 To return to normal terminal server operations, press Ctrl-C at the Password Mode prompt.

Connecting to a remote network from a DOS workstation

To initiate a connection to a remote secure network, you reboot the PC. After the initial session negotiation, the remote ACE or SafeWord server returns a password challenge that looks similar to this one:

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

<hostname> is the name of the NAS the user is calling; it is optional on some systems.

If the Send Auth parameter is configured incorrectly, no challenge prompt appears, or you see an error message such as this one:

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

You have 60 seconds to enter the password correctly. When you enter the correct password, the MAX establishes the connection to the secure network. If you do not specify the correct password within 60 seconds, the login attempt times out. If you enter the password incorrectly, the challenge prompt displays again, up to three times.

If more than one user uses the APP Server to log into a remote secure network through the MAX, each user must include a user name in this format:

password.username

Connecting to a remote network from a Windows workstation

The user interface is the same for all Windows versions of the APP Server utility. To use the Windows utility, follow these steps:

1. Start the utility by using the Services applet on the Control Panel.
2. In the dialog that displays, click Connect.
   The Settings dialog box opens.
3. Enter the name of the Connection profile used to log into the remote secure network.
4. Enter your username.
   You can specify up to 32 characters; you cannot enter spaces.
5. Click OK.
   After the initial session negotiation, the remote ACE or SafeWord server returns a password challenge; the challenge displays in its own dialog box. You have 60 seconds to obtain the current dynamic password from the security card and enter it correctly.
6. Type the current password and click OK.
7. To log out of the remote network, click Disconnect.
8. In the dialog that displays, type the name of the Connection profile that defines your connection to the remote network; then, click OK.

Connecting to a remote network from a UNIX workstation

When you start an application that requires a connection to a host on a secure network, the MAX initiates a call. After the initial session negotiation, the remote ACE or SafeWord server returns a password challenge that looks similar to this one:

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

hostname is the name of the NAS you are calling; it is optional on some systems.

If the Send Auth parameter is configured incorrectly, no challenge prompt appears, or you see an error message such as this one:

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

You have 60 seconds to enter the password correctly. When you enter the correct password, the MAX establishes the connection to the secure network. If you do not specify the correct password within 60 seconds, the login attempt times out. If you enter the password incorrectly, the challenge prompt displays again, up to three times.

If more than one user uses the APP Server to log into a remote secure network through the MAX, each user must include a user name in this format:

password.username

How the SecurID ACE/Server works without RADIUS

Users dialing into a MAX who are authenticated by a SecurID ACE server directly (without RADIUS) can specify one of the MAX unit's local profiles to be used for session parameters. When a user dials into the MAX, the usual banner and prompt appear: For example:

```
** Ascend Pipeline Terminal Server **
Login:
```

When the user enters a name, the screen prompts for a password, just as for a "normal" login without:

```
Password:
```

At this point, the user must enter his or her PIN, followed by the numbers currently being displayed on the SecurID token card.

Note: Unlike the SecurID ACE support in RADIUS, which ignores the input to "Password:" and asks for a "Passcode," this direct implementation does not take the extra step. The Ascend unit sends the input to the Password prompt to the ACE server as the passcode. If you want the Ascend unit to ask for a passcode, you can change the password prompt using the Password Prompt parameter in the TServ Options submenu of the Ethernet Profile.

If the login is correct, the terminal server prompt appears:

```
ascend%
```

If the login is incorrect, this message appears:

```
** Bad Password
```

The Ascend unit requests another login. This process repeats three times, or until the user enters a valid login name/password (or passcode) combination.

NextCode Mode

If a particular user has three or more consecutive incorrect logins, the server marks that user's token card as being in "NextCode" mode. When the user finally logs in successfully, he or she must enter in an extra passcode from his or her token to verify actual possession of the token card. When the user has sent his or her first correct PIN + passcode to the Ascend unit, this message appears:

```
Wait for the code on your token to change, then enter the new
code (without PIN).
Passcode:
```

The user must then wait until the number displayed on the token card changes, and then type in that number without the PIN. If the user enters a correct code, the terminal server command prompt or menu appears. If the user enters an incorrect code, the Ascend unit displays a "**Bad Password" message and the user's token remains in "NextCode" mode.

New PIN Mode

The ACE server system administrator can place particular tokens in "New PIN" mode. The next time the user successfully authenticates and wants access to the system, he or she must choose a new PIN or allows the server to generate one.

After the normal authentication, the Ascend unit displays one of the following three messages.

1 If the server was configured to allow the user to choose a new PIN or request one from the server, this 5-line message displays:

```
Enter your new PIN, containing 4 to 8 digits:
                  or
<Return> to generate a new PIN and display it on the screen:
                  or
<Ctrl C> to cancel the New PIN procedure:
```

Note: The number of allowed digits may change according to the server configuration; the server can also be configured to allow alphabetic characters in the PIN, in which case the word "characters" appears in place of "digits" in the first message.

2 If the server was configured to force the user to choose his or her own PIN, this message displays:

```
Enter your new PIN, containing 4 to 8 digits:
```

3 If the server was configured to restrict the user from choosing a PIN, and to always generate a random PIN for the user, this message displays:

```
Press <Return> to generate a new PIN and display it on the
screen:
```

User-chosen PIN

In cases 1 and 2, when the user enters a new PIN, the server checks the PIN. If the new PIN has the appropriate number of characters or digits, the Ascend unit asks the user to retype the same PIN for verification:

```
Please re-enter new PIN:
```

The user types in the new PIN. If the PINs match, the new PIN is sent to the server, and the user is informed that the PIN has changed:

```
Wait for the code on your token to change, then log in with the
new PIN
Login:
```

If, after the second verifying PIN entry, the Ascend unit sees that the user entered two different PINs, this message appears:

```
PINs do not match. Please try again.
Login:
```

The user must log in again. The server then asks the user to choose a new PIN.

Server-chosen PIN

In cases 1 and 3, when the server generates a PIN for the user, the user simply presses Enter in response to the initial "New PIN" prompt. The server then displays this question:

```
ARE YOU PREPARED TO HAVE THE SYSTEM GENERATE A PIN? (y or n)
[n]:
```

If the user presses "y" or "Y", the screen displays a new PIN chosen by the ACE server:

```
Your new PIN: 6467
Press Enter to clear screen:
```

The user must immediately memorize the PIN, and then press Enter. The screen clears, the PIN is sent back to the Ascend unit for confirmation, and if the ACE server accepts the PIN, the Ascend unit displays this message:

```
Wait for the code on your token to change, then log in with the
new PIN
Login:
```

Note: Changing your PIN counts as one of the three allowed logins per dialup, so a correct PIN change followed by a login counts as two attempts. Therefore, if you fail twice, you need to redial and connect in order to complete authentication.

Configuring direct SecurID ACE authentication

This section describes how to configure a SecurID ACE server as your MAX's external authentication server. When you configure the ACE server as an external authentication server, any calls that are not authenticated by local Connection profiles are forwarded to the ACE server for authentication. If you requires your MAX to reach more than one authentication server, see the *MAX RADIUS Configuration Guide* . Other software products, such as Ascend's Access Control, support multiple external authentication servers through the MAX. Although SecurID ACE authentication is indirectly supported via RADIUS, direct support for the SecurID ACE server can be useful for two main reasons:

1. For those installations where other RADIUS features are not required, direct SecurID ACE support on the Ascend unit decreases the complexity of the system, making the system easier to configure and maintain.
2. The SecurID ACE support via RADIUS does not support the "New PIN Mode" feature, which allows a dial-in user to change the personal identifying number (PIN).

You can specify one of the MAX unit's local profiles to be used for session parameters with ACE authentication, and configure different profiles/addresses for each user based upon whether the user has dialed in with a modem (analog call) or ISDN (digital call). You can also

specify a Lan Address setting that overrides the Lan Address in the specified profile (or in the default profile, if no specific profile is given). This means that you can specify two different remote settings for a user with a single token card. See "Configuring user shell settings on the ACE server" on page 5-20.

Note: The MAX does not support ACE authentication for PPP dial-in users.

To configure the MAX for direct authentication using a SecurID ACE server, follow these steps:

1 Open the Ethernet> Mod Config>Auth menu:

```
X0-X00 Mod Config
 Auth
 >Auth=SECURID
  Auth Host #1=137.175.80.24
  Auth Host #2=0.0.0.0
  Auth Host #3=0.0.0.0
  Auth Port=2626
  Auth Timeout=10
  Auth Key=N/A
  Auth Pool=No
  APP Server=No
  APP Host=N/A
  APP Port=
  SecurID DES encryption=N/A
  SecurID host retries=N/A
  SecurID NodeSecret=N/A
```

2 Set Auth to SECURID.

Auth Host #2 and Auth Host #3 are not applicable, because the Ascend unit can support only one SecurID ACE authentication server at this time.

3 For the Auth Port parameter, enter the UDP port number used by the SecuridID ACE server.

For example, you might specify this setting:

```
Auth Port=1545
```

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

If the MAX does not receive a response within the time specified by Auth Timeout, it assumes the SecurID ACE server has become nonfunctional.

5 To specify whether the server uses standard DES or the native encryption provided by SecurID, choose one of the following values for the SecurID DES encryption parameter:

- Yes specifies that the server uses standard DES encryption.
- No specifies that the server uses the native encryption provided by SecurID.

6 To specify the number of times the Ascend unit attempts to contact the SecurID host before timing out, enter an integer in the SecurID Host Retries parameter.

```
The default value is 3.
```

7 Set the SecurID Node Secret parameter.

For details on this parameter, see the *MAX 200Plus Reference Guide*.

8 Save your changes.

Configuring user shell settings on the ACE server

You can configure a shell setting for each user on the ACE server to store several parameters about the user, including the name of a MAX local profile which should be used when setting up the call for that user, as well as the address and netmask to be used in place of the Lan Address in the given profile.

Shell string structure

The shell string returned by ACE is limited to 64 characters, so brevity is very important. The names of parameters are extremely short. The basic structure of the string is:

```
<parameters> |<CallType> <parameters> |<CallType> <parameters> ...
```

Table 5-6. SecurID-ACE shell string structure

Parameter	Possible Values	Description
<CallType>	A	Following information is only for analog (modem) calls). See the RADIUS NAS-Port attribute for an explanation of which calls are classified as analog and which are classified as digital.
	D	Following information is only for digital (ISDN) calls. See the RADIUS NAS-Port attribute for an explanation of which calls are classified as analog and which are classified as digital.
	" " (space)	Following information is for all types of calls.
		Note: Everything from a <CallType> up to the next "|" (or the end of the string) is put into the caller's profile if and only if the call was of the given type.
<parameters>	one or more of <parameter>	

Table 5-6. SecurID-ACE shell string structure (continued)

Parameter	Possible Values	Description
<parameter>	rp=<string>	Applies only to PAP-TOKEN-CHAP calls, since direct SecurID authentication does not support CACHE-TOKEN. This parameter is put in place of the Receive Password in the Connection Profile, and is used for authentication in subsequent calls. rp is only used to authenticate the second and subsequent calls in an MP bundle, never the first call. The first call must be authenticated by the user with a token value from the SecurID card.
	la=<address>	The IP address of the caller. This parameter functions the same as LAN Adrs in the Connection Profiles. You can use it to specify an address for the remote caller that is different from the address given in the selected (or default) Connection Profile.
	prf=<string>	The name of the Connection Profile stored in the MAX's NVRAM; provides the configuration of the caller. If there is no profile for a call: If Use Answer as Default=Yes (from the Answer profile), the Answer profile is used as the default. If Use Answer as Default=No, the Factory Default Profile is used.
<string>	<stuff> "<stuff>" '<stuff>' [<stuff>]	<stuff>is the value of the parameter.

String syntax conventions

The conventions in the following table apply to all strings.

Table 5-7. Format conventions for strings

Convention	Description
quotes and brackets	Only needed when the value itself has a space in it. Table 5-6 shows the multiple types of quoting in case you need both a space and one of the other quote characters in a string.
| (vertical bar character)	Has a special meaning, and cannot appear in any string.
<address>	An <address> is a string (that is, you can quote or bracket it if you like), but it should take on the form of an IP address, (for example, 1.2.3.4) optionally followed by a netmask (for example, /24).

Examples of String Contents:

For example, the following string

```
|D prf="isdnroute" rp=[greco] la=192.0.2.1/24 |A prf=modemroute
```

specifies:

- if the caller is digital
  - use the profile called isdnroute
  - set the Receive PW to greco
  - set the Lan Addr to 192.0.2.1/24
- if the caller is analog
  - use the profile called modemroute

Shortening a string

The above string is just short enough to fit. If the string was any longer, the end of modemroute would be cut off and authentication would fail for analog calls. The same shell string could be given as:

```
|D prf=isdnroute rp=greco la=192.0.2.1|A prf=modemroute
```

Although this example specifies the same information as the previous example, it has been shortened in the following ways:

- The quotation symbols have been removed. In general, quotes are needed only if there is a space in the character string.
- The space has been removed from before the **`|A`** (the | character indicates the end of a string, just like a space).
- The netmask was not given (/24 is the default netmask for 192.0.2.1, a class C network address).

Setting common parameters for analog and digital calls

It is also possible to have common parameters preceding the sections specific to just analog or digital. For example:

```
prf=john |D la=135.2.2.4/24 |A la=135.2.3.20
```

In this example, the settings would always be taken from the profile john, but the address would be set differently depending on whether the call was analog or digital.

The section with common parameters can be placed after the specific sections as well as before. For example, the following string:

```
|A prf=modemroute |D prf=isdnroute | la=10.0.0.20/32
```

says to use modemroute as the profile template for analog calls, isdnroute for digital calls, and in both cases to use the address 10.0.0.20/32 as the LAN Address.

Separate sections are not required. For example:

```
prf=john la=10.0.0.20/32
```

would use the profile named john and set the Lan Address to 10.0.0.20/32 whether the call was analog or digital.

Or you can have just one or the other:

```
|D prf=isdnroute rp= "go for it"
```

In this case, an analog caller would be given the default or answer profile depending on the setting of the Use Answer as Default parameter in the answer profile.

String errors

If there is an error or unrecognized string in the shell string for a user, the authentication will fail. If you have trouble seeing what caused the failure, enter the MAX's debug mode and turn on a diagnostic display of the string interpretation using the command **`securiddebug`**. This is a toggle that turns the display on and off.

String too long

Check to see that you have not exceeded the 64 character limit (the ACE server's sdadmin program does not check for this limit). This is indicated when the final parameter is not complete. For security reasons, the password string is not displayed by this debug mode.

For security reasons, the password string is not displayed by this debug mode, so you will not be able to tell directly from the debug output whether the rp parameter is being truncated. If you encounter problems with the 2nd and subsequent channels of an MP call automatically authenticating, the problem could be that the end of the rp parameter is being cut off.

Setting overwritten

Each new parameter is copied over the current state of the caller's profile at each step. It is therefore possible to overwrite one setting with another. For example:

```
rp=joebob prf=john
```

will cause the Receive Password joebob to be overwritten by the Receive Password in the profile john. Be careful always to list prf's before rp's or la's.

Configuring PAP-TOKEN-CHAP using direct ACE authentication

PAP-TOKEN-CHAP stores a static password in the user's shell setting on the ACE server and sends it back to the MAX when the user first connects. Except for this, PAP-TOKEN-CHAP configuration on the calling router is identical to configuring PAP-TOKEN-CHAP for any other type of token card authentication.

To set the static password to use during PAP-TOKEN-CHAP for a particular user:

1. Run the sdadmin program on the ACE server machine.
2. From the Client menu, select Edit.
3. Pick the MAX from the list of clients and click OK.
4. Click User Activations.
5. From the Directly Activated Users list, select the user that will be using PAP-TOKEN-CHAP, then click Edit Activation Data.
6. In the Activation Data window, delete any existing text in the Shell field, and replace it with:

   rp="*password*"

   where *password* is the password to be configured as the Aux Send PW on the calling router (usually a Pipeline). This is done in Step 8.

   For example, if you type

   rp="Little Big"

   in the Shell field (with quotation marks), the password the user types is

   Little Big (without quotation marks).

   In this example, the quotes are delimiters for the password. Different delimiters are allowed is so that the user can choose a password containing those delimiters, for example:

   rp='Quote"quote'

   which contains a double quote in the middle of the password.

   You can use any character you like for the delimiters in place of the double quotes except the vertical bar ("|"), which has a special meaning in the shell field. For example, the following entry would produce the same Receive Password setting as `rp="Little Big":`

   rp=/Little Big/

   However, `rp=[Little Big]` is not identical and would an produce error, since the left bracket and right bracket are different characters.
7. Press OK to clear the Activation Data dialog, and Exit to clear the Edit Client dialog
8. Configure the calling router (usually a Pipeline) to use PAP-TOKEN-CHAP authentication, and set Aux Send PW in the Connection profile Encaps options to be identical to the string you entered in the ACE server as rp (Receive Password) in Step 6.

Assuming all other configuration was already done (configuring the answering MAX to use SecurID authentication, and configuring the calling router to use the App Server, for example), you should now be able to bring up a multi-channel call, while only performing a single token authentication.

Configuring direct Defender server authentication

This section describes how to configure the Defender as your MAX's external authentication server. When you configure the Defender as an external authentication server, any calls that are not authenticated by local Connection profiles are forwarded to the Defender server for authentication. If you requires your MAX to reach more than one authentication server, see the *MAX RADIUS Configuration Guide* . Other software products, such as Ascend's Access Control, support multiple external authentication servers through the MAX.

Note: The Defender server does not provide per-user control, such as enforcing a maximum number of channels. It provides only per-user authentication. If you need both per-user control and authentication, you need RADIUS.

To configure a Defender server for direct authentication, follow these steps:

1 Open the Ethernet > Mod Config > Auth menu:

```
X0-X00 Mod Config
 Auth
 >Auth=Defender
  Auth Host #1=137.175.80.24
  Auth Host #2=0.0.0.0
  Auth Host #3=0.0.0.0
  Auth Port=2626
  Auth Timeout=10
  Auth Key=****************
  Auth Pool=No
  APP Server=No
  APP Host=N/A
  APP Port=N/A
  SecurID DES encryption=N/A
  SecurID host retries=N/A
  SecurID NodeSecret=N/A
```

2 Set Auth to Defender.

Auth Host #2 and Auth Host #3 are not applicable, because the Ascend unit can support only one Defender authentication server at this time.

3 Set the value of Auth Port to the TCP port number of the Defender authentication server, usually 2626.

4 Set the value of Auth Key.

Auth Key is used as a DES secret key shared between the Ascend unit and the Defender authentication server. This key is also used for authentication by the Ascend unit in its role as a Defender authentication agent.

5 Set Auth Timeout to indicate the number of seconds the Ascend unit waits before assuming that the Defender server has become nonfunctional.

6 Enter the port number for the source port for remote authentication requests.

Type a port number between 0 and 65535. The default value is 0 (zero); if you accept this value, the Ascend unit can use any port number between 1024 and 2000.

You can specify the same port for authentication and accounting requests.

7. Normally APP Server = No. APP Server only applies when the MAX makes outgoing calls to MAX units and other sites using token card authentication. See the *MAX 200Plus Reference Guide* for more information.
8. If the MAX must make outgoing calls to other MAX units and to other sites using token-card authentication, you may need to set APP Server=Yes. Normally this parameter is set to APP Server=No. For more details see the *MAX 200Plus Reference Guide*.
9. Save your changes.

Setting Up User Authorization

6

User authorization enables you to tighten network security. You can control access on a per-user basis, and authorize access to selected enterprise resources and services. This chapter describes how to carry out the following user authorization tasks:

Setting up terminal server security

A terminal server connection is typically an incoming call that uses V.34, V.42, V.110 or V.120 encapsulation. The call can also consist of an asynchronous data stream, such as when a user dials in from an analog modem or a serial connection to the MAX. This section also applies to locally connected terminal server users, and describes how to limit access to the terminal server features such as Telnet server, raw-TCP, Rlogin server, and modem dialout. See "Setting up remote terminal server authentication" on page 3-14 for more information about the authentication required before a remote user can get access to any of these features.

When the MAX receives a call that uses 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. If no PPP encapsulation is present, the MAX establishes a terminal server connection.

In Figure 6-1, a PC running SoftComm initiates an incoming modem call. The MAX directs the call to its digital modems, and then forwards the call to its terminal server software. In Figure 6-1, the MAX immediately directs the call to a Telnet host.

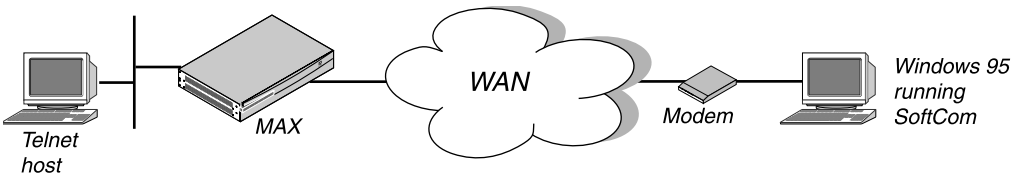

Figure 6-1. A terminal server connection

You can customize and limit access to the terminal server interface in these ways:

- Turn terminal server operation on or off.
- Specify customized prompts for remote terminal server users.
- Restrict use of terminal server commands and protocols.
- Restrict access to the terminal server command line.
- Restrict Telnet, raw TCP, and Rlogin access to the terminal server.

Table 6-1 lists the parameters you can use to customize and restrict access to the terminal server environment.

Table 6-1. Terminal server security parameters

Location	Parameters with sample values
Ethernet > Mod Config > TServ Options	TS Enabled=Yes Passwd=*SECURE* Login Prompt= Passwd Prompt= 3rd Prompt= Initial Scrn=Cmd Toggle Scrn=No Security=None Telnet=Yes Rlogin=No PPP=No SLIP=No Host #*n* Addr=0.0.0.0 Host #*n* Text= Immed Host=0.0.0.0 Immed Port=0 Immed Service=Telnet Imm. Modem Pwd=*password* Imm Modem Auth=Ye

For complete information on setting up terminal server connections in the MAX configuration interface, see the *MAX ISP & Telecommuting Configuration Guide*. For complete information on setting up terminal server connections in RADIUS, see the *MAX RADIUS Configuration Guide.*

Turning terminal server operation on or off

To specify whether users can access the terminal server interface, follow these steps:

1 Open the Ethernet > Mod Config > TServ Options menu.

2 To enable terminal server access, set TS Enabled=Yes; to disable terminal server access, set TS Enabled=No.

3 Save your changes.

Table 6-2. Characters used in the terminal server prompt specification

Character combination	Description
\n	carriage return/line feed
\t	tab
\\	displays "\\" on the screen

Note: Any characters other than **\n** and **\t** that have a single backslash (\) in front of them are removed.

For example, you could enter

Welcome to\n\t\\Ascend Remote Server\\\nEnter your user name:

to display the following on the terminal server screen:

```
Welcome to
       \\Ascend Remote Server\\
Enter your user name:
```

4 Set Prompt Format=Yes.

This is the field that determines whether you are able to use the multi-line format for the terminal server prompt. If Prompt Format=No, the MAX does not interpret the line feed/carriage return character or the tab character.

5 Set the Login Timeout parameter.

This value can be an integer between 0 and 300 seconds. The default value is 300 seconds.

Users are disconnected if they have not completed logging in when the number of seconds set in the Login Timeout field has elapsed. A user has the total number of seconds indicated in the Login Timeout field to attempt a successful login. This means that the timer begins when the login prompt appears on the terminal server screen, and continues (is not reset) when the user makes unsuccessful login attempts.

6 To customize the password prompt, set the Passwd Prompt parameter.

This parameter specifies the prompt the terminal server displays when asking the user for his or her password. You can specify up to 80 characters. The default value is "Password:".

7 To specify a third prompt to follow the login and password prompts, specify a prompt string in the 3rd Prompt parameter.

You can specify up to 20 characters. The default value is null. If you accept the default, the MAX does not display an additional prompt.

The remote terminal server user can enter up to 80 characters after this prompt. The MAX passes the information the user enters to the RADIUS server as an attribute called Ascend-Third-Prompt; this attribute appears in the Access-Request packet. If the user enters more than 80 characters, RADIUS truncates the data before assigning a value to the Ascend-Third-Prompt attribute.

The 3rd Prompt parameter does not apply if the Auth parameter has a value other than RADIUS or RADIUS/LOGOUT. If authentication occurs through a local Connection profile, and not through the RADIUS server, the MAX ignores the 3rd Prompt specification.

8 Select First or Last for the 3rd Prompt Seq parameter to select whether the additional prompt appears at the beginning or the end of the login sequence.

3rd Prompt Seq works with any authentication method except Auth=None.

The default is Last. 3rd Prompt Seq is N/A if TS Enabled=No or 3rd Prompt= is empty.

The third prompt feature works slightly differently depending upon whether you specify that it appear in the Last position (a prompt issued after the login and password prompts) or the First position (a prompt issued before login and password prompts). For more complete information on how the third prompt feature works, see “Understanding how the third login prompt works” on page 6-5.

9 Save your changes.

Sample prompts

Suppose you accept the default settings for the Login Prompt and Passwd Prompt parameters, and specify this setting for 3rd Prompt:

```
3rd Prompt=Password2>>
```

The terminal server displays these prompts:

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

Understanding how the third login prompt works

You can configure a prompt by specifying the string that appears with the prompt and where it appears in the login sequence (first or last). This prompt can emulate an existing terminal server login prompt sequence, depending upon what you specify in the prompt string.

The third prompt feature works differently depending upon whether you select First or Last for the 3rd Prompt Seq parameter.

Similarities in the way the 3rd prompt works in either First or Last position are:

- Both work with any value for the Auth parameter except Auth=None.
- User's input is passed to RADIUS with the authentication request as the value of the “Ascend-Third-Prompt” RADIUS attribute.

Differences in the way the 3rd prompt works, depending upon whether 3rd Prompt Seq=First or Last, are:

- The First prompt appears before Login & Password prompts, the Last prompt appears after Login & Password prompt
- User's input is echoed in response to a First prompt and is not echoed in response to a Last prompt.

Restricting the use of terminal server commands and protocols

To specify whether users can initiate Telnet, Rlogin, PPP, or SLIP sessions from the terminal server interface, follow these steps:

1 Open the Ethernet > Mod Config > TServ Options menu.

2 To specify whether a user can start a Telnet session, set the Telnet parameter.

– Yes indicates that a user can begin a Telnet session.

The default value is Yes.

– No indicates that a user cannot begin a Telnet session.

3 To specify whether a user can initiate an Rlogin session, set the Rlogin parameter.

– Yes indicates that a user can begin an Rlogin session.

– No indicates that a user cannot begin an Rlogin session.

The default value is No.

4 To specify whether a client can use asynchronous PPP, set the PPP parameter.

– Yes indicates that a client can use asynchronous PPP.

– No indicates that a client cannot use asynchronous PPP.

The default value is No.

5 To specify whether a user can initiate a SLIP (Serial Line IP) session, set the SLIP parameter. SLIP is a protocol that enables your computer to send and receive IP packets over a serial link.

– Yes indicates that a user can begin a SLIP session.

– No indicates that a user cannot begin a SLIP session.

The default value is No.

6 Save your changes.

Restricting access to the Immediate Modem feature

The Immediate Modem feature allows local terminal server users (who have not dialed into the MAX and have therefore not been authenticated) to Telnet to a MAX to access the MAX unit's modems, so that they can place outgoing calls without going through MAX terminal server interface. You can choose to restrict access to the Immediate Modem feature on a per-user basis, or you can specify a global password for all users. You can also disable call restriction for the Immediate Modem feature, so that all users can place outgoing calls.

To use immediate modem service, users specify the port number configured in the Imm. Modem Port parameter when opening a Telnet session to the MAX. For example, a user can access a digital modem on port 5000 in a MAX unit named "max1" by typing this command:

```
telnet> open max1 5000
```

When the modem responds, the user can begin entering AT commands to dial out.

Understanding per-user Immediate Modem access restriction

The following applies to local terminal server users who have not dialed into the MAX and therefore have not been authenticated. When per-user Immediate Modem is enabled, the MAX does the following:

1 Requests a login name before allowing any user access to the Immediate Modem feature.

2 The MAX attempts to find a profile with the name provided by the user, looking first for a local Connection profile, then for a simple Name/Password profile, and finally for a RADIUS profile.

– If the MAX finds a matching profile, it prompts the user for the password (if any) associated with the profile and verifies that the user enters the correct password.

- If no profile matching the name provided by the user can be found, the MAX rejects the user and closes the Telnet session.

3 If the user enters the correct password, the MAX then checks the Dialout-OK parameter of the appropriate profile.

- If Dialout OK is set to Yes, the user can access the immediate modem feature.
- If the user gets the password wrong or the Dialout OK parameter is set to No, the MAX rejects the user (with an appropriate message) and closes the telnet session.

Understanding password restriction for Immediate Modem

The immediate modem password separately governs whether a user is allowed to use the immediate modem functionality. If Telnet is password-protected, a user must know the Telnet password as well as the immediate modem password in order to dial out. To use Telnet but not the dialout functionality, a user only needs to know the Telnet password.

Configuring access to the Immediate Modem feature

To restrict access to the Immediate Modem feature, follow these steps:

1 Open the Ethernet > Mod Config > TServ Options menu.

2 Set TS Enabled=Yes.

The Imm. Modem Pwd field is N/A if TS Enabled=No. You cannot specify a password for the Immediate Modem feature.

3 Set the Modem Dialout parameter to specify whether the user can use this MAX unit's V.34 digital modems to dial out.

Modem Dialout=Yes permits terminal server users access the digital modems.

Modem Dialout=No denies terminal server users access to the digital modems. The default value is No.

4 Set the Immediate Modem parameter to enable or disable the Immediate Modem feature.

Immediate Modem=Yes enables the Immediate Modem feature.

Immediate Modem=No disables the Immediate modem feature. The default value is Yes.

5 Set the Imm. Modem Access parameter to specify whether the access is restricted on a global or per-user basis, or unrestricted.

- None indicates that call restriction is disabled, and that all users can place outgoing calls.
- Global indicates that a single password exists for dialout (set in the Imm. Modem Pwd parameter). Any user who knows this password can place outgoing calls.
- User (the default) indicates the MAX requires a login before any user can access the Immediate Modem's dialout feature. The MAX attempts to match the user's name and password to a name and receive password in a Connection profile, Name/Password profile, or RADIUS users profile. If the user is authenticated by matching a Password profile, the Password profile must point to a Connection profile for the setting of the Dialout OK parameter.

6 Specify a password in the Imm. Modem Pwd. parameter if you set Imm. Modem Access=Global,

This parameter is N/A if Imm. Modem Access=None or User.

Note: To allow unlimited access to the Immediate Modem feature, set Imm. Modem Access=None. Do not set Imm. Modem Access=Global and then leave the Imm. Modem Pwd parameter null in order to allow unlimited access to the Immediate Modem feature.

7 Close the Ethernet > Mod Config > TServ Options menu.

8 Open the Telco options submenu of the appropriate Connection profile.

9 Set the Dialout OK parameter to indicate whether modem dialout is allowed for this Connection profile.

- Dialout OK=Yes indicates that the Connection profile allows modem dialout.
- Dialout OK=No indicates that the Connection profile does not allow modem dialout. Dialout OK=No is the default.

Disconnecting a user's terminal server session

You can disconnect a user who establishes a Telnet connection with the Ascend unit. You can disconnect the user by session ID. The disconnect code that results is identical to the RADIUS disconnect code, allowing you to track all administrative disconnects.

Displaying a list of active terminal server sessions

To display a list of active user session on an Ascend MAX, type:

```
show users
```

Note: at the terminal server prompt. `show users` displays a list of user sessions active on a system. Each user session is identified by the sessionID, with additional information about the session. The show users command has also been added to the online help for the show command.

Killing an active terminal server session

To terminate a Telnet session, enter this command line at the terminal server prompt:

```
kill <session ID>
```

For the <session ID> argument, specify the session ID as displayed by the terminal server "show users" command. The disconnect reason for the session is reported as DIS_LOCAL_ADMIN.

The active Security Profile must have Edit All Calls=Yes. If Edit All Calls=No, this message displays when you issue the kill command:

```
Insufficient security level for that operation.
```

If you issue the kill command without the <session ID> argument, this message displays:

```
kill command requires an argument
```

When the session is properly terminated, a message like this one displays:

```
Session 216747095 killed.
```

When the session is not terminated, a caution like this one displays:

Unable to kill session 216747095.

Setting up SNMP security

SNMP (Simple Network Management Protocol) provides a way for computers to share networking information. In SNMP, two types of communicating devices exist: agents and managers. An agent (such as the MAX) provides networking information to a manager application running on another computer. The agents and managers share a database of information, called the Management Information Base (MIB).

A trap is a mechanism in SNMP for reporting system change in real time. To report system change, the MAX sends a traps-PDU across the Ethernet interface to the SNMP manager. A complete list specifying the events that cause the MAX to send a traps-PDU appears in the Ascend Enterprise Traps MIB.

You can set up SNMP security in these ways:

- Specify passwords for SNMP managers with access to the MAX.
- Set up SNMP traps.
- Restrict the hosts that can issue SNMP commands.

Table 6-3 shows the SNMP security parameters on the MAX.

Table 6-3. SNMP security parameters

Location	Parameters with sample values
Ethernet > Mod Config > SNMP Options	Read Comm=new-string R/W Comm=unique-string Security=Yes RD Mgr1=10.21.4.5 RD Mgr2=10.21.4.7 RD Mgr3=10.21.4.55 RD Mgr4=10.21.4.103 RD Mgr5=10.21.4.64 WR Mgr1=10.21.4.11 WR Mgr2=0.0.0.0 WR Mgr3=0.0.0.0 WR Mgr4=0.0.0.0 WR Mgr5=0.0.0.0
Ethernet > SNMP Traps > Any SNMP Traps profile	Name= Alarm=Yes Port=No Security=No Comm= Dest=0.0.0.0

Password-protecting SNMP

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, you must assign the Read and Read/Write SNMP community strings. Follow these steps:

1. Open the Ethernet > Mod Config > SNMP Options menu.
2. Set the Read Comm parameter.

   This parameter specifies the Read community string. This string authenticates an SNMP manager accessing the MAX to perform read commands—that is, the Get and Get Next commands. The Get command requests information. The Get Next command enables an SNMP manager to obtain a table of information, such as a routing table. After you enter a string for the Read Comm parameter, users must supply it to use the Get and Get Next commands.
3. Set the R/W Comm parameter.

   This parameter specifies the Read/Write community string. This string authenticates an SNMP manager accessing the MAX to perform read and write commands—that is, the Get, Get Next, and Set commands. The Set command enables an SNMP manager to change information maintained by the MAX. After you enter a string for the R/W Comm parameter, users must supply it to use the Get, Get Next, and Set commands.

   Note: You cannot turn SNMP write off, so you must set a secret R/W Comm string. The default R/W Comm string is “write”. Anyone who has used an Ascend product probably knows this default string.
4. Save your changes.

Setting up SNMP traps

To configure parameters related to SNMP traps security, follow these steps:

1. Open the Ethernet > SNMP Traps menu.
2. Open a blank SNMP Traps profile.
3. For the Name parameter, specify the SNMP manager to which the MAX sends traps-PDUs.

   You can specify up to 31 characters. The default value is null. The value you specify becomes the name of the profile.
4. Set the Alarm parameter.

   This parameter specifies whether the MAX sends a traps-PDU to the SNMP manager when an alarm event occurs. Alarm events are defined in RFC 1215 and include the following:

   – coldStart

     This event indicates that the MAX started up from a power-off condition.

   – warmStart

     This event indicates that the MAX started up from a power-on condition, typically by a system reset.

   – linkDown

     This event indicates that a WAN link or Ethernet interface has gone offline.

   – linkUp

     This event indicates that a WAN link or Ethernet interface has come online.

You can specify either Yes or No for the Alarm parameter. Yes specifies that the MAX traps alarm events. No specifies that the MAX does not trap alarm events. The default value is Yes.

5 Set the Port parameter.

This parameter specifies whether the MAX traps serial host port state changes and sends traps-PDUs to the SNMP manager. The MAX can record these serial host port events:

- portInactive
- portDualDelay
- portWaitSerial
- portHaveSerial
- portRinging
- portCollectDigits
- portWaiting
- portConnected
- portCarrier
- portLoopback
- portAcrPending
- portDteNotReady

You can specify either Yes or No for the Port parameter. Yes specifies that the MAX traps serial host port state changes. No specifies that the MAX ignores serial host port state changes. The default value is No.

6 Set the Security parameter.

This parameter specifies whether the MAX traps these events:

- authenticationFailure

  This event occurs when authentication has failed. See RFC-1215 for a full explanation of this event.

- consoleStateChange

  This event occurs when a VT100, Palmtop, or Telnet port changes its state.

- portUseExceeded

  This event occurs when the port exceeds the maximum number of DS0 minutes set by the Max DS0 Mins parameter in the Port profile.

- systemUseExceeded

  This event occurs when the MAX exceeds the maximum number of DS0 minutes set by the Max DS0 Mins parameter in the System profile.

You can specify either Yes or No for the Security parameter. Yes specifies that the MAX traps the events. No specifies that the MAX does not trap the events. The default value is No.

7 Using the Comm parameter, specify a community name.

The string you specify becomes a password that the MAX sends to the SNMP manager when an SNMP trap event occurs. The password authenticates the sender identified by the IP address in the IP Adrs parameter.

For the community name, you can enter an alphanumeric string containing up to 31 characters. The default value is null. To turn off SNMP traps, leave the Comm parameter blank and set Dest=0.0.0.0.

8 Using the Dest parameter, specify the IP address of the SNMP manager to which the MAX sends traps-PDUs.

Specify an IP address in dotted decimal notation. An IP address consists of four numbers between 0 and 255, separated by periods. If a netmask is in use, you must specify it. Separate a netmask from the IP address with a slash. The default value is 0.0.0.0/0.

The MAX ignores any digits in the IP address hidden by a netmask. For example, the address 200.207.23.1/24 becomes 200.207.23.0. To specify a route to a specific host, use a mask of 32.

The Dest parameter does not apply if the MAX does not support IP (Route IP=No).

9 Save your changes.

Restricting the hosts that can issue SNMP commands

The MAX is an SNMP-enabled device that supports a variety of MIBs. Especially on a large network, you may want to specify which stations can use SNMP manager applications to initiate read or read/write access to those MIBs.

You can list up to five IP hosts that can read traps and other information from the Ascend unit, and five hosts that can access MIB read-write access. The MAX checks the version and community strings before making source IP address comparisons.

To restrict the hosts that can issue SNMP commands, follow these steps:

1 Open the Ethernet > Mod Config > SNMP Options menu.

2 Make sure that the Security parameter is set to Yes.

This parameter specifies that the MAX must compare the source IP address of packets containing SNMP commands against a list of qualified IP addresses.

3 Specify the IP addresses of hosts that have SNMP read permission.

For example, you might make these settings:

```
RD Mgr1=10.1.2.3
RD Mgr2=10.1.2.4
RD Mgr3=10.1.2.5
RD Mgr4=10.1.2.6
RD Mgr5=10.1.2.7
```

If the Security parameter is set to Yes, only SNMP managers at the specified IP addresses can execute the SNMP Get and Get Next commands.

4 Specify the IP addresses of hosts that have SNMP write permission.

For example, you might make these settings:

```
WR Mgr1=10.9.8.1
WR Mgr2=10.9.8.2
WR Mgr3=10.9.8.3
WR Mgr4=10.9.8.4
WR Mgr5=10.9.8.5
```

If the Security parameter is set to Yes, only SNMP managers at the specified IP addresses can execute the SNMP Get, Get Next, and Set commands.

5 Save your changes.

Setting up DNS (Domain Name System)

DNS is a TCP/IP service that enables you to specify a symbolic name instead of an IP address. A symbolic name consists of a username and a domain name using the format *username@domain name*. The username corresponds to the host number in the IP address; the domain name corresponds to the network number in the IP address. A symbolic name might be steve@abc.com or joanne@xyz.edu.

DNS maintains a database of network numbers and corresponding domain names on a domain name server. When you use a symbolic name, DNS translates the domain name into an IP address, and sends it over the network. When the Internet service provider receives the message, it uses its own database to look up the username corresponding to the host number.

You can set up two types of DNS configurations:

- Local DNS

  When you set up local DNS, you specify the DNS server(s) known to users on connected local interfaces.

- Client DNS

  A client DNS configuration defines DNS server addresses that the MAX presents to WAN connections during IPCP negotiation. This type of configuration provides a way to protect your local DNS information from WAN users.

  Client DNS has two levels: a global configuration that applies to all PPP connections, and a connection-specific configuration that applies to each individual connection. You set up the global configuration in the Ethernet profile, and the connection-specific configuration in the Connection profile. The MAX uses the global addresses only if a user's Connection profile does not specify any.

  You can also specify that WAN connections use a local DNS server if no client DNS servers are available.

Table 6-4 lists the parameters you can set.

Table 6-4. DNS parameters

Location	Parameters with sample values
Ethernet > Mod Config > DNS	Domain Name=abc.com Pri DNS=10.2.3.56/24 Sec DNS=10.2.3.107/24 List Attempt=No List Size=6 Client Pri DNS=101.10.10.1 Client Sec DNS=101.10.10.2 Allow as Client DNS=Yes Sec Domain Name=xyz.com
Ethernet > Connections > Any Connection profile > IP Options	Client Pri DNS Client Sec DNS

Setting global DNS parameters

To set global DNS parameters, follow these steps:

1 Open the Ethernet > Mod Config > DNS menu.

2 To specify a primary domain name to use for lookups, set the Domain Name parameter.

This parameter specifies the local domain name. When the MAX needs to look up a hostname, it tries various combinations, including appending the configured domain name.

3 To specify a secondary domain name to use for lookups, set the Sec Domain Name parameter.

This parameter specifies the domain name to use if the lookups using the Domain Name specification fail.

4 Using the Pri DNS parameter, specify the IP address of the primary domain name server for use on connected local interfaces.

The address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0. Accept this default if you do not have a domain name server.

5 Using the Sec DNS parameter, specify the IP address of the secondary domain name server for use on connected local interfaces.

The address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0. Accept this default if you do not have a secondary domain name server.

The MAX uses the secondary server only if the primary one is inaccessible. The Sec DNS parameter applies only to Telnet and raw TCP connections running under the MAX unit's terminal server interface.

6 Set List Attempt=Yes.

DNS can return multiple addresses for a hostname in response to a DNS query, but it does not include information about availability of those hosts. Users typically attempt to access the first address in the list. If that host is unavailable, the user must try the next host, and so forth. However, if the access attempt occurs automatically as part of immediate services, the physical connection is torn down when the initial connection fails.

The DNS List Attempt feature helps the MAX avoid tearing down physical links by enabling the user to try one entry in the DNS list of hosts when logging in through Telnet from the terminal server or immediate Telnet; if that connection fails, the user can try each succeeding entry.

You can specify one of these settings:

- Yes specifies that the MAX enables a user to try the next host in the DNS list if the first Telnet login attempt fails.
- No turns off the List Attempt feature. The default value is No.

7 If you set List Attempt=Yes, set the List Size parameter.

The List Size parameter specifies the maximum number of hosts the MAX can list in response to a DNS query. You can specify a number between 0 and 35. The default value is 6. Users logging in via Telnet or immediate Telnet see a list containing up to the specified number of hosts available for access.

8 Set the Client Pri DNS parameter.

This parameter enables you to set up client DNS—that is, to specify a primary DNS server address that the MAX sends to any client connecting to the MAX over the WAN. Specify the IP address of a DNS server for all connections that do not have a DNS server defined

in a Connection profile. The default value is 0.0.0.0. Accept this default if you do not have a client DNS server.

9 Set the Client Sec DNS parameter.

This parameter specifies a secondary DNS server address that the MAX sends to any client connecting over the WAN when the server specified by Client Pri DNS is unavailable. The MAX uses this global client address only if the Connection profile does not specify one.

The default value is 0.0.0.0. Accept this default if you do not have a secondary client DNS server.

10 Set the Allow As Client DNS parameter.

This parameter specifies whether the local DNS servers should be accessible to PPP connections across the WAN if the client DNS servers are unavailable. You can specify either Yes or No:

– Yes enables WAN clients to use local DNS servers.

– No disables WAN clients from using local DNS servers. No is the default.

Sample DNS configuration

This sample specifies two local DNS servers and enables the DNS list feature.

1 Open the Ethernet > Mod Config > DNS menu.

2 Specify your domain name.

3 Specify the IP addresses of a primary and secondary DNS server and turn on the DNS list attempt feature.

```
Mod Config
    DNS…
        Domain Name=abc.com
        Pri DNS=10.2.3.56/24
        Sec DNS=10.2.3.107/24
        List Attempt=Yes
```

4 Save your changes.

Setting connection-specific DNS parameters

To set up connection-specific DNS parameters, follow these steps:

1 Open the Ethernet > Connections menu.

2 Open a Connection profile

3 Open the IP Options menu.

4 Set the Client Pri DNS parameter.

This parameter specifies the primary client DNS server address the MAX sends to this client. Specify the IP address of a DNS server. The default value is 0.0.0.0. Accept this default if you do not want to specify a particular DNS server for this connection.

5 Set the Client Sec DNS parameter.

This parameter specifies a secondary client DNS server address that the MAX sends to the client on this connection if the primary server is unavailable. The default value is 0.0.0.0. Accept this default if you do not want to specify a secondary DNS server for this connection.

6 Save your changes.

Disabling remote management access

To prevent an operator from accessing the MAX from a remote Ascend unit using MP+ remote management, use the parameter listed in Table 6-5.

Table 6-5. Remote management parameter

Location	Parameter
System > Sys Config	Remote Mgmt=No

To disable remote management access, follow these steps:

1 Open the System > Sys Config menu.

2 Set Remote Mgmt=No.

3 Save your changes.

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

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. Use the parameter listed in Table 6-6.

Table 6-6. Telnet password parameter

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

To assign a Telnet password, follow these steps:

1 Open the Ethernet > Mod Config menu.

2 Set the Telnet PW parameter.

The Telnet password you supply can contain up to 20 characters. Any user who initiates an incoming Telnet session to the MAX must supply this password before the Telnet session is established.

If a user initiates the Telnet session from the WAN, the connection must first be authenticated as specified in a Connection profile.

See Chapter 3, “Setting Up User Authentication,” for additional information about restricting Telnet in the terminal server interface.

3 Save your changes.

Understanding secure Dynamic Bandwidth Allocation

Dynamic Bandwidth Allocation (DBA) enables the MAX to increase bandwidth as needed and drop bandwidth when it is no longer required. MP+ is the only PPP-based encapsulation method that supports DBA.

When the system adds additional channels, the MAX must authenticate each one. You can secure each circuit using one of the following methods:

- Static passwords

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

  For information on specifying a static password and requiring CHAP authentication in the MAX configuration interface, see "Configuring PAP, CHAP, and MS-CHAP for PPP, MP, and MP+ calls" on page 3-9. For information on configuring static passwords and CHAP in RADIUS, see the *MAX RADIUS Configuration Guide.*

- Dynamic passwords

  Using PAP-TOKEN authentication, the MAX can require a user to specify a one-time-only password, generated by a security-card server, for each additional channel.

  For information on setting up PAP-TOKEN authentication in the MAX configuration interface, see "Requesting PAP-TOKEN authentication" on page 5-7. For information on setting up PAP-TOKEN authentication in RADIUS, see the *MAX RADIUS Configuration Guide*.

- Combination of static and dynamic password

  In the MAX configuration interface, you can indicate that the user need only specify a dynamic password for the initial channel, and that all other channels are authenticated by CHAP. Whenever the MAX adds channels to a PPP or MP+ call using PAP-TOKEN-CHAP authentication, the calling unit sends the encrypted value of Aux Send PW (found in the Connection profile used to dial the call), and the answering unit checks this password against the value of Recv Auth (in a Connection profile) or Ascend-Receive-Secret (in a RADIUS user profile). The answering unit receives the password when the first channel of the call connects.

  For details on setting up PAP-TOKEN-CHAP authentication in the MAX configuration interface, see "Configuring PAP-TOKEN-CHAP using direct ACE authentication" on page 5-24. For information on setting up PAP-TOKEN-CHAP authentication in RADIUS, see the *MAX RADIUS Configuration Guide*.

- Cached passwords

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

  For details on setting up cached passwords in the MAX configuration interface, see "Requesting CACHE-TOKEN authentication" on page 5-7. For information on setting up cached passwords in RADIUS, see the *MAX RADIUS Configuration Guide*.

Index

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X