MAX 6000 Series Security Supplement

Ascend Communications, Inc.
Part Number: 7820-0580-001
For software version 6.0.0

Ascend Customer Service

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

Obtaining Technical Assistance

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

Information you will need

Before contacting Ascend Customer Service, gather the following information:

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

How to contact Ascend Customer Service

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

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

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

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

Ascend Communications
1701 Harbor Bay Parkway
Alameda, CA 94502

Need information about new features and products?

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

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

  `http://www.ascend.com`

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

  `ftp.ascend.com`

Important safety instructions

The following safety instructions apply to the MAX:

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

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

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

4 Ensure proper procedures for static electricity, such as using a grounding mat and a wrist strap.

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

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

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

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

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

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

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

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

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

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

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

16 Do not attempt to service this product yourself, as opening or removing covers may expose you to dangerous high voltage points or other risks. Refer all servicing to qualified service personnel.

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

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

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

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

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.
- Avoid using equipment connected to telephone lines (other than a cordless telephone) during an electrical storm. There is a remote risk of electric shock from lightning.

- Do not use a telephone or other equipment connected to telephone lines to report a gas leak in the vicinity of the leak.

Warning: To reduce the risk of fire, communication cable conductors must be 26 AWG or larger.

Attention: Afin de reduire les risques d'incendie, les fils conducteurs du cable de communication doivent etre d'un calibre minimum de 26 AWG (American Wire Gauge), cest-a-dire d'un minimum de 0,404 mm.

Warnung: Um Feuerrisiken zu reduzieren, müssen die Kommunikationskabel-Anschlüße 26 AWG oder größer sein.

Contents

Figures

Tables

About This Guide

How to use this guide

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: Basic Security Measures,” 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, “Defining Static 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 guide 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 the following publications:

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	You should read Firewalls and Internet Security by William R. Cheswick and Steven M. Bellovin

What you should know

You should read this supplement if you will be setting up security in the MAX. This supplement 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 Configuration Guide*.

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

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

Convention	Meaning
⚠ **Caution:**	Warns that a failure to follow the recommended procedure could result in loss of data or damage to equipment.
⚡ **Warning:**	Warns that a failure to take appropriate safety precautions could result in physical injury.

Manual set

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

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

Getting Started: Basic Security Measures 1

This chapter describes how to set up basic security on the MAX. The chapter contains:

Introducing Security profiles

Security profiles consist of parameters you configure 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
```

All MAX units provide two special profiles:

- Full Access

  Provides full access to the MAX. It is the *super-user* profile that enables you to configure your system, dial remote locations, reset the unit, and upgrade system software.

Whoever knows the password for the Full Access profile can perform any operation on the MAX. The default Full Access password is `Ascend`. To maintain security, you should change the Full Access password from its default value. 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: You should 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 Default and Full Access profiles. However, you can define additional security levels and enable specific 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. You must assign a name to a security profile to activate it, so you can activate only the Default and Full Access profiles initially. The default security settings of the Full Access profile enable you to configure and set up the MAX without any restrictions. Before you make the MAX generally accessible, you should protect the configured unit from unauthorized access. Proceed as follows:

1. Activate the Full Access profile
2. Change the Full Access password.
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.
8. Specify the number of times the MAX retries a connection
9. Retrieving configuration updates from RADIUS.

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, proceed as follows:

1 From any VT100 menu, press <Ctrl> D.

The DO menu appears. For example:

```
DO...
>0=Esc
 P=Password
 C=Close TELNET
```

2 Press P or select P=Password.

A menu appears listing all security profiles:

```
Security profile...?
>00-301 Default
 00-302 test
 00-303
 00-304
 00-305
 00-306
 00-307
 00-308
 00-309 Full Access
```

3 Select Full Access.

The MAX displays a password prompt.

4 Enter the password assigned to the Full Access security profile.

If you enter the correct password, the MAX displays the message `Password accepted. Using new security level.` If you enter the incorrect password, the MAX prompts you again for the password.

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. Because this profile is intended to be totally open, all privileges are 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.

To assign a password protecting the Full Access profile, proceed as follows:

1 From any VT100 menu, press <Ctrl> D.

The DO menu appears. For example:

```
DO...
>0=Esc
 P=Password
 C=Close TELNET
```

2 Press P or select P=Password.

A menu appears listing all security profiles:

```
Security profile...?
>00-301 Default
 00-302 test
 00-303
 00-304
 00-305
 00-306
 00-307
 00-308
 00-309 Full Access
```

3. Select Full Access.

   The MAX displays a password prompt.

4. Enter the password assigned to the Full Access security profile.

   If you enter the correct password, the MAX displays the message `Password accepted. Using new security level.` If you enter the incorrect password, the MAX prompts you again for the password.

5. Open the System > Security > Full Access profile.
6. Select the Passwd parameter and press Enter to open a text field.
7. Type a new password, and press Enter.
8. Exit the Full Access profile, saving your changes.

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, proceed as follows:

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
 Edit Com Call=N/A
 Edit Own Call=N/A
 Edit Cur Call=N/A
 Sys Diag=N/A
 All Port Diag=N/A
 Own Port Diag=N/A
 Download=N/A
 Upload=N/A
 Field Service=N/A
```

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

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, saving 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, proceed as follows:

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, saving 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, proceed as follows:

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, saving 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, proceed as follows:

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 configure the MAX to support AppleTalk Remote Access (ARA) connections, setting Profile Reqd=Yes disables Guest access to your network.

3 Exit the Answer profile, saving 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, proceed as follows:

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

Specifying the number of retry attempts

When an Ascend unit attempts to make a connection and the attempt fails, the MAX continues to attempt to complete the connection. The number of retry attempts allowed without using call blocking is very large; successive retries can cause excessive charges, congestion, and performance problems. With call blocking, you can specify the number of unsuccessful attempts to place a call that a MAX makes before blocking further attempts to make that connection. After the specified number of attempts have been made and failed, the blocking timer starts. The MAX continues to block further calls for a the length of time you specify.

To configuring call blocking, proceed as follows:

1. Open the Ethernet > Connections > *Any* Connection profile > Session options menu.
2. Set `Block calls after` to the number of retry attempts the MAX allows when placing a call.
3. Set `Blocked duration` to the length of time the MAX continues to block calls.

Note: Call blocking applies only to outgoing calls that are not answered by the far end. It does not apply to incoming calls or outgoing calls that connect and are immediately disconnected

Retrieving configuration updates from RADIUS

When you power up the MAX, it can retrieve a potentially large quantity of configuration information from the RADIUS server. Some of the data on the RADIUS server can change during operation. You can direct the MAX to retrieve this information in one of two ways:

- Using the Upd Rem Cfg command from the Sys Diag menu, you can instruct the MAX to retrieve a fresh configuration.
- You can initiate a RADIUS configuration update using the SNMP Set command, and use SNMP to poll the status of the update.

  The SNMP variable sysConfigRadiusCmd enables an SNMP manager to initiate a RADIUS configuration retrieval of routes, IP pools, connection information, and terminal server banners. You can poll the status of the retrieval by getting the value of another new SNMP variable, sysConfigRadiusStatus.

Setting Up Security Profiles

2

This chapter contains:

Understanding 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. 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 is Yes.
Edit Security	Grants or restricts privileges to edit Security profiles.	Yes No The default value is Yes.
Edit System	Grants or restricts privileges to edit the System profile and the Read Comm and R/W Comm parameters in the Ethernet profile.	Yes No The default value is Yes.
Edit Line	Indicates whether an operator can edit Line profiles.	Yes No The default value is Yes.
Edit All Ports	Indicates whether an operator can edit all Port profiles.	Yes No The default value is Yes.
Edit Own Port	Indicates whether an operator can edit their own Port profile.	Yes No The default value is Yes. To keep an operator from editing their own Port profile, you must set Edit Own Port=No *and* Edit All Ports=No.
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.

Table 2-1. Security profile parameters (continued)

Parameter	Description	Possible values
Edit Com Call	Indicates whether an operator can edit Call profiles that are not specific to any serial host port. Call profiles not specific to any serial host port are known as common Call profiles.	Yes No The default value is Yes. To keep an operator from editing common Call profiles, you must set Edit Com Call=No *and* Edit All Calls=No.
Edit Own Call	Indicates whether an operator can edit the Call profile that defines the connection between the user's MAX and the MAX being remotely managed over an AIM channel.	Yes No The default value is Yes. To keep an operator from editing the Call profile between a local and a remotely managed MAX, you must set Edit Own Call=No *and* Edit All Calls=No.
Edit Cur Call	Indicates whether an operator can edit all the parameters in the current Call profile.	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 Cur Call=No *and* Edit All Calls=No.
Sys Diag	Indicates whether an operator can perform all system diagnostics.	Yes No The default value is Yes.
All Port Diag	Indicates whether an operator can perform all serial host port diagnostics.	Yes No The default value is Yes.
Own Port Diag	Indicates whether an operator can perform port diagnostics for his or her own serial host port.	Yes No The default value is Yes. To completely disable the operator's ability to perform diagnostics for his or her own port, you must set Own Port Diag=No and All Port Diag=No.

Table 2-1. Security profile parameters (continued)

Parameter	Description	Possible values
Download	Indicates whether an operator can download the configuration of the MAX using the Save Cfg command.	Yes No The default value is Yes. **Note:** Whether you choose Yes or No, a user cannot download passwords to another device.
Upload	Indicates whether an operator can upload the MAX configuration from another device using the Restore Cfg command.	Yes No The default value is Yes. **Note:** When you save a configuration to file, passwords are not included in the download, so restoring from file clears all passwords in the MAX.
Field Service	Grants or restricts privileges to perform field service operations, such as uploading new system software.	Yes No The default value is Yes.

Configuring a Security profile

To configure a Security profile, follow these steps:

1 Open the System > Security menu.

2 Open any Security profile.

3 Set Name to a descriptive designation for the profile.

You can enter up to 16 characters. For example:

Name=Calabasas

4 For the Passwd parameter, specify a password containing up to 20 characters.

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 most DO commands. Only DO Esc, DO Close Telnet, and DO password are available.

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*."

Note: 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 edit the System profile and the Ethernet profile, set the Edit System parameter.

Yes enables an operator 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 edit privileges.

8 To indicate whether an operator can edit Line profiles, set the Edit Line parameter.

Yes enables an operator to edit Line profiles. The default value is Yes.

No prevents an operator from editing Line profiles.

9 To indicate whether an operator can edit all Port profiles, set the Edit All Ports parameter.

Yes specifies that an operator can edit all Port profiles by local or remote management. The default value is Yes.

No specifies that an operator cannot edit Port profiles.

10 To indicate whether an operator can edit his or her own Port profile, set the Edit Own Port parameter.

Yes specifies that the operator can use remote management to edit the Port profile for the port that has been called. The default value is Yes.

No specifies that an operator cannot edit his or her own Port profile. To keep an operator from editing his or her own Port profile, you must set Edit Own Port=No and Edit All Ports=No.

11 To indicate whether an operator can edit all the parameters in all Call profiles and Connection profiles, set the Edit All Calls parameter.

Yes specifies that an operator can edit all the parameters in all Call profiles and Connection profiles by Telnet, by local management (the Control port), or by remote management. 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 parameter, you must set Edit All Calls=No and Edit Cur Call=No.

12 To indicate whether an operator can edit Call profiles that are not specific to any serial host port, set the Edit Com Call parameter.

Call profiles not specific to any serial host port are known as common Call profiles. Numbers 201 through 216 denote port-specific Call profiles. Numbers 217 through 232 denote common Call profiles.

Yes specifies that an operator can edit common Call profiles by local or remote management. The default value is Yes.

No specifies that an operator cannot edit common Call profiles. To keep an operator from editing common Call profiles, you must set Edit Com Call=No and Edit All Calls=No.

13 To indicate whether an operator can edit the Call profile that defines the connection between the user's MAX and the MAX being remotely managed over an AIM channel, set the Edit Own Call parameter.

Yes specifies that the operator can edit the Call profile. The default value is Yes.

No specifies that an operator cannot edit the Call profile. To keep an operator from editing the Call profile between a local and a remotely managed MAX, you must set Edit Own Call=No and Edit All Calls=No.

14 To indicate whether an operator can edit all the parameters in the current Call profile, set the Edit Cur Call parameter.

Yes specifies that an operator can edit all the parameters in the current Call profile by local or remote management. Yes is the default.

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 Cur Call=No and Edit All Calls=No.

15 To indicate whether an operator can perform all system diagnostics, set the Sys Diag parameter.

Yes specifies that an operator can use any of the options in the Sys Diag menu by local or remote management. The default value is Yes.

No specifies that an operator cannot use any of the options in the Sys Diag menu.

16 To indicate whether an operator can perform all serial host port diagnostics, set the All Port Diag parameter.

Yes specifies that an operator can perform all the tasks listed in the Port Diag menu. The default value is Yes.

No specifies that an operator cannot perform any of the tasks listed in the Port Diag menu.

17 To indicate whether an operator can perform port diagnostics for his or her own serial host port, set the Own Port Diag parameter.

Yes specifies that an operator can use remote management to perform any of the options in the Port Diag menu for the port that has been called. The default value is Yes.

No specifies that the operator cannot perform port diagnostics for his or her own serial host port. To completely disable the operator’s ability to perform diagnostics for his or her own port, you must set Own Port Diag=No and All Port Diag=No.

18 To indicate whether an operator can download the configuration of the MAX using the Save Cfg command, set the Download parameter.

Yes specifies that a user can download profiles and other configuration parameters to another device for backup. The default value is Yes.

No specifies that an operator cannot download profiles and other configuration parameters.

Note: Whether you choose Yes or No, you cannot download passwords to another device.

19 To indicate whether an operator can upload the MAX configuration from another device using the Restore Cfg command, set the Upload parameter.

Yes specifies that the user can upload profiles and other configuration parameters from another device to the MAX. You must set Upload=Yes in order to use the Restore Cfg command. The default value is Yes.

No specifies that the user cannot upload profiles and other configuration parameters from another device to the MAX.

Note: When you save a configuration to file, passwords are not included in the download, so restoring from file clears all passwords on the MAX.

20 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.

21. 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. Specify the appropriate password, and press Enter.

   When you enter the correct password, the MAX displays the message `Password accepted. Using new security level`. If you enter an incorrect password, 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.

Note: To prevent unauthorized access, make sure to change the default password as soon as possible.

These are the default settings for the Full Access profile:

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

Setting Up User Authentication

3

This chapter contains:

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.

Types of Authentication

The MAX supports these types of authentication:

CLID (Calling Line ID)

You can require the MAX to authenticate incoming calls by checking the calling party’s phone number. The MAX performs CLID authentication before answering an incoming call. For details on configuring the MAX for CLID authentication, see “Setting up CLID authentication” on page 3-6.

Called Number

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

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 3-11.

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:

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

Call Type	Description
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 3-16
Terminal server	You can specify that users logging into the terminal server via a V.34, V.42, V.110, or V.120 connection must supply a username and password before gaining admission to the terminal server. See “Setting up authentication for dial-in terminal server users” on page 3-24.
Combinet	Combinet authentication uses the remote station’s MAC address as its username, and allows you to require a password for incoming calls. For details, see “Setting up Combinet authentication” on page 3-29.
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 3-33.
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 3-39.

How does user authentication work?

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

Note: You can also specify that the Answer profile be used for authentication. See “Preventing dial-in calls with the Name/Password profile” on page 3-36.

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

1 Before the MAX answers a call, it checks whether the Answer-Defaults profile requires Calling Line ID (CLID) authentication, called number authentication, or both.

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

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

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

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

   If CLID authentication is set to Fallback, the MAX must receive a CLID in the incoming call. The MAX answers the call if the CLID matches the local Connection profile or a RADIUS user profile. If the MAX does not receive a response from RADIUS, it uses the authentication set up in the Answer profile.

3. If a matching profile to the CLID or called number is found, the call is answered and further authentication is normally not required. If a matching profile to the CLID or called number is not found, and ID Auth=Require or Called Require, the call is not answered.

   Note: The RADIUS attribute Ascend-Require-Auth specifies whether additional authentication is required. See the *RADIUS Configuration Guide* for more information.

4. If CLID authentication and called number authentication are not required, or if the MAX finds a matching phone number in a local Connection profile or RADIUS user profile, it answers the call.

5. The MAX checks its other Answer profile settings.

6. 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.

7. 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. Setting up Profile Reqd configures user authentication for the following:

   – unencapsulated calls

   – calls using ARA or any other encapsulation listed in step 7

8. 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.

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 Connection profile, the MAX looks for a Name/Password profile.

If the MAX finds a Name/Password profile, it uses the name and password in the Name/Password profile and builds the connection using the settings in the Answer profile.

Note: The Name/Password profile applies only to ARA, PPP, MP, and MP+ calls. It does not apply to terminal server users.

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

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

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

12 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.

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

Note: You can limit the duration of incoming calls. See “Setting Connection profile parameters” on page 3-31

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, TACACS+, or RADIUS server.

  For details on configuring the MAX to use a TACACS or TACACS+ server, see “Setting up an authentication server” on page 3-44. For details on configuring the MAX to use a RADIUS server, see the MAX *RADIUS Configuration Guide*.
- Remote authentication using a AssureNet Defender server.

  For details on configuring the MAX to use a Defender server, see “Configuring direct Defender server authentication” on page 5-25.
- 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 3, “Setting Up User Authentication.”

Setting up CLID authentication

You can require the MAX to authenticate incoming calls by checking the calling party's phone number. The MAX performs CLID authentication before answering an incoming call. You can thereby ensure that the call originates from a known location. To set up CLID authentication, use the parameters listed in Table 3-2.

Table 3-2. CLID authentication parameters

Location	**Parameters with sample values**
System > Sys Config	Name=mygw
Ethernet > Answer	Id Auth=Require Profile Reqd=Yes
Ethernet > Answer > PPP Options	Recv Auth=Either
Ethernet > Answer > COMB Options	Password Reqd=Yes
Ethernet > Connections > *Any Connection profile*	Station=Emma Calling #=555-1213
Ethernet > Connections > *Any Connection profile* > Encaps Options	Recv PW=*SECURE*
Ethernet > Ethernet > Mod Config > Auth menu	CLID Timeout Busy=No CLID Fail Busy=No

When you set up CLID authentication, you can choose one of these configurations:

- Authenticate all callers using name, password, and calling line ID.

  For details, see "Setting up authentication using a name, password, and calling line ID" on page 3-7.
- Authenticate all callers using a calling line ID only.

  For details, see "Setting up authentication using a calling line ID only" on page 3-8.
- Use an external authentication server, such as a token-card authentication server, to authenticate users after CLID authentication.

  For details, see the MAX *RADIUS Configuration Guide*.
- Request PAP, CHAP, or MS-CHAP after CLID authentication.

  For details, see the MAX *RADIUS Configuration Guide*.

General guidelines

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

- In some installations, the WAN provider might not be able to deliver CLIDs, or a caller might choose to keep a CLID private.
- CLID authentication applies only where CLID is available end-to-end and ANI (Automatic Number Identification) applies to the call.

- T1 access lines and Switched-56 lines do not support CLID.
- When a user dials into the MAX using MP or MP+, the calling device may have more than one phone number associated with it; in these types of cases, the CLID is the phone number associated with the channel in use.
- If you set up a RADIUS user profile for callback and CLID-only authentication, the MAX never answers the call; the caller can therefore avoid billing charges.

CLID authentication requirement options

The *ISP/Telecommuting Guide* gives instructions for setting up CLID authentication and requiring that a RADIUS entry be used for the CLID authentication. You can also configure Connection Profiles to authenticate using caller ID, Ascend recommends that you perform this function in RADIUS.

When you set up CLID authentication either in RADIUS or in a MAX Connection profile, you must specify what the MAX requires for the CLID authentication. There are three options:

Table 3-3. CLID authentication requirement options

Option	Description
Require	The MAX must receive a CLID from the incoming call. The CLID must match a Calling # parameter in a local Connection profile or in a RADIUS user profile with Password = Ascend-CLID (see the *RADIUS Configuration Guide* for more information). If the MAX does not receive a CLID or if it cannot match the CLID, the call is not answered. **Note:** The matching user profile in RADIUS can require name and password authentication in addition to CLID. See the Ascend-Require-Auth attribute.
Prefer	The MAX does not require a CLID from the incoming call. If a CLID is received, however, the MAX compares the CLID with a Calling # parameter in a local Connection profile or with a RADIUS user profile with Password = Ascend-CLID. If the MAX does not receive a CLID from the incoming call, it uses the authentication configured in the Answer profile.
Fallback	The MAX must receive a CLID in the incoming call. If no CLID is received, the MAX does not answer the call. If a CLID is received, the MAX compares the CLID with a Calling # parameter in a local Connection profile or with a RADIUS user profile with Password = Ascend-CLID. If the CLID does not match either the Connection profile and the MAX does not receive a response from the RADIUS server, it uses the authentication configured in the Answer profile.

Setting up authentication using a name, password, and calling line ID

Note: To authenticate on all three criteria (name, password, and Caller ID), you must configure authentication in RADIUS by setting the Auth parameter to RADIUS. For information, see the MAX *RADIUS Configuration Guide*.

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

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

The Prefer setting specifies that whenever CLID is available, the MAX compares the calling party’s phone number to the value of the Calling # parameter in the Connection profile or a RADIUS user profile set up for Ascend-CLID.

– If a match is found, and no further authentication is required, the MAX accepts the call.

– If a match is found and the MAX requires further authentication (Profile Reqd=Yes in the Answer profile), the MAX applies authentication using the Recv Auth or Password Reqd parameters in the Answer profile.

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

Note: You can also set Id Auth=Require or Id Auth=Fallback.

2 Verify no local profiles are set up for CLID authentication.

3 Set Profile Reqd=Yes.

4 For PPP calls, set Recv Auth to the authentication protocol.

5 For Combinet calls, set Password Reqd=Yes.

6 Set the CLID Timeout Busy parameter to specify whether the MAX returns User Busy when CLID authentication fails due to a RADIUS timeout.

Set CLID Timeout Busy=Yes, to specify that MAX returns User Busy as the disconnect cause when CLID authentication fails due to a RADIUS timeout.

The default value is No. When CLID Timeout Busy=No, the MAX returns Normal Call Clearing as the disconnect cause.

7 Set the CLID Fail Busy parameter to specify whether the MAX returns User Busy when CLID authentication fails for any reason other than a RADIUS timeout.

Set CLID Fail Busy=Yes to specify that the MAX returns User Busy when CLID authentication fails to any reason other than a RADIUS timeout.

The default is No. CLID Fail Busy=No specifies that the MAX return Normal Call Clearing.

Note: You can choose the value for this field regardless of the Server setting since the occurrence of this failure does not depend upon using a RADIUS server.

8 Save your changes.

See the *RADIUS Configuration Guide* for further information.

Setting up authentication using a calling line ID only

Note: Although you can configure local Connection profiles to authenticate using a calling line ID only, we recommend that you perform this function in RADIUS.

To require all callers to authenticate using a calling line ID only, follow these steps:

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

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

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

The Require setting indicates that the calling party's phone number must match the value of the Calling # parameter in the Connection profile before the MAX can answer the call. If CLID is not available, the MAX does not answer the call.

4 Open the Ethernet > Connections menu.

5 In the Connection profile, specify the caller's phone number using the Calling # parameter.

6 Save your changes.

Setting up called number authentication

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

To set up called number authentication, use the parameters listed in Table 3-4.

Table 3-4. Called Number authentication parameters

Location	**Parameters with sample values**
System > Sys Config	Name=mygw
Ethernet > Answer	Id Auth=Called Require Profile Reqd=Yes
Ethernet > Answer > PPP Options	Recv Auth=Either
Ethernet > Answer > COMB Options	Password Reqd=Yes
Ethernet > Connections > *Any Connection profile*	Station=Emma Called #=555-1213
Ethernet > Connections > *Any Connection profile* > Encaps Options	Recv PW=*SECURE*

Setting up called number authentication options

You can choose one of these configurations for called number authentication:

- Authenticate all callers using name, password, and called number.

  For details, see "Setting up authentication using a name, password, and called number" on page 3-10.
- Authenticate all callers using the called number only.

  For details, see "Setting up authentication using the called number only" on page 3-11.
- Authenticate using an external authentication server, such as a token-card authentication server, to authenticate users after called number authentication.

When you configure called number authentication either in RADIUS or in a MAX connection profile, you must specify what the MAX requires for the called number authentication in the ID Auth parameter. There are two options:

Table 3-5. Called Number authentication options

Option	Description
Called Require	The MAX must receive a called number from the incoming call. The called number must match a Called # parameter in a local Connection profile or in a RADIUS user profile (see the *RADIUS Configuration Guide* for more information). If the MAX does not receive a called number or if it cannot match the called number, the call is not answered. **Note:** The matching user profile in RADIUS can require name and password authentication in addition to called number. See the Ascend-Require-Auth attribute.
Called Prefer	The MAX does not require a called number from the incoming call. If a called number is received, however, the MAX compares the called number with a Called # parameter in a local Connection profile or with a RADIUS user profile. If the MAX does not receive a called number from the incoming call, it uses the authentication configured in the Answer profile.

Setting up authentication using a name, password, and called number

Note: To authenticate on all three criteria (name, password, and called number), you must configure authentication in RADIUS by setting the Auth parameter to RADIUS. For information, see the MAX *RADIUS Configuration Guide*.

For further information, see the *RADIUS Configuration Guide*.

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

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

   The Prefer setting specifies that whenever the called number is available, the MAX compares the phone number called to the value of Called # in the Connection profile.

   – If a match is found, and no further authentication is required, the MAX accepts the call.

   – If a match is found and the MAX requires further authentication (Profile Reqd=Yes in the Answer profile), the MAX applies authentication using the Recv Auth or Password Reqd parameters in the Answer profile.

   – If the called number is not available, or 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.

2. Verify no Connection profiles are set up to authenticate users via called number.
3. Set Profile Reqd=Yes.
4. For PPP calls, set Recv Auth to the authentication protocol.

5. For Combinet calls, set Password Reqd=Yes.
6. Save your changes.

Setting up authentication using the called number only

Note: Although you can configure local Connection profiles to authenticate using the called number only, we recommend that you perform this function in RADIUS.

To require all callers to authenticate using a called number only, 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=Called Require.

   The Called Require setting indicates that the called number must match the value of the Called # parameter in the Connection profile before the MAX can answer the call. If the called number is not available, the MAX does not answer the call.
4. Open the Ethernet > Connections menu.
5. In the Connection profile, specify the called number using the Called # parameter.
6. Save your changes.

Setting up callback security

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

Ascend 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 (ID Auth=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 is 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.

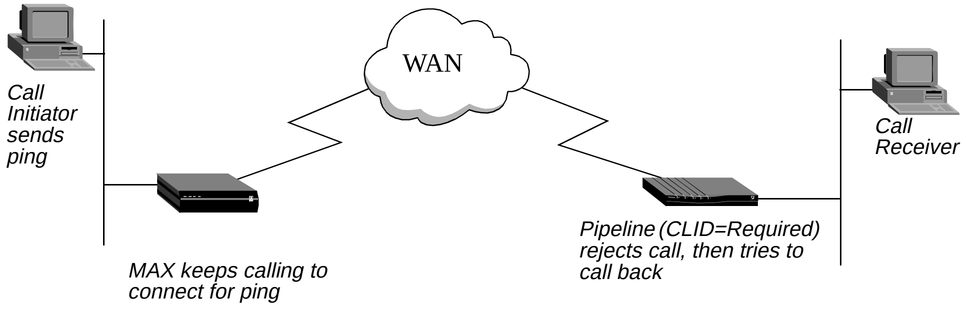
Call Initiator sends ping
WAN
Call Receiver
Pipeline (CLID=Required) rejects call, then tries to call back
MAX keeps calling to connect for ping

Figure 3-1. Callback connection failure

The Callback process is disrupted when protocols like ping and telnet continuously try to open a connection.

When Expect 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 Expect Callback is set to Yes.

Table 3-6 lists the Ascend callback parameters on the MAX.

Table 3-6. Ascend 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
```

Note: The MAX can also use the CLID in order to reach the remote end of the connection, if the CLID is available.

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.

Microsoft's Callback Control Protocol (CBCP)

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

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

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

Ascend's implementation of CBCP

CBCP is an option negotiated during the LCP negotiation of a PPP session. While support for CBCP is configured system-wide on the MAX, not every connection must negotiate its use. Parameters exist in the Answer Profile under Ethernet > Answer > PPP Options, and to each Connection Profile under Ethernet > Connections > *Any Connection profile* > Encaps Options.

The calling and called sides of a PPP session initiate authentication after acknowledging that CBCP is to be used.

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

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

Both sides of the connection must agree on whether the callback phone number is supplied by the client or by the MAX. A new trunk group parameter, configured on the MAX, supplies a trunk group that is prepended to phone numbers when supplied by the client.

Table 3-7 lists Microsoft's callback parameters on the MAX.

Table 3-7. Microsoft's CBCP parameters on the MAX

Location	Sample parameters
Ethernet > Answer > PPP options	CBCP Enable
Ethernet > Connections > *Any Connection profile* > Encaps options	CBCP Mode
Ethernet > Connections > *Any Connection profile* > Encaps options	CBCP Trunk Group

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

Negotiation of CBCP

Following are the steps from initial connection to MAX callback:

1 Caller connects to MAX.

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

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

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

5 The MAX verifies that the profile has CBCP Mode set. CBCP begins.

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

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

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

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

Configuring Microsoft's CBCP to use a Connection Profile

To configure CBCP to work with a Connection profile:

1 Open the Ethernet > Answer > PPP Options menu.

2 Set CBCP Enable = Yes.

3 Open the Ethernet > Connections > *Any Connection profile* > Encaps Options menu.

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

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

6 Save your changes.

Setting up call authentication via serial AIM ports

You can specify a password for calls placed across the Host serial inverse multiplexing ports in the Call profile for outgoing calls and in the Port configuration profile for incoming calls.

Understanding serial call authentication

Authentication is used only if the receiving unit has a password defined in the Port profile. If the Port profile in the receiving unit does not have a password defined, the units connect without authentication even though the originating unit may have sent authentication parameters.

Note: The MAX only authenticates AIM and BONDING calls; dual-port calls are not authenticated.

Upon initial connection of the first channel, the originating unit passes the Call profile password to the authenticating unit. The authenticating unit compares the password received with that stored in the Port configuration profile. If the password received matches the stored password, the session is established normally for the remainder of the call. If there is no match, the authenticating unit sends a message back to the originator and drops the session. The port status screen in Host > Dual > portname > Message Log indicates that the call failed authentication.

Configuring serial port passwords

To set the passwords, follow these steps:

1 For outgoing AIM or BONDING calls, enter the DBA call password at Call Password in the Host/Dual (or Host/6) > Port N Menu > Directory > *any Call profile*.

Dynamic Bandwidth Allocation (DBA) enables the MAX to increase bandwidth as needed and drop bandwidth when it is no longer required.

2 For incoming AIM and BONDING calls, enter the Port password at Port Password in Host/Dual (or Host/6) > Port N Menu > Port Config (the Port profile)

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 *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.

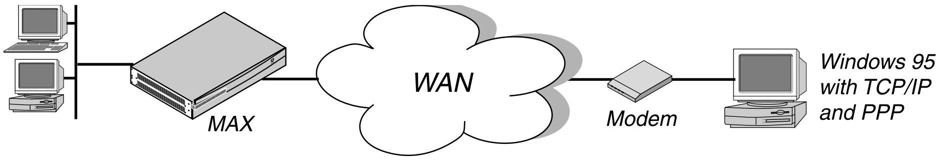

Figure 3-2. A PPP connection

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.

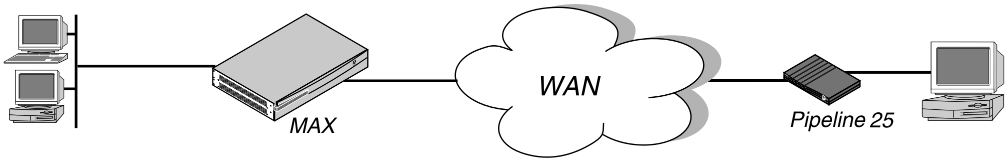

Figure 3-3. An MP+ connection

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, CHAP, and MS-CHAP authentication is not available for Combinet, ARA, V.34, V.42, V.110, or V.120 calls.

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

- The calling unit's secret is called the remote secret; the MAX does not know the value of this secret.
- The MAX unit's secret is called the NAS secret (because the MAX is an 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, or MS-CHAP for PPP, MP, and MP+ calls

To configure incoming and outgoing connections using PAP, CHAP, or 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 3-8.

Table 3-8. Parameters for incoming connections using PAP, CHAP, or MS-CHAP

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

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=100.0.0.20 Pool#1 Count=90 Pool Only=Yes

Ethernet > Connections > *Any Connection profile*	Station=dialmax
	Encaps=PPP, MP, or MPP

Ethernet > Connections > *Any Connection profile* > Telco Options	Dialout OK=Yes
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 for 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 *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, CHAP, or MS-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.

MP+ calls cannot combine an ISDN BRI channel with a channel on a T1 access line or a T1 PRI line.

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

If you set up a Name/Password profile, by default 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, CHAP, or MS-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).

Using 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, CHAP, or MS-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 3-9.

Table 3-9. 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, or 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.

  MP+ calls cannot combine an ISDN BRI channel with a channel on a T1 access line or a T1 PRI line.

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 answering side of the connection determines which authentication protocol the connection uses (if any).

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 authentication for dial-in terminal server users

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.

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

Table 3-10.Dial-in terminal server encapsulation types

Encapsulation Type	**Description**
Modem calls	These types of calls originate from either analog or digital modems. Incoming modem calls and incoming digital calls come over the same digital line to the MAX unit's integrated V.34 or V.42 digital modem. 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 digital 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.
V.110	A V.110 card provides eight V.110 modems, each of which enables the MAX to communicate with an asynchronous device over synchronous digital lines. An asynchronous device such as an ISDN modem encapsulates its data in V.110. The V.110 module in the MAX removes the encapsulation and enables an asynchronous session—that is, a terminal server session.
V.120 calls	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.

How terminal server authentication works

Note: The following does not apply to authentication using the an Answer or Connection profile as a template. See "Using an Answer or Connection profile as a template" on page 3-28.

More general information on how authentication works in the MAX is in "How does user authentication work?" on page 3-3. See"Per-user terminal server authentication" for the differences between standard terminal server authentication and per-user terminal server authentication, such as CLID and Called-party authentication.

Standard terminal server authentication

Terminal server authentication 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.

Per-user terminal server authentication

Authentication by CLID or Called-party number is slightly different from authentication on a general basis. For per-user terminal server authentication, the following events occur:

1 Before the MAX answers a call, it checks whether the Answer-Defaults profile requires Calling Line ID (CLID) authentication, called number authentication, or both.

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

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

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

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

3 If CLID authentication and called number authentication are not required, or if the MAX finds a matching phone number in a local Connection profile or RADIUS user profile, it answers the call.

4 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.

5. 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.

Modem calls

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 3-16. In these cases, none of the above steps 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.

This section describes first-level authentication using the Passwd parameter. For information on authentication using a Connection profile, see “Setting Connection profile parameters” on page 3-20.

Dial-in calls with no login host specified

You can configure the MAX to accept dial-in calls when Login-Service=TCP-CLEAR or Login-Service=Telnet, and no Login Host is specified in the RADIUS users profile. This does not apply to PPP encapsulated calls, since the MAX does not accept dial-in PPP calls with the Login-Service set either to Telnet or TCP-CLEAR.

To set up the MAX to accept dial-calls when no login server is specified, set Auth TS Secure=No in the Ethernet > Mod Config > Auth menu. The default is Auth TS Secure=Yes, which means the MAX drops dial-in calls if there is no login server and Login-Server is Telnet or TCP-CLEAR.

Immediate 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.

Configuring terminal server authentication

Table 3-11 lists the parameters you can use to set up terminal server password authentication.

Table 3-11.Terminal server security parameters

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

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 3-28.

5 Set the Login Timeout parameter.

Specify the number of seconds the MAX waits 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 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 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 3-28.

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*.

3 Save your changes.

Setting up Combinet authentication

The MAX supports Combinet bridging to link two LANs as though they were one segment. Figure 3-4 shows a Combinet connection between two networks.

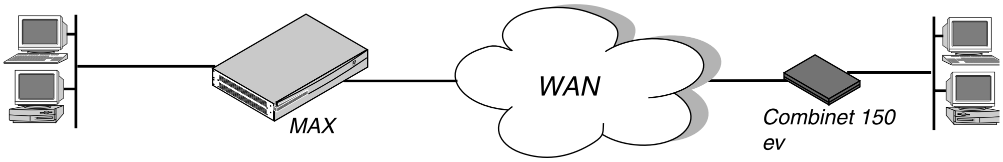

Figure 3-4. A Combinet connection

Combinet bridging uses a physical MAC (Media Access Control) address and a password to authenticate calls. For information on how MAX authentication works, see “How does user authentication work?” on page 3-3.

Table 3-12 lists the Combinet authentication parameters.

Table 3-12.Combinet authentication parameters

Location	Parameters with sample values
System > Sys Config	Name=mygw
Ethernet > Answer	Profile Reqd=Yes
Ethernet > Answer > PPP Options	Bridge=Yes
Ethernet > Answer > Encaps	COMB=Yes
Ethernet > Answer > COMB Options	Password Reqd=Yes
Ethernet > Mod Config	Bridging=Yes

Ethernet > Connections > *Any Connection profile*	Station=000145CFCF01
	Encaps=COMB
	Bridge=Yes
	Max Call Duration=0

Ethernet > Connections > *Any Connection profil*e > Telco Options	Dialout OK=Yes
Ethernet > Connections > *Any Connection profile* > Encaps Options	Recv PW=*SECURE* Send PW=*SECURE* Password Reqd=Yes

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

Understanding Combinet authentication

To configure incoming connections using Combinet 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, and whether a password is required.
- Set up a Connection 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 a Combinet call, it checks whether COMB encapsulation is enabled in the Answer profile and, if so, whether a Combinet password is required. It then looks for a Connection profile that matches the caller's MAC address (and, if appropriate, the caller's password). If it finds a match, it accepts the call.

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

Setting system-wide parameters

To set system-wide parameters for authenticating a Combinet connection, follow these steps:

1 Set the Name parameter in the System > Sys Config menu to specify the name of the MAX.

2 Open the Ethernet > Answer menu.

3 To disable Guest access via Combinet, set Profile Reqd=Yes.

Note that Combinet does not support PAP, CHAP, or MS-CHAP authentication.

4 In the Ethernet > Answer > PPP Options menu, set Bridge=Yes.

5 In the Ethernet > Answer > Encaps menu, set COMB=Yes.

6 To require a password in addition to a MAC address, set Password Reqd=Yes in the Ethernet > Answer > COMB Options menu.

When Password Reqd=Yes, the MAX compares the caller's MAC address to each of these values until it finds a match:

– Station parameter in a Connection profile

– User-Name attribute in a RADIUS user profile

The MAX also compares the value of the caller's password to one of these values:

– Recv PW in a Connection profile

– Password attribute in a RADIUS user profile

When Password Reqd=No, the MAX uses the caller's MAC address only.

7 Set Bridging=Yes in the Ethernet > Mod Config menu.

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 authenticating a Combinet connection, follow these steps:

1 Open the Ethernet > Connections menu.

2 Open the Connection profile.

3 Set the Station parameter to the MAC address of the device making the call.

4 Set Encaps=COMB.

5 Set Bridge=Yes.

6 To limit the duration of calls that use this Connection profile, specify a value for the Max Call Duration parameter.

You can specify between 1 and 1440 minutes. The connection is checked once per minute, so the actual time of the call is slightly longer (usually less than a minute longer) than the actual time you set.

The default is Max Call Duration=0. This means that incoming calls is not timed and can be of unlimited duration.

Note: If you have set this call to use the Answer profile for authentication, you must set the Max Call Duration value in the Answer profile.

7 Open the Encaps Options submenu of the Connection profile.

8 For incoming calls, set the Recv PW parameter.

The Recv PW parameter specifies the password that the remote end of the link must send;

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.

You set the Recv PW parameter only if Password Reqd=Yes in the Ethernet > Answer menu.

9 For outgoing calls, set the Password Reqd and Send PW parameters.

– To require the MAX to send a password for outgoing connections, set Password Reqd=Yes.

– Using the Send PW parameter, specify 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.

10 Close the Encaps Options submenu.

11 To grant access to the Immediate Modem feature, open the Telco options submenu of the Connections profile and set Dialout OK=Yes.

For more information on restricting the Immediate Modem feature, see“Restricting access to the Immediate Modem feature” on page 6-7.

12 Save your changes.

Setting up a RADIUS user profile

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

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 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, and V.120 calls only. It does not support V.110 calls or synchronous connections.

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

Figure 3-5 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.

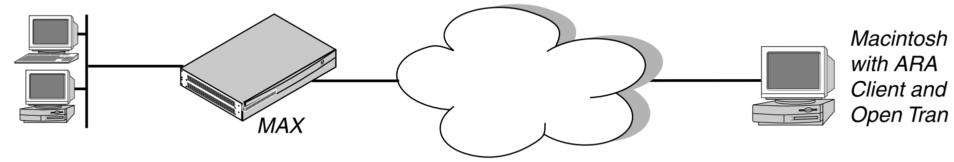

Figure 3-5. An ARA connection

Table 3-13 shows ARA authentication parameters on the MAX.

Table 3-13.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

Ethernet > Connections > *Any Connection profile*	Station=Ted
	Encaps=ARA

Ethernet > Connections > *Any Connection profile* > Encaps Options	Password=*SECURE*
Ethernet > Names/Passwords > *Any Name/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

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, Name/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, TACACS 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.

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

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.

Preventing 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 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).

Using 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*.

Using a SecurID server with AppleTalk Remote Access (ARA)

A SecurID server can authenticate ARA callers using the following:

- Connection profile (see "Setting Connection profile parameters" on page 3-31)
- Password profile (see "Setting Name/Password profile parameters" on page 3-36)
- RADIUS user profile

Authentication using RADIUS and a SecurID server

For authentication with RADIUS and a SecurID server, set Auth=RADIUS/LOGOUT in the Ethernet>Mod Config menu.

The SecurID client module must be version 1.3 or later.

Once the user makes the initial connection, SecurID authentication begins with a pop-up screen on the Macintosh. At this point, the user must enter the *User ID* and *Passcode*. When Auth=LOGOUT/RADIUS, the username must be SecurID, and there no password should be given. If the user enters incorrect values, he or she gets two more tries to authenticate before the connection fails.

If the user is required to enter a new PIN, a pop-up screen prompts for this information. The user has three chances to enter the correct PIN. Once the new PIN is accepted, a pop-up screen instructs the Macintosh user to wait for the token code to change and then to log in with the new PIN and token code.

Setting up X.25 authentication

X.25 is an international standard protocol established by the Consultative Committee on International Telephony and Telegraphy (CCITT) to transmit information between users over a WAN. It handles both high-volume data transfers and interactive use of host machines.

X.25 exchanges packets between a local DTE (Data Terminal Equipment) and a remote DCE (Data Circuit-Terminating Equipment). The remote DCE is itself attached to a remote DTE.

X.25 terminals can connect to the MAX via an X.25/PAD or X.25/IP session. The MAX unit's X.25/PAD (Packet Assembler/Disassembler) implementation allows users to access a packet-switched network over a leased line or a nailed-up ISDN connection.

A PAD is an asynchronous terminal concentrator that enables several asynchronous devices to share a single network line. The PAD assembles data from terminals into packets for transmission to an X.25 network, and disassembles incoming packets from the network into a separate data stream for each terminal. In addition to this multiplexing function, the PAD also provides a nearly error-free connection.

The MAX unit's X.25/IP implementation supports the use of IP routing over an X.25 link; it does not support bridging or other routing protocols. Ascend's implementation of IP over X.25 follows the specification for IETF RFC1356 encapsulation. This implementation connects two or more IP networks linked to a public or private packet-switched network (PSPDN).

Table 3-14 lists the parameters for X.25 authentication

Table 3-14.X.25 authentication parameters

Location	Parameters with sample values
Ethernet > Answer	Profile Reqd=Yes
Ethernet > Answer > Encaps	X25/PAD=Yes X25/IP=Yes
Ethernet > Answer > PPP Options	Recv Auth=Either
Ethernet > Mod Config/TServ Options	Immed Service=X25/PAD Immed Host=311021755555

Ethernet > Connections > *Any Connection profile*	Station=dialmax
	Encaps=X25/PAD or X25/IP

Ethernet > Connections > *Any Connection profile* > Encaps Options	Recv PW=*SECURE*

This section describes how to set up X.25 authentication in the MAX configuration interface. For complete information on setting up X.25 connections on the MAX, see the MAX *ISP & Telecommuting Configuration Guide*. For complete information on setting up X.25 calls and authentication in RADIUS, see the MAX *RADIUS Configuration Guide*.

To set up X.25 authentication, follow these steps:

1 Open the Ethernet > Answer menu.

2 Set Profile Reqd=Yes.

3 Open the Ethernet > Answer > Encaps menu.

4 Set X25/PAD=Yes and X25/IP=Yes.

5 Open the Ethernet > Answer > PPP Options menu.

6 For an X.25/IP user, set Recv Auth=Either.

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

8 If you want terminal server users to immediately begin an X.25/PAD session, set these parameters:

- Set Immed Service=X.25/PAD.
- Set the Immed Host parameter to the X.121 address of the remote device.

Terminal server users must pass authentication according to the terminal server parameters you set. For information, see “Setting up authentication for dial-in terminal server users” on page 3-24.

9 Open the Ethernet > Connections menu.

10 Open the X.25 user’s Connection profile.

11 For an X.25/PAD connection, set Encaps=X.25/PAD; for an X.25/IP connection, set Encaps=X.25/IP.

12 For an X.25/IP connection, set the Station name parameter to the name of the remote device.

13 Open the Encaps Options submenu of the Connection profile.

14 For an X.25/PAD or an X.25/IP connection, set the Recv PW parameter to the password the remote user must enter.

15 Save your changes.

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 3-15.

Table 3-15.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 *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 *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 3-16 shows the relevant parameters on the MAX.

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 4-12.

Table 3-16.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 profile*	Name=Ted Recv PW=*SECURE*

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), TACACS (Terminal Access Concentrator Access Control Server), or TACACS+ (Terminal Access Concentrator Access Control Server Plus) to centrally control, manage, and audit security.

Understanding authentication servers

When the MAX receives an incoming call, it first looks through its resident profiles (Connection and Name/Password profiles). If it does not 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

  RADIUS is a protocol originally developed by Livingston Enterprises, and extended by Ascend Communications, Inc. The extensions 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), Combinet name and password validation, 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 or TACACS+ server" on page 3-45.

- TACACS+

  TACACS+ is an extension of TACACS. For information on setting up the MAX to operate with a TACACS+ server, see "Configuring the MAX to use a TACACS or TACACS+ server" on page 3-45.

- AssureNet Defender

  The MAX supports terminal server authentication through the Defender server. If the MAX is configured to use Defender authentication, all authenticated users are given service only according to the parameters of the TServ Options submenu for the Ethernet profile.

- 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 a significant advantage. 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.

Configuring the MAX to use a TACACS or TACACS+ server

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

This section describes how to configure the MAX to communicate with a TACACS or 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=Yes
  APP Server=No
  APP Host=N/A
  APP Port=N/A
  CLID Timeout Busy=No
  CLID Fail Busy=No
  SecurID DES encryption=N/A
  SecurID host retries=N/A
  SecurID NodeSecret=N/A
```

2 Set Auth=TACACS or TACACS+.

3 For each Auth Host parameter, specify the IP address of a TACACS or 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 again to connect to to Auth Host #1 and waits for the same amount of time. If the MAX does not receive a response within the specified timeout, it sends a request for authentication to Auth Host #2; if it again receives no response within the time specified by Auth Timeout, it tries to connect to the next server on the Auth Host List and repeats the process. 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. If the MAX is unsuccessful in obtaining a response from any of the servers on the list, the connection fails.

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 or TACACS+ software.

For example, you might specify this setting:

```
Auth Port=1645
```

The MAX and the TACACS or 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 or 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 3-17 shows authentication methods and the specific information you should consider if you use a particular method with Local Profile First=No.

Table 3-17.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 does not produce a challenge if there is a local profile. This defeats the security of using PAP-TOKEN.
PAP-TOKEN-CHAP	Brings up one channel, but all other channels fail.
CACHE-TOKEN	If the remote side has ever authenticated using a challenge, CACHE-TOKEN does not work with local profiles. If the remote side has not ever authenticated, there are 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.

Defining Static Filters

4

This chapter contains:

Introduction to Ascend filters

A packet filter contains rules that specifies what the MAX does when it encounters different types of packets. When you specify a packet filter in a RADIUS user profile, the MAX monitors the data stream associated with that profile and takes a specified action when packet contents match the filter rules. Each filter specification either forwards or drops packets. You can apply a filter to inbound packets, outbound packets, or both. In addition, you can specify that the MAX forward or drop those packets that match the rules, or all packets *except* those that match the rules.

You can set up three types of packet filters on a per-user basis:

- generic filter

  A generic filters examine the byte- or bit-level contents of a packet. It focuses on certain bytes or bits and compare them with a value defined in the filter. To use generic filters effectively, you need to know the contents of certain bytes in the packets you wish to filter. Protocol specifications are usually the best source of such information

- IP filter

  An IP filter examines higher level fields specific to IP packets. It focuses on known fields, such as source or destination address, protocol number, and so forth. An IP filter operates on logical information that is relatively easy to obtain.

- IPX filter

  An IPX filter examines fields specific to IPX packets. You can direct the MAX to filter on the basis of network address, node address and socket number.

How packet filters work

You can specify several filters in a RADIUS user profile. Filter entries apply on a first-match basis. Therefore, the order in which you specify filter entries is significant. When you define a filter in a RADIUS user profile, it applies to data the user sends or receives. If you make changes to a filter, the changes do not take affect until a call uses that profile.

A match occurs at the first successful comparison between a filter and the packet being examined. When a comparison succeeds, the filtering process stops and the MAX applies the forward or drop action to the packet.

If no comparisons succeed, the packet does not match the filter. However, the MAX does not forward the packet. When no filter is in use, the MAX forwards all packets. However, once you apply a filter to a connection, this default is *reversed*. For security purposes, the MAX does not automatically forward non-matching packets. It requires a rule that explicitly allows those packets to pass.

In a generic filter, all settings work together to specify a location in a packet and a number that the MAX compares to the value in that location. In an IP filter, the MAX makes a set of distinct comparisons in order. When a comparison fails, the packet goes on to the next comparison. When a comparison succeeds, the filtering process stops and the MAX applies the forward or drop action to the packet. The IP filter tests proceed in the following order:

1. Compare the source address specified by the filter to the source address of the packet. If they are not equal, the comparison fails.
2. Compare the destination address specified by the filter to the destination address in the packet. If they are not equal, the comparison fails.
3. If the protocol specified by the filter is zero (which matches any protocol), the comparison succeeds. If it is non-zero and not equal to the protocol field in the packet, the comparison fails.
4. If the source port specified by the filter does not compare to the source port of the packet as the filter indicates, the comparison fails.
5. If the destination port specified by the filter does not compare to the destination port of the packet as the filter indicates, the comparison fails.

If the filter specifies a match only if a TCP session is already established, and a TCP session is up, the comparison succeeds. Filter entries apply on a first-match basis. Therefore, the order in which you specify filter entries is significant. When a comparison succeeds, the filtering process stops and the MAX applies the forward or drop action to the packet.

If no comparisons succeed, the packet does not match the filter and the MAX does not forward the packet. When no filter is in use the MAX forwards all packets. Once you aply a filter to a connection, this default is reversed. For security purposes, the MAX does not automatically foward non-matching packets. It requires a rule that explicitly allows these packets to pass. 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.

When you define a filter in a user profile, it applies to data the user sends or receives. If you make changes to a filter or filter reference in a RADIUS user profile, the changes do not take effect until a call uses that profile. For complete information about how filters work, see the chapter on using filters in the MAX *ISP and Telecommuting Configuration Guide*.

You can also set up filters on the MAX or define firewalls in SAM, and then specify those filters or firewalls in a RADIUS user profile. When the connection is made the RADIUS user profile determines which filters are used for the connection. For more information, see the *MAX RADIUS Configuration Guide*, or your SAM documentation.

Note: This chapter describes how to set up and use data filters only. For information on how to configure call filters, see the MAX *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 *ISP and Telecommuting Configuration Guide*.

Data filters for dropping or forwarding certain packets

A data filter defines which packets the MAX can transmit on a connection. Many sites use data filters for security purposes, but you can apply data filters to any purpose that requires the MAX to drop or forward only specific packets. For example, you can use data filters to drop packets addressed to particular hosts or to prevent broadcasts from going across the WAN. You can also use data filters to allow users to access only specific devices across the WAN.

When you apply a data filter, its forward or drop action affects the actual data stream by preventing certain packets from reaching the Ethernet from the WAN, or vice versa (Figure 4-1).

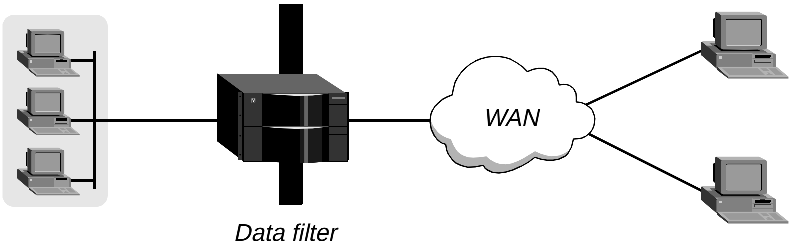

Figure 4-1. Data filters can drop or forward certain packets

Data filters do not affect the idle timer, and a data filter applied to a RADIUS user profile does not affect the answering process.

Overview of filter profiles

Figure 4-2 shows how filters are organized adn the terminology used to describe each part of a filter.

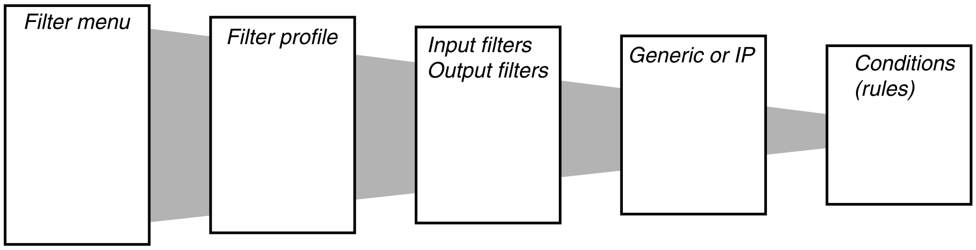

Figure 4-2. Filter terminology

- 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 conditions within that profile.

- Filter profile

  A Filter profile is a set of filter conditions.

- 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 4-4 for details.

- Generic, IP, or IPX filters

  Each input filter or output filter can be one of two types: Generic or IP, or IPX.
- Filter conditions

  Filter conditions specify the actual packet characteristics that the MAX examines in the data stream. Generic filter conditions specify locations and values that can appear in any packet. IP filter conditions specify IP-specific packet characteristics, such as address, mask, and port. IPX filter conditions specify IPX-specific packet characteristics, such as network address, node address, and socket number. Once you assign a type, you can open the corresponding submenu to define the packet-level filter conditions. For details, see “Defining generic filter conditions” on page 4-5 and “Defining IP filter conditions” on page 4-7.

Filtering inbound and outbound packets

To set up filters, you must complete 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 a descriptivee name for the profile. For example,

   ```
   Name=IP Data
   ```
4. Open the Input Filters or Output Filters submenu.

   When you select Input Filters, the following 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...
  IPX...
```

For example, when you open an *Out filter,* the following menu appears:

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

6 To activate the filter, set Valid=Yes.

To be able to apply the filter, you must activate it.

7 Define the filter type, Generic; IP filter, or IPX filter.

Defining generic filter conditions

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

Table 4-1. Generic filter conditions

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 conditions, 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 conditions

If Type=IP, you can define filter conditions 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 conditions you can specify in an IP filter.

Table 4-2. IP filter conditions

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 conditions, 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 both mask and address 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

– 89 — OSPF

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).

Defining IPX filter conditions

If Type=IPX, you can define filter conditions relevant IPX packets and bridged packets.

An IPX filter can examine network address, node address, and socket number. Table 4-2 shows the filter conditions you can specify in an IPX filter.

Table 4-3. IP filter conditions

Location	Parameters with sample values
Ethernet > Filters > Any Filter profile > Input filters > 01 to 12 > Ipx Ethernet > Filters > Any Filter profile > Output filters > 01 to 12 > Ipx	Forward=Yes Src Network Adrs=aaaa1234 Dst Network Adrs=bc34aa56 Src Node Adrs=111111111111 Dst Node Adrs=00000000000 Src Socket #=0451 Src Socket Cmp=Eql Dst Socket #=N/A Dst Socket Cmp=None

To specify IPX filter conditions, follow any or all of these steps:

1 Set the Forward parameter.

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 Src Network Adrs.

Specifies the address to which the MAX compares a packet's source network address. Enter the address in hexadecimal format. The null address (000000000000) is the default. If you accept the default, the MAX does not use the source network address as a filtering criterion.

3 Set Dst Network Adrs.

Specifies the address to which the MAX compares a packet's destination network address. Enter the address in hexadecimal. The null address (000000000000) is the default. If you accept the default, the MAX does not use the destination nework address as a filtering criterion.

4 Set Src Node Adrs.

Specifies the node address to which the MAX compares a packet's source node address. Enter the address in hexadecimal. The null address (000000000000) is the default. If you accept the default, the MAX does not use the source node address as a filtering criterion.

5 Set Dest Node Adrs.

Specifies the node address to which the MAX compares a packet's source node address. Enter the address in hexadecimal. The null address (000000000000) is the default. If you accept the default, the MAX does not use the destination node address as a filtering criterion.

6 Set the Src Socket # parameter.

This parameter identifies a specific IPX socket. For example, 0451is the socket used for NetWare file services.

7 Set the Src Socket Cmp parameter.

This parameter specifies the type of comparison the MAX makes when using the Src Socket # parameter.

8 Set the Dst Socket # parameter.

This parameter identifies a specific IPX socket. For example, 0451is the socket used for NetWare file services.

9 Set the Dst Socket Cmp parameter.

This parameter specifies the type of comparison the MAX makes when using the Dest Socket # parameter.

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 3-42.

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 contains:

How security cards work

You can configure your network site to require that users change passwords several 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 typically the size 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 configure a remote authentication server supporting 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 "How the SecurID ACE/Server works without RADIUS" on page 5-16 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.

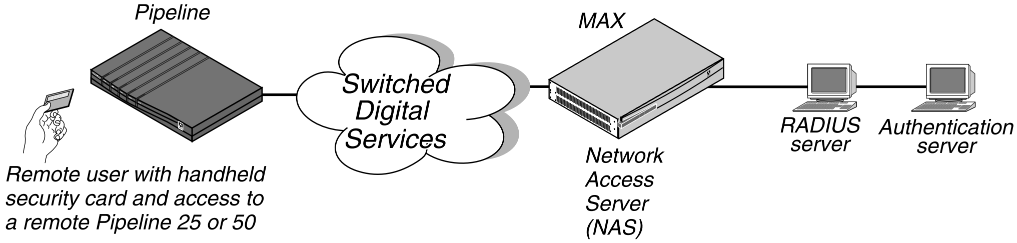
Pipeline
Switched Digital Services
MAX
RADIUS server
Authentication server
Remote user with handheld security card and access to a remote Pipeline 25 or 50
Network Access Server (NAS)

Figure 5-1. Using an external authentication server

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

1 A user attempts to open a connection to the MAX, sending his or her 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 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 should 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 5-23.

Understanding security-card authentication methods

You can set up SafeWord and ACE/Server 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.

- 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

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/Server or SafeWord server. 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 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 5-23.

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 an ACE/Server or 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 5-6.
- 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 MAX to recognize the APP Server utility

To allow users to supply token passwords from a PC or UNIX host on the local network, you must configure the MAX to communicate with the APP Server utility on that host. 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 might 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 *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 request 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 call's base channel, CHAP encrypts the auxiliary password specified by Aux Send PW 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/Server 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 5-9.
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 option 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 forces 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 appsrvr.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 5-9.

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/Server or SafeWord server returns a password challenge that looks similar to this one:

```
From: hostname
0-Challenge: challenge
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/Server 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/Server 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 *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.

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

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

1 Open the Ether > net > 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.

   Note: For a SecurID server to authenticate an AppleTalk Remote Access (ARA) caller through RADIUS, set Auth=RADIUS/LOGOUT. See "Setting up ARA authentication" on page 3-33 for more information about setting up a ARA connection through RADIUS.

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 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 Reference Guide`*`.`

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>	
<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.

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

Parameter	Possible Values	Description
	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.

Conventions

The conventions in the following table apply to all 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>	Is a string, but it should take on the dotted decimal form of an IP address, optionally followed by a subnet mask; for example, 1.2.3.4/24.

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 one 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 is 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 *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.

How Defender server authentication works

There are three major stages in authentication using AssureNet Pathways' Defender. The MAX' behavior will depend upon the stage the call dialing the MAX was in when the connection with the host is lost.

Table 5-7. Token card authentication

1	Usually a short time after the caller has connected to the MAX and before the MAX has received the first prompt from the authentication host. The Defender server provides the text of the prompts or challenges, and the MAX passes them through to the caller.	Calls in Stage 1 are preserved if an authentication host is unavailable or loses its connection. This might be the case when the very first caller is authenticating with Defender after the router boots up, and the first authentication host is unavailable. The Defender authentication code in the router will try the second and third hosts in order to authenticate the user.
2	During the time the caller is interacting with the authentication host, but before the authentication sequence is complete. The Defender uses a challenge-response protocol, with a token card to provide the responses.	Calls in Stage 2 are never preserved if an authentication hosts loses its connection. Defender has no mechanism for having one authentication server take over for another if the first loses connection in the middle of a state.
3	When the caller has completed authentication and is interacting with the MAX normally (either asynchronously or framed).	Callers in Stage 3 are not dropped by the router since their calls are already authenticate. However, because the host on which they authenticated is no longer available, their logout time will not be sent (as would be the case if the host had remained connected). Defender provides no mechanism to notify one authentication host when a user call that was authenticated by another host is terminated.

When no authentication host is available

When a MAX can not establish contact with any of the authentication hosts in the list, all sessions are dropped, including calls in Stage 1.

If a caller who has been disconnected tries again to make a connection, the MAX will begin again the process of connecting to authentication hosts on the list until it either succeeds or has tried every host in the list.

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=0137.174.81.0
Auth Host #3=0137.174.80.25
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.

3 Specify up to three authentication hosts for the Auth Host # parameters.

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

5 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.

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

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 Normally APP Server = No. APP Server only applies when the MAX makes outgoing calls to MAXs and other sites using token card authentication. See the *MAX Reference Guide* for more information.

9 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 Reference Guide*.

10 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. This chapter contains:

Setting up terminal server security

A terminal server connection is host-to-host connection that uses analog modem, ISDN Terminal Adapter (using V.110 or V.120 encapsulation), or raw TCP. 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 authentication for dial-in terminal server users" on page 3-24 for more information about the authentication required before a remote user can get access to any of these features.

When the MAX receives an analog modem, ISDN TA, or raw TCP call, it determines whether the call is PPP-encapsulated. If it is, the MAX forwards the call to the router. If it is not PPP-encapsulated, 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.

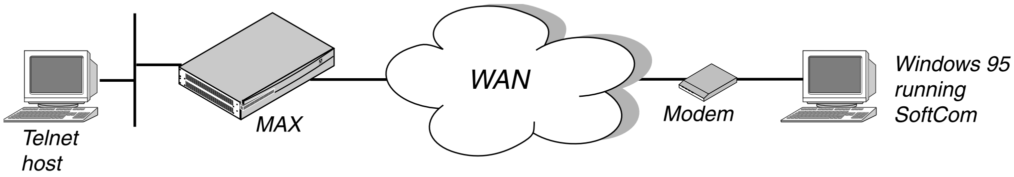

Figure 6-1. A remote terminal server connection

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.
- Permit TCP-CLEAR or Telnet dial-in access even when the RADIUS user's profile does not specify a login host.
- Set a timeout value so that users are disconnected if they have not completed logging in when the timer has elapsed.
- Disconnect a user's Telnet connection using the session ID for the connection.

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= Password Prompt= 3rd Prompt=Service? 3rd Prompt Seq=First 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=Yes

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 *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 Password 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 6-4.

9 Save your changes.

Sample prompts

Suppose you accept the default settings for the Login Prompt and Password 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.

Dial-in calls with no login host specified in RADIUS

You can configure the MAX to accept dial-in calls when Login-Service-TCP-CLEAR or Login-Service=Telnet, and no Login Host is specified in the RADIUS users file. This does not apply to PPP encapsulated calls, since the MAX does not accept dial-in PPP calls with the Login-Service set either to Telnet or TCP-CLEAR.

To set up the MAX to accept dial-calls when no login server is specified, set Auth TS Secure=No in the Ethernet > Mod Config > Auth menu. The default is Auth TS Secure=Yes, which means the MAX drops dial-in calls if there is no login server and Login-Server is Telnet or TCP-CLEAR.

Configuring per-user access to terminal server commands

The Framed Only parameter in the Answer profile and the Connection profiles enables you to limit specific users to the PPP, SLIP, CSLIP, and Quit commands in the MAX terminal server interface.You can configure per-user access to the terminal server commands in the Answer profile or in the Connection profile:

- The Answer profile affects users who do not have a Connection profile, users with a Name/Password profile, or RADIUS-authenticated users whose connections are built in part with the Answer profile

- The Connection profile only affects individual users connecting to the MAX using a particular Connection profile

To configure per-user access to the terminal server:

1 Select Ethernet > Answer > Session Options *or*

Ethernet > Connections > *a Connection profile* > Session Options

2 Specify one of the following values for Framed Only:

– No (the default)

Specifies that terminal server users connecting through this profile have unlimited access to the terminal server commands.

– Yes

Specifies that terminal server users connecting through this profile only have access to the PPP, SLIP, CSLIP, and Quit terminal server commands.

3 Save and exit the profile.

If a user restricted to these commands tries to execute any other terminal server command, the MAX displays the following message:

```
Unauthorized Terminal Server Command.
```

Dealing with unauthorized Telnet and terminal server sessions

When a user activates a Security profile, the MAX generates a Syslog message notifying you that the event occurred. A user can activate a Security profile in a Telnet session or a serial-line COM port session by selecting the Security profile and specifying the proper password. When a user activates a Security profile, the new Syslog messages show the name of the Security profile, the IP address of the Telnet client or the COM port number, and the local IP address.

The EventSyslog message has one of these formats:

```
^DP(assword)ASCEND: "<profile_name>" ... for <remote_IP> on <local_IP>
```

```
ASCEND: "<profile_name>" ... from <COM_port> on <local_IP>
```

- The <profile_name> argument specifies the name of the activated Security profile.
- The <remote_IP> argument specifies the IP address of the Telnet client.
- The <local_IP> argument specifies the local IP address of the MAX.
- The <COM_port> argument specifies the COM port number for the session.

On system login, the MAX does not generate a Syslog message for the Default Security profile; for all events other than system login, the MAX generates a Syslog message for the Default Security profile. If Syslog is enabled, messages at LEVEL_NOTICE appear when a user activates a Security profile and the MAX accepts the Security profile password.

These two messages signal that a Telnet client has enabled a Security profile:

```
Jan 10 10:05:17 eng-lab-141 ASCEND: "Full Access" security profile
enabled for 206.65.212.9 on 192.168.6.141.
```

```
Jan 10 10:07:26 eng-lab-141 ASCEND: "Default" security profile enabled
for 206.65.212.23 on 192.168.6.141.
```

This message signals that a COM port user has enabled the Full Access profile:

```
Jan 10 10:03:52 eng-lab-141 ASCEND: "Full Access" security profile
enabled from com port 0 on 192.168.6.141.
```

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

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 defaul 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.

You can detect multiple concurrent sessions for the same user with the sessionActiveTable in the Ascend MIB.

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 MIB (Management Information Base).

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 parameters for protecting access to SNMP 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. To assign 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. You can use the original SNMPv1 definition of the community string (a string of octets that is compared to a similar string in the receiving SNMP entity). If the string in the packet received exactly matches a community string in the receiving entity, then the packet is considered "authentic".

The defaults for SNMP v1 (without authentication) are:

Ethernet > Mod Config > SNMP Options > Read Comm=public

Ethernet > Mod Config > SNMP Options > R/W Comm=write

You use a new version of the Read/Write community string if you wish to use SNMP authentication, with the format:

Ethernet > Mod_config > SNMP Options > R/W Comm=write|secretkey

This causes the Ascend unit to require SNMP SET REQUEST packets to be authenticated, using "secretkey" as the shared (but not transmitted) secret.

– ***`name`*** is the name you want to assign to the read-write community name.

– ***`secretkey`*** is the alphanumeric key used for authentication.

– a vertical bar separates the ***`name`*** from the ***`secretkey`***.

The data, time, and hash values are transmitted with the packet. This allows the management station and Ascend unit to verify that the packet has been produced by an authorized system, and that the packet not been altered or significantly delayed in transmission.

The MD5 hash guarantees a high likelihood that only a system that knows the secret authentication key generated the packet, while the time variables guarantee a high likelihood that an attacker did not collect an authenticated packet and transmit it at a time of its own choosing, after a significant delay.

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, so it does not provide any real security.

4 If you are using authenticated SNMP, configure the SNMP management station to communicate with a MAX using authenticated SNMP. See “Configuring the SNMP manager to use SNMP authentication.”

5 Save your changes.

Configuring the SNMP manager to use SNMP authentication

To communicate with an Ascend unit that has been configured to use authenticated SNMP, an SNMP management station must construct an SNMP packet using the new format for the Read/Write community string, including the secret key:

name|secretkey

If the Ascend unit has been configured to use authenticated SNMP, it will not accept packets from an SNMP management station using the string format without the pipe/vertical bar.

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) or if Combinet encapsulation is in use (Encaps=COMB).

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 specify 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

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 Sec Domain Name=xyz.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.

The MAX searches for the DNS Server(s) in the Domain Name parameter first, and then in the domain specified in the Sec Domain Name parameter.

3 To specify a secondary domain name to use for lookups, set the Sec Domain Name parameter.

The MAX searches for the DNS Server(s) first in the domain specified by the Domain Name parameter, and then in the domain specified in the Sec. Domain Name parameter.

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.
8. 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. Set the Client Pri DNS parameter.
9. MAXhe Client Sec DNS parameter.

   MAXMAXThe 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.

    – 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.
5. MAXSet the Client Sec DNS parameter.

Disabling remote management access

To prevent an operator from accessing the MAX from a remote Ascend unit using AIM or MP+ remote management, set 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 Exit and 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 setting Ethernet > Mod Config > Telnet PW.

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 “Restricting Telnet, raw TCP, and Rlogin access to the terminal server” on page 3-28 for additional information about restricting Telnet in the terminal server interface.

3 Save your changes.

Note: The Telnet password does not automatically grant access to the Immediate Modem feature, which allows a user to dial out through the MAX modems without going through the terminal server interface. See “Restricting access to the Immediate Modem feature” on page 6-7 for more information.

Understanding secure Dynamic Bandwidth Allocation

DBA (Dynamic Bandwidth Allocation) 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, or MS-CHAP for PPP, MP, and MP+ calls” on page 3-18. 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 5-6. 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 “Requesting PAP-TOKEN-CHAP authentication” on page 5-8. 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