MAX 2000 Series Network Configuration Guide

Ascend Communications, Inc.
Part Number: 7820-0631-001
For software version 7.0.0

Ascend Customer Service

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

Obtaining technical assistance

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

Enabling Ascend to assist you

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

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

Calling Ascend from within the United States

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

Priority Technical Assistance

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

Ascend Advantage Pak

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

Other telephone numbers

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

Calling Ascend from outside the United States

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

Telephone outside the United States	(510) 769-8027
Asia Pacific (except Japan)	(+61) 3 9656 7000
Austria/Germany/Switzerland	(+33) 492 96 5672
Benelux	(+33) 492 96 5674
France	(+33) 492 96 5673
Italy	(+33) 492 96 5676
Japan	(+81) 3 5325 7397
Middle East/Africa	(+33) 492 96 5679
Scandinavia	(+33) 492 96 5677
Spain/Portugal	(+33) 492 96 5675
UK	(+33) 492 96 5671

For the Asia Pacific Region, you can find additional support resources at `http://apac.ascend.com/contacts.html`.

Obtaining assistance through correspondence

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

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

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

Finding information and software on the Internet

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

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

Contents

Figures

Tables

About This Guide

How to use this guide

This guide explains how to configure and use the MAX as an Internet Service Provider (ISP) or telecommuting hub. Following is a chapter-by-chapter description of the topics:

- Chapter 1, “Getting Acquainted with the MAX,” lists the MAX features as they apply to an ISP or telecommuting hub application.
- Chapter 2, “Configuring the MAX for WAN Access,” shows you how to configure the MAX for various types of WAN connectivity.
- Chapter 3, “Configuring WAN Links,” explains how to set up your connections for PPP, MP+, Combinet, or Frame Relay protocols.
- Chapter 4, “Configuring Frame Relay,” explains how to set up your connections for Frame Relay.
- Chapter 5, “AppleTalk Routing” explains how to set up your connections for AppleTalk.
- Chapter 6, “Configuring X.25,” describes X.25 support on the MAX.
- Chapter 7, “Defining Static Filters,” explains how filters work and how to define filters.
- Chapter 8, “Configuring Packet Bridging,” explains how to configure the MAX for bridging.
- Chapter 9, “Configuring IPX Routing,” explains how to configure the MAX for IPX routing.
- Chapter 10, “Configuring IP Routing,” explains how to configure the MAX for IP routing.
- Chapter 11, “Configuring OSPF Routing,” explains this Internet routing protocol.
- Chapter 12, “Setting Up IP Multicast Forwarding,” explains how to configure multicast forwarding.
- Chapter 13, “Setting Up Virtual Private Networks,” explains show to set up VPNs through ATMP and PPTP protocols.

This guide also includes an index.

What you should know

This guide is for the person who configures and maintains the MAX. To configure the MAX, you need to understand the following:

- Wide area network (WAN) concepts
- Local area network (LAN) concepts, if applicable

Documentation conventions

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

Note: In a menu-item path, include a space before and after each ">" character.

MAX 2000 Series documentation set

The MAX 2000 Series documentation set consists of the following manuals:

- *MAX 2000 Series Administration Guide*
- *MAX 2000 Series Hardware Installation Guide*
- *MAX 2000 Series Network Configuration Guide (this guide)*
- *MAX Glossary*
- *MAX Reference Guide*
- *MAX Security Supplement*
- *MAX RADIUS Configuration Guide*

Related publications

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

Here are some related publications that you may find useful:

- *The Guide to T1 Networking, William A. Flanagan*
- *Data Link Protocols, Uyless Black*
- *The Basics Book of ISDN, Motorola University Press*
- *ISDN, Gary C. Kessler*
- *TCP/IP Illustrated, W. Richard Stevens*
- *Firewalls and Internet Security, William R. Cheswick and Steven M. Bellovin*

Getting Acquainted with the MAX

1

Using the MAX as an ISP or telecommuting hub

The MAX is a high-performance WAN router that concentrates many incoming connections onto a corporate backbone or another network, such as the Internet or a Frame Relay network. The connections are usually switched, but the MAX also supports leased connections for those users whose connection times justify a permanent virtual connection to the backbone network.

A switched connection is a temporary link between devices, established only for the duration of a call. When you use bandwidth-on-demand, the MAX adds and subtracts bandwidth as necessary, keeping connection costs as low as possible.

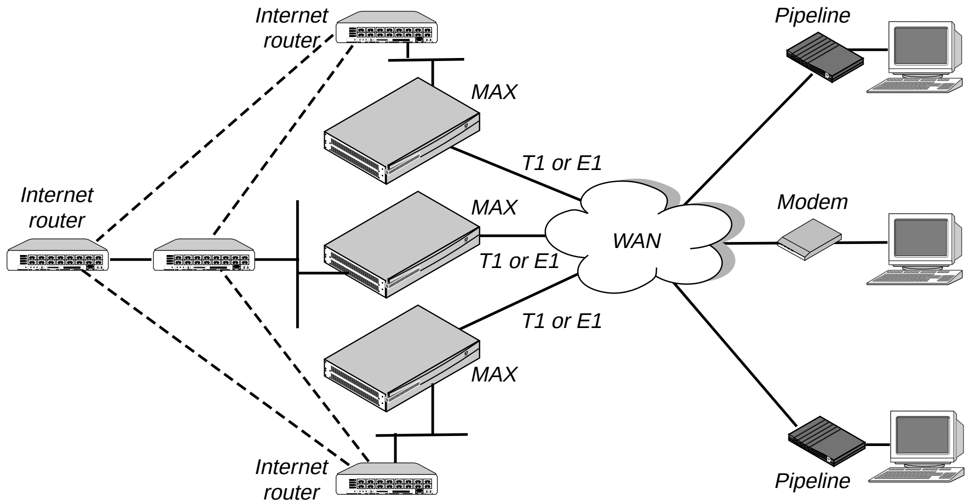
The MAX most commonly serves as an Internet Service Provider (ISP) hub, managing many switched IP connections to the Internet, or as a telecommuting hub, providing high-speed connections between a corporate backbone and remote locations. MAX configuration options provide the flexibility you need to optimize your installation. Management features include a comprehensive set of control and monitoring functions and easy upgrades.

Using the MAX as an ISP hub

Individuals subscribe to an Internet Service Provider to get a TCP/IP connection to the Internet. Subscribers dial in to a local Point-of-Presence (POP), typically by means of an analog modem, an ISDN V.120 terminal adapter, or an ISDN router such as an Ascend Pipeline. If you use the MAX as an ISP hub, configure it as an IP router, because it establishes the dial-in WAN connection with subscribers and routes their data streams to other Internet routers.

Figure 1-1 shows a typical ISP configuration with three POPs. Each POP has at least one MAX on an Ethernet LAN that also includes another Internet router, which could be, for example, an Ascend GRF 400 router.

Figure 1-1. Using the MAX as an ISP hub

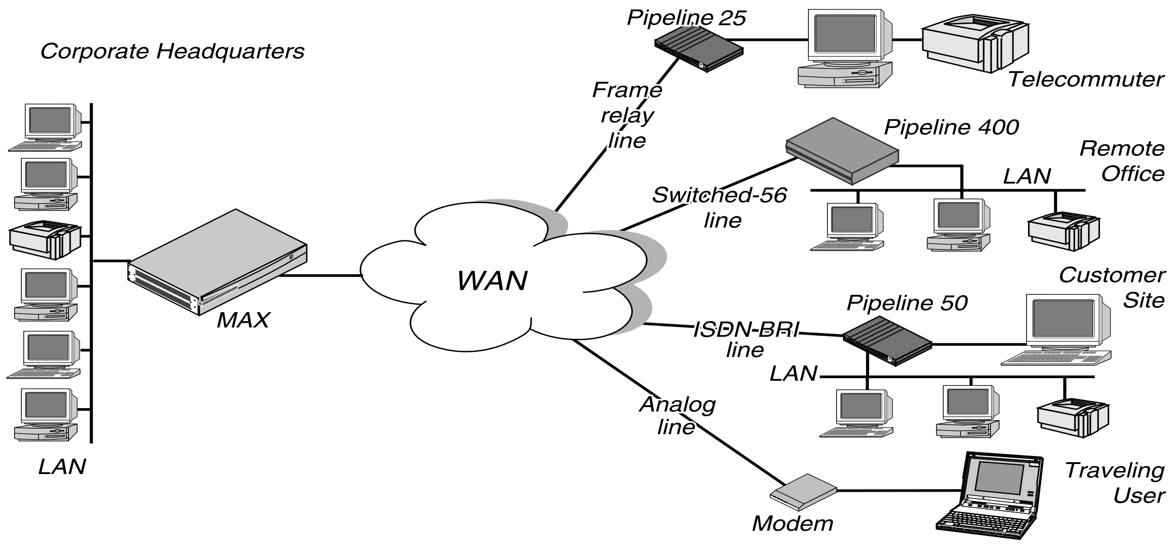


Typically, the MAX has T1 or E1 lines that use ISDN signaling to connect to the WAN and handle the incoming switched connections. To connect to Internet routers, the MAX most often uses the local Ethernet, but the connections between Internet routers can be any high bandwidth connection, such as Frame Relay, nailed T1, nailed E1, HSSI, FDDI, or Sonet. Large ISPs often support redundant MAX units and Internet routers on each Ethernet segment.

Using the MAX as a telecommuting hub

Telecommuters are typically at branch offices, at home, at customer sites, at vendor sites, or on the road. The MAX enables these remote users to access the corporate backbone just as though they were connected locally. The backbone might be a NetWare LAN, an IP network, or a multiprotocol network. Figure 1-2 shows an example in which home users, remote offices, and customer sites can access the backbone network.

Figure 1-2. Using the MAX as a telecommuting hub



In this sample network, a telecommuter in a home office uses a Pipeline 25 and Frame Relay to log into the corporate LAN. Users on a remote office LAN access the backbone via a Pipeline 400 with a Switched-56 connection. A customer can access selected corporate network resources by means of a Pipeline 50 with an ISDN BRI connection. A mobile user with an analog modem can dial into the backbone, provided that the MAX has a digital modem card installed.

Notice that each user can access the MAX through a different type of line. While one user might access the MAX by using the switched services on an ISDN BRI or Switched-56 line another might require a nailed 56K Frame Relay circuit.

Overview of MAX configuration

Before you configure the MAX, you should create a network diagram. Configuration tasks generally consist of:

- Configuring the lines, channels, and ports, and how calls are routed between them
- Configuring wide area network connections and security
- Configuring the MAX as a Frame Relay or X.25 concentrator
- Configuring routing and bridging across the WAN
- Configuring Internet services, such as multicast, OSPF, and virtual private networks

Creating a network diagram

Ascend strongly recommends that, after you have read these introductory sections, you diagram your network and refer to the diagram while configuring the MAX. Creating a comprehensive network diagram helps prevent problems during installation and configuration, and can help in troubleshooting any problems later.

Configuring lines, slots, and ports for WAN access

The MAX has one built-in T1 or E1 line and a Leased T1/E1 with optional CSU, as well as a a V.35 serial port (8 Mbps). The T1 or E1 line has a wide variety of configuration options, including whether or not you use ISDN signaling, the type of physical-layer framing, cable length, and telco options. The way you configure the line affects how much bandwidth will be available and whether you can direct outbound calls to use specific channels. The way you configure channels depends on your connectivity needs.

Use the serial WAN port for a leased high-speed connection to a Frame Relay switch or to another WAN router. The port itself requires little configuration. A Frame Relay or Connection profile specifies most of the required information.

You can add expansion modules to support additional bandwidth (BRI lines), serial host ports modules to support videoconferencing, and digital modems to support analog modem connections over digital lines. The lines and ports on the modules (cards) have their own configuration requirements, including the assignment of phone numbers and information about routing calls.

Once you enable the lines, slots, and ports for WAN access, you need to configure the way in which outbound calls are routed to them (for dial-out access to the WAN) and the way in which inbound calls are routed from them to other destinations (such as the local network).

Configuring WAN connections and security

When the MAX receives packets that require establishment of a particular WAN connection, it automatically dials the connection. Software at both ends of the connection encapsulates each packet before sending it out over the phone lines. Each type of encapsulation supports its own set of options, which can be configured on a per-connection basis to enable the MAX to interact with a wide range of software and devices.

After a connection’s link encapsulation method has been negotiated, the MAX typically uses a password to authenticate the call. For detailed information about authentication and authorization, see the *MAX Security Supplement*. Following are some of the connection security features the MAX supports:

Feature	Description
Authentication protocols	For PPP connections, the MAX supports both Password Authentication Protocol (PAP) and Challenge-Handshake Authentication Protocol (CHAP). CHAP is more secure than PAP, and is preferred if both sides of the connection support it.
Callback security	You can have the MAX call back any user dialing into it, thus ensuring that the connection is made with a known location.
Caller-ID and called-number authentication	You can restrict who can access the MAX, by verifying the caller-ID before answering the call. You can also use the called number to authenticate and direct the call.
Authentication servers	You can offload the authentication responsibility to a RADIUS or TACACS server on the local network.

Feature	Description
Security card authentication	The MAX supports hand-held personal security cards, such as those provided by Enigma Logic and Security Dynamics. These cards provide users with a password that changes frequently, usually many times a day. Support for dynamic passwords requires the use of a RADIUS server that has access to an authentication server, such as an Enigma Logic SafeWord AS or Security Dynamics ACE authentication server.
Terminal-server	After a dial-in user has passed the initial connection security, you ca demand another password for access to the MAX terminal services. Within the terminal server, you can restrict commands that are accessible to users, or prevent them from executing any command other than Telnet.
Filters and firewalls	Packet-level security mechanisms can provide a very high level of network security.

Concentrating Frame Relay connections

The MAX provides extensive support for Frame Relay. Using a T1 or E1 line or serial WAN port for a nailed connection to a switch, it can function as a network-to-network interface (NNI) switch, a data communications equipment (DCE) unit responding to users, or as a data terminal equipment (DTE) unit requesting services from a switch.

Enabling X.25 terminal connections

X.25 is a precursor to Frame Relay and is generally considered less efficient. However, many sites use it to transmit information between users across the WAN. It accommodates both high-volume data transfers and interactive use of host machines. The MAX can have one physical connection to an X.25 DCE at the other end of a T1, E1, or BRI line. To support interactive use, the connection must be nailed.

Configuring routing and bridging across the WAN

Routing and bridging configurations enable the MAX to forward packets between the local network and the WAN and also between WAN connections.

Enabling protocol-independent packet bridging

The MAX can operate as a link-level bridge, forwarding packets from Ethernet to a WAN connection (and vice versa) on the basis of the destination hardware address in each packet. Unlike a router, a bridge does not examine packets at the network layer. It simply forwards packets to another network segment if the address does not reside on the local segment.

Using IPX routing (NetWare 3.11 or newer)

The MAX can operate as an IPX router, linking remote NetWare LANs with the local NetWare LAN on Ethernet. IPX routing has its own set of concerns related to the client-server model and user logins. For example, users should remain logged in for some period even if the connection has been brought down to save connection costs.

IP routing

IP routing is the most widespread use of the MAX, and it has a wide variety of configurable options. IP routing is the required protocol for Internet-related services such as IP multicast support, OSPF, and cross-Internet tunneling for virtual private networks. Most sites create static IP routes to enable the MAX to reliably bring up a connection to certain destinations or to change global metrics or preferences settings.

Configuring Internet services

All Internet services and routing methods require that the MAX function as an IP router, so an IP routing configuration is a necessary precondition.

Multicast

The multicast backbone (MBONE) is a virtual network layered on top of the Internet to support IP multicast routing across point-to-point links. It is often used for transmitting audio and video on the Internet in realtime, because multicasting is a much cheaper and faster way to communicate the same information to multiple hosts.

OSPF routing

Open Shortest Path First (OSPF) is the next generation Internet routing protocol. The MAX can be configured to communicate with other OSPF routers within an autonomous system (AS). To enable this routing function, you must configure the OSPF options on the Ethernet interface and for each WAN connection that supports remote OSPF routers.

OSPF can import routes from RIP as well. You can control how these imported external routes are handled by adjusting systemwide routing options such as route preferences and ASE-type metrics.

Virtual private networks

Many sites use the Internet to connect corporate sites or to enable mobile nodes to log into a corporate backbone. Such virtual private networks use cross-Internet tunneling to maintain security or to enable the Internet to transport protocols that it would otherwise drop, such as IPX. To implement virtual private networks, the MAX supports both ATMP, which is an Ascend proprietary tunneling mechanism, and Point-to-Point Tunneling Protocol (PPTP).

ATMP enables the MAX to create and tear down a tunnel to another Ascend unit. In effect, the tunnel collapses the Internet cloud and provides a direct access to a home network. Packets received through the tunnel must be routed, so ATMP applies only to IP or IPX networks at this time.

A PPTP session occurs between the MAX and a Windows NT server over a special TCP control channel. Either end might initiate a PPTP session and open the TCP control channel. Note that opening a PPTP session does not mean that a call is active, it simply means that a call can be placed and received.

Management features

The terminal-server command line provides access to management features that are not available through the menus. The VT100 window does, however, provide status information. The MAX supports SNMP, remote management, serial port software upgrades, and Call Detail Reporting (CDR).

The MAX provides up to nine security levels to control the management and configuration functions that are accessible to users. For detailed information about security profiles, see the *Security Supplement* for your MAX. For more information on management features, see the *Administration Guide* for your MAX.

Using the terminal-server command line

To invoke the terminal server command-line interface, you must have administrative privileges. Once you have activated a Security profile that enables these privileges, you can invoke the command line by selecting Term Serv in the Sys Diag menu. To close the command line, use the Quit command at the command-line prompt. The command-line interface closes and the cursor returns to the VT100 menus. For detailed information on the terminal-server, see Chapter 2, "Configuring the MAX for WAN Access."

Using status windows to track WAN or Ethernet activity

The VT100 interface displays eight status windows to the right of the configuration menus. The windows provide a great deal of read-only information about what is currently happening in the MAX. If you want to focus on the activity of a particular slot card, you can change the default contents of the windows to show what is currently occurring in that slot.

Managing the MAX using SNMP

Many sites use Simple Network Management Protocol (SNMP) applications to obtain information about the MAX and make use of it to enhance security, set alarms for certain conditions, and perform simple configuration tasks.

The MAX supports the Ascend Enterprise MIB, MIB II, and some ancillary SNMP features. The MAX can send management information to an SNMP manager without being polled. SNMP security uses a community name sent with each request. The MAX supports two community names, one with read-only access, and the other with read/write access to the MIB.

Using remote management to configure far-end Ascend units

When you have an MP+ or AIM connection to another Ascend unit, you can use the management subchannel established by those protocols to control, configure, and obtain statistical and diagnostic information about that Ascend unit. Multi-level password security ensures that unauthorized personnel do not have access to remote management functions.

Flash RAM and software updates

Flash RAM technology enables you to perform software upgrades in the field without opening the unit or changing memory chips. You can upgrade the MAX through its serial port by accessing it either locally or through a dial-in modem. You cannot perform remote software upgrades over the WAN interface because of a conflict between running the WAN and reprogramming the software.

Call Detail Reporting (CDR)

Call Detail Reporting (CDR) is a feature that provides a database of information about each call, including date, time, duration, called number, calling number, call direction, service type, associated inverse multiplexing session, and port. Because the network carrier bills for bandwidth on an as-used basis, and bills each connection in an inverse multiplexed call separately, you can use the CDR feature to understand and manage bandwidth usage and the cost of each inverse multiplexed session.

You can arrange the information to create a wide variety of reports that can be based on individual call costs, inverse multiplexed WAN session costs, costs on an application-by-application basis, bandwidth usage patterns over specified time periods, and so on. With the resulting better understanding of your bandwidth usage patterns, you can make any necessary adjustments to the ratio of switched to nailed bandwidth between network sites.

MAX profiles

A profile is a group of related settings that appear on the VT100 interface. To navigate the interface, use the arrow keys or Control-key combinations as described in the *Hardware Installation Guide* for your MAX. When you first telnet to the VT100 interface, the Main Edit Menu typically appears:

```
Main Edit Menu
  >00-000 System
  10-000 Net/T1
  20-000 Host/Dual
  30-000 Empty
  40-000 Serial Port WAN
  50-000 Ethernet
```

The items in the Main Edit Menu open submenus, many of which have sub-menus. The 10-100 Net/T1 item, for example, represents the T1 slot on the MAX. (If your MAX has an E1 slot instead, the item name is 10-100 Net/E1.) By selecting this item, you open a submenu from which you can select line configuration or line diagnostics:

```
10-000 Net/T1
>10-100 Line Config
 10-200 Line Diag
```

If you select line configuration, a list of slot-configuration profiles appears:

```
10-100 Line Config
>10-1** Factory
 10-101
 10-102
 10-103
 10-104
```

Each of the slot-configuration profiles provides access to the same set of parameters. You can configure multiple profiles to create alternative configurations for the slot. If you select one of the profiles, a subprofile of three parameters and two submenus appears:

```
10-101
>Name=
 1st Line=Trunk
 2nd Line=Disabled
 Line 1...
 Line 2...
```

The two submenus (Line 1 and Line2, often referred to collectively as Line *N*) provide access to the parameters for configuring the first and second line, respectively, of the slot. For example, if you select Line 1, the following set of parameters appears:

```
10-101
 Line 1...
 >Sig Mode=Inband
  NFAS ID num=N/A
  Rob Ctl=Wink-Start
  Switch Type=N/A
  Framing Mode=D4
  Encoding=AMI
  FDL=N/A
  Length=N/A
  Buildout=0 dB
  Clock Source=Yes
  Collect DNIS/ANI=N/A
  Pbx Type=N/A
  Delete Digits=N/A
  Add Number=N/A
  Call-by-Call=N/A
```

In this manual, an instruction to access a parameter in the Line 1 profile is written as follows:

Net/T1 > Line Config > *slot profile* > *parameter name*

or, alternatively,

Net/T1 > Line Config > *any slot profile* > *parameter name*

In an example of the settings in a profile, levels of indentation represent the levels of nested subprofiles. For example, a Net/T1 > Line Config > *any slot profile* > Line *N* profile could be shown as follows:

```
Net/T1
  Line Config
    any slot profile
      Line N
        Sig Mode=Inband
          NFAS ID num=N/A
          Rob Ctl=Wink-Start
          Switch Type=N/A
          Framing Mode=D4
          Encoding=AMI
          FDL=N/A
          Length=N/A
          Buildout=0dB
          Clock Source=Yes
          Collect DNIS/ANI=N/A
          Pbx Type=N/A
          Delete Digit=N/A
          Add Number=N/A
         Call-by-Call=N/A
```

Obtaining privileges to use the menus

As explained in the *Hardware Installation Guide* for your MAX, privileges are often required for changing settings in the MAX menus. To activate a profile, for example, you need full privileges. Unless you have a personal profile that grants full privileges, activate the Full Access profile, as follows:

1. At the Main Edit Menu, press Ctrl-D.
   The Main Edit Menu's DO menu appears.
2. Select P (Password).
3. Press Enter or the Right-Arrow key.
   The Security Profile menu appears.
4. Select Full Access.
5. Press Enter or the Right-Arrow key.
   A password entry field appears.
6. Enter your password within the brackets.
7. Press Enter or the Right-Arrow key.
   If your password is accepted, you have Full Access privileges.
8. Press Enter.
   The Main Edit Menu reappears.

Activating a profile

After you have full privileges as described in the previous procedure, you can now make a profile (such as one of the slot-configuration profiles described on page 1-9) active. Proceed as follows:

1 Open the profile that you want to make current.

2 Press Ctrl-D.
The profile's DO menu appears.

3 Select L (Load).
The Load Profile menu appears.

4 Select 1 to load the profile.
`Profile loaded as current profile` appears.
The profile reappears.

Where to go next

When you have planned your network, you are ready to configure the MAX. The flexibility of the MAX and its ever-increasing number of configurations means there is no set order for configuration. You can perform configuration tasks in any order you want. Table 1-1 shows where to look for the information you need.

Table 1-1. Where to go next

To do this:	Go to this chapter or document:
Configure slots, lines, and ports	Chapter 2, "Configuring the MAX for WAN Access"
Configure WAN connections	Chapter 3, "Configuring WAN Links"
Set up Frame Relay	Chapter 4, "Configuring Frame Relay"
Set up X.25	Chapter 6, "Configuring X.25"
Set up packet bridging	Chapter 8, "Configuring Packet Bridging"
Set up IPX routing	Chapter 9, "Configuring IPX Routing"
Set up IP routing	Chapter 10, "Configuring IP Routing"
Set up OSPF routing	Chapter 11, "Configuring OSPF Routing"
Set up multicast forwarding	Chapter 12, "Setting Up IP Multicast Forwarding"
Set up virtual private networks	Chapter 13, "Setting Up Virtual Private Networks"

Table 1-1. Where to go next (continued)

To do this:	Go to this chapter or document:
Work with status windows	*MAX Reference Guide*
Write configuration scripts	*MAX 2000 Series Administration Guide*
Set up security	*MAX Security Supplement*
Set up RADIUS	*MAX RADIUS Configuration Guide*

Configuring the MAX for WAN Access

2

Introduction to WAN configuration

The MAX has a built-in T1 or E1 slot, a Leased T1 or E1 with optional CSU, and a V.35 serial port for WAN access. (You can use the Leased T1/E1 or the serial port at once, not both.) It also has two expansion slots, which can support cards for additional bandwidth (BRI lines), AIM-port modules for videoconferencing, and digital modems for analog modem connections over digital lines.

Menus and profiles

To configure the MAX, you set parameters in the VT100 menus. Many of the menus and submenus include profiles, which are groups of related parameters. (For a description of navigating the interface, see the *Hardware Installation Guide* for your MAX.)

Menu numbers

The numbers in the VT100 menus relate to slot numbers in the MAX unit, which correspond to actual expansion slots or *virtual* slots on the MAX unit's motherboard. Following are the slot assignments.

System slot

The system itself is assigned slot number 0 (menu 00-000). The System menu contains the following profiles and submenus that are related to systemwide configuration and maintenance:

```
00-000 System
   00-100 Sys Config
   00-200 Sys Diag
   00-300 Security
   00-400 Destinations
   00-500 Dial Plan
```

T1 or E1 slot

The built-in T1 or E1 line is slot 1 (menu 10-000). The T1 or E1 slot includes two lines. The menus for configuring and testing the lines are organized as follows:

```
10-000 Net/T1 (Net/E1)
   10-100 Line Config
   10-200 Line Diag
```

Expansion slots

The two expansion slots are slots 2 and 3 (menus 20-000 and 30-000). The actual expansion slots are numbered beginning on the left (2) to the right (3).

Serial WAN slot

The serial port is slot 4 (menu 40-000). It is used for the serial WAN connection or the Leased T1 or E1.

Ethernet slot

The Ethernet port slot 5 (menu 50-000). The Ethernet menu contains submenus and profiles related to the local network, routing and bridging, and WAN connections.

Phone number assignments

The MAX receives calls on phone numbers assigned to its T1 or E1 and (if applicable) Net BRI channels. In the MAX configuration, each phone number has a limit of 24 characters, which can include the following: 1234567890()[]!z-*#|. To assign the phone numbers you must understand add-on numbers, hunt-groups, and Service Profile Identifiers (SPIDs).

Add-on numbers

You build multichannel calls (MP, MP+, AIM, or BONDING) by specifying add-on numbers. A multichannel call begins as a single-channel connection to one phone number. The calling unit then requests additional phone numbers that it can dial to connect additional channels, and stores the add-on numbers it receives from the answering unit. To add channels to the call, the calling unit must integrate the add-on numbers with the phone number it dialed initially. Three parameters specify add-on numbers: Ch *N*#, PRI Num and Sec Num.

Typically, the phone numbers assigned to the channels share a group of leading (leftmost) digits. Enter only the unique digits identifying each phone number, as following:

- If the add-on number in the called unit is shorter than the phone number dialed by the calling unit, the MAX replaces only the rightmost digits.
  - For example, suppose you dial 777-3330 to reach channel 1 of line 1, and dial 777-3331 through 777-3348 to reach other channels (on the same line or a different line). In this case, set Ch1#=30, and set the Ch *N*# parameter for the other channels to 31, 32, and so forth.
- If the add-on number is longer than the phone number dialed, the MAX discards the extra digits. For example:
  - Ch1# = 510-655-1212
  - Dial# = 655-1212
  - Derived number for channel 1 = 655-1212
- If there is no add-on number, the derived number equals the dialed number. For example:
  - Ch1# = (null)
  - Dial# = 555-1213
  - derived number for channel 1 = 555-1213

The most common reason multichannel calls fail to connect beyond the initial connection is that the answering unit sends the calling unit add-on numbers it cannot use to dial the other channels. The group of channels that make a multichannel call is called a bundle. A 10-channel bundle in which each channel is 64Kbps, provides a 640 Kbps connection.

Note: AIM and BONDING call bundles should not span dial plans. If you are receiving AIM or BONDING calls and have multiple dial plans, set up each dial plan as a separate trunk group. This also prevents MP and MP+ call bundles from spanning dial plans.

For example, you have two PRI lines from different service providers. You set the Ch*N* Trnk Grp parameters for the first line to 9 and for the second line to 8. Also, enabling trunk groups on your MAX separates the two dial plans and prevents the formation of bundles with channels from both PRI lines.

Hunt groups

A hunt group is a group of channels that has the same phone number. When a call comes in on that number, the MAX uses the first available channel to which the number was assigned.

Because channels in a hunt group share a common phone number, the add-on numbers in the profile are the same.

Note: If all of a line's channels have the same add-on number, you can leave the phone number assignment blank.

SPIDS (for Net BRI lines)

The SPIDs assigned to a BRI line operating in multipoint mode are numbers used at the central switch to identify services provisioned for your ISDN line. Your carrier bases the SPIDs on the telephone numbers assigned to your BRI lines, and tells you the SPIDs when it installs the lines.

Note: Not all telephone companies include a suffix on their SPIDs. When receiving SPIDs from your telephone company, ask them to verify whether or not suffixes are included. The SPID formats described in the next sections have been agreed upon by most telephone companies.

For example, for an AT&T switch in multipoint mode, SPIDs have one of the following formats:

`01`*`nnnnnnn`*`0`

`01`*`nnnnnnn`*`00`

In the AT&T SPID formats, *nnnnnnn* is the 7-digit phone number (not including the area code). For example, if the phone number is 555-1212, the SPID is 0155512120 or 01555121200. For a Northern Telecom switch, SPIDs have one of the following formats:

`aaannnnnnnSS`

`aaannnnnnnSS``00`

In the Northern Telecom SPID formats, *aaannnnnnn* is the 10-digit phone number (including the area code). SS is an optional suffix. If specified it is a one or two-digit number differentiating the channels. For example, if the phone numbers are 212-555-1212 and 212-555-1213, the SPIDs might be:

`21255512121`

`21255512132`

or:

`212555121201`

`212555121302`

or one of the above formats followed by 00 (for example, 21255512130200).

How the MAX routes inbound and outbound calls

When the MAX receives a call on one of its phone numbers, it routes that call internally to one of its slots or ports. When a digital modem, AIM port, or a host on the local Ethernet port originates a dial-out connection, the MAX routes that call internally to an available WAN channel to place the call. The channel configuration of a WAN line determines how the channel routes inbound calls and places outbound calls. For details, see "Configuring call routing" on page 2-51.

Configuring T1 lines

A built-in T1 line contains 24 channels, each of which can support one single-channel connection. Depending on the signaling mode used on the line, all 24 channels are available for user data, or 23 channels are available for data and the 24th channel is reserved for signaling.

T1 line configuration parameters are in a Line Config profile, as shown in the following example:

```
Net/T1
   Line Config
     slot profile
        Name=mytelco
        1st Line=Trunk
        2nd Line=Trunk
        Line 1...
           Sig Mode=Inband
           NFAS ID num=N/A
           Rob Ctl=Wink-Start
           Switch Type=N/A
           Framing Mode=D4
           Front End=CSU
           Encoding=AMI
           FDL=N/A
           Length=1-333
           Buildout=N/A
           Clock Source=Yes
           Pbx Type=N/A
           Delete Digits=N/A
           Add Number=N/A
           Call-by-Call=N/A
           T1-PRI:PRI # Type=Unknown
           T1-PRI:NumPlanID=ISDN
           Ans #=N/A
           Ans Service=N/A
           Input Sample count=N/A
           Send Disc=0
           Ch 1=Switched
           Ch 1 #=12
           Ch 1 Slot=3
           Ch 1 Prt/Grp=1
           Ch 1 TrnkGrp=5
          Ch 2=Switched
```

The Ch *N* parameters are repeated for each channel in the line. (There are 23 channels if you use PRI signaling and 24 channels if you use robbed-bit.) For detailed information about each parameter, see the *MAX Reference Guide*.

In the slot menu, you can assign a name to the line configuration of the slot's two lines. You can configure several such slot profiles and activate a profile when it is needed. To activate a profile, see "Activating a profile" on page 1-11.

You can set Line 1 and Line 2 to trunk service (indicating a standard T1 interface with signaling information) or disabled. For Line 2, you can also specify D&I (Drop-and-Insert) service. Drop-and-Insert on Line 2 specifies that some of Line 1's channels transparently pass over to Line 2. A device (such as a PBX) connected to Line 2 assumes that it is connected to the WAN switch and is not aware that the channels actually pass through the MAX before going to the WAN.

Understanding the line interface parameters

This section provides background information about the T1 line interface parameters. For complete information, see the *MAX Reference Guide*.

Sig Mode

A T1 line's signaling mode (Sig Mode) can be one of the following:

- Inband, robbed-bit signaling—The MAX uses the Rob Ctrl parameter for the Call Control mechanism.
- ISDN signaling—Designate the 24th channel of the T1 line as the D channel.
- ISDN NFAS (Non-Facility Associated Signaling)—Enables two or more T1 lines to share a D channel. One of the lines must be configured as the primary D channel and one as the secondary (backup) D channel.
- PBX (Private Branch Exchange) T1 signaling—The second T1 line can receive calls placed on the first T1 line. The MAX emulates a WAN switch, and the PBX (or other device connected to the second T1 line) places and answers calls by using the Call Control mechanism.

NFAS ID Num

The NFAS ID Num value is a different interface ID for each NFAS line. In most cases, the default *1* for the first line and *2* for the second line are correct. If the carrier requires different NFAS interface IDs, type the numbers they specify.

Inband, robbed-bit call control mechanism

Rob Ctl is the call-control mechanism for robbed-bit signaling. When it is set to Wink-Start (the default), the switch can seize the trunk by going off hook. The local unit requires the switch to wait for a 200 msec wink before it seizes a trunk.

Switch Type

The Switch Type parameter specifies the network switch providing ISDN service on a T1/PRI line. The ISDN carrier supplies the setting, which can be one of the following:

- AT&T
- NTI (Northern Telecom)
- NI-2 (National ISDN-2)
- GloBanD
- Japan

Framing Mode and Encoding

The Framing Mode parameter specifies the physical layer frame format for the T1 line. The two possible settings are D4 or ESF. The D4 format, also known as the superframe format, consists of 12 consecutive frames separated by framing bits. The line may not use ISDN signaling with D4 framing. If it does, false framing and Yellow Alarm emulation can result. ESF specifies the extended superframe format, consisting of 24 consecutive frames separated by framing bits. The ISDN specification advises that you use ESF with ISDN D-channel signaling.

The Encoding parameter sets the layer-1 line encoding used for the physical links, which affects the way the digital signals on the line represent data. Your carrier can tell you which encoding to use. AMI (the default) specifies Alternate Mark Inversion encoding. B8ZS specifies Bipolar with 8-Zero Substitution. The None setting is identical to AMI, but without density enforcement.

Front End

Enable the internal CSU of any TR/PRI port by setting the Net/T1 > Line Config > *slot profile* > Line *N* > Front End parameter to CSU. If you use external CSUs, disable the MAX internal CSU by setting Front End to DSX.

FDL for monitoring line quality

The telephone company uses a facilities data link (FDL) protocol to monitor the quality and performance of T1 lines. If your carrier's maintenance devices require regular data-link reports and the line is not configured for D4 framing, you can specify the type of protocol (AT&T, ANSI, or Sprint) to use for the reports.

You cannot use FDL reporting on a line configured for D4 framing. However, you can obtain D4 and ESF performance statistics in the FDL Stats windows even if you do not choose an FDL protocol.

Length and Buildout

Assign a value to the Length parameter if you use an external Channel Service Unit (CSU) for a T1 port in the MAX. Choose the value that corresponds to the length of the line from the CSU to the MAX. The value should reflect the longest line length you expect (up to a maximum of 655 feet). A length of more than 655 feet requires that you enable the internal CSU.

The Buildout parameter specifies the amount of attentuation to apply to the MAX T1 transceiver's internal CSU. The amount, if any, depends on the length of the line between the MAX and the repeater from which it receives the signal. If the MAX is too close to a repeater, you might need to specify some attenuation to reduce the strength of the signal. Valid values are 0 dB (decibels) through 22.5 dB.

Clock Source

The Clock Source parameter determines whether the T1 line can be used as the master clock source for synchronous connections. In synchronous transmission, both the sending device and the receiving device must maintain synchronization in order to determine where one block of data ends and the next begins.

If two Ascend units connect to each other through a crossover cable (with optional T1 repeaters) between their network ports, you might need to disable this parameter on one of the units.

PBX parameters

The PBX Type parameter specifies the signaling to use with the PBX on line 2. When the parameter is set to Voice, the PBX that connects to line two views the MAX as a switch. A switch is the device that connects the calling party to the answering party. The MAX switches an incoming call on line 1 to line 2 only if it is a voice-service call.

To allow a PBX one line for dialing out through the MAX, specify a number of digits to delete from the dialed number (Delete Digits). The MAX deletes the digits, and then (if applicable) adds numbers to the beginning of a dialed number (Add Number). The MAX can add any digits required by the T1/PRI switch, or it can be used to specify a trunk group that is used in the current T1 profile.

Use the Answer # and Answer Service parameters to route calls to the device terminating the second T1 line when the second line's signal mode is PBX T1. The answer number is one of the MAX unit's phone numbers, and answer service is a data service type, such as voice. (For more information, see "Configuring call routing" on page 2-51.)

Note: When you use Answer Service to route all voice calls received on line 1 to a PBX on line 2, you can no longer receive modem calls on line 1. All voice calls received on the line route to the PBX, without exception.

Input Sample Count lets you specify 2 rather than the default of 1 sample for standard tone durations and other PBXs that use a nonstandard tone duration of less than 50ms. Using one sample set seems to work with most PBXs, in most cases, but using two samples is more accurate. Where the tone duration is long (more than 70ms), setting the Input Sample Count to 2 is recommended.

Call-by-Call

The Call-by-Call parameter specifies The service provider's call-by-call signaling value for routing calls from a local device to the network through the MAX. The values differ by service provider.

Understanding the channel configuration parameters

This section provides background information on the T1 channel configuration parameters. For complete information, see the *MAX Reference Guide*.

Specifying how the channel will be used

Each of the 24 channels of a T1 line can be configured for one of the following uses:

Use	Description
Switched (the default)	Supports switched connections. Can be robbed-bit or a B channel, depending on the line's signal mode.
Nailed	A clear-channel 64K circuit

Use	Description
D channel	Channel used for ISDN D-channel signaling. Assigned automatically to channel number 24 when ISDN signaling is in use.
NFAS-Prime	Primary D channel for two T1 lines that support NFAS signaling. Used as the D channel for both lines, unless it becomes unavailable.
NFAS-Second	Secondary D channel for two T1 lines that support NFAS signaling. Used as the secondary (backup) D channel.
Drop-and-Insert	Passes calls received on this channel through to the second line. The second line must use Drop-and-Insert service. The MAX directs calls on the Drop-and-Insert channel to a PBX on the second line.
Unused	Unavailable for use.
Phone number assignments	The phone number that the MAX dials to reach that channel.
Ch N #	Add-on number associated with each switched channel (as described in “Add-on numbers” on page 2-3.)

Associating the channel with a slot/port in the MAX

With the Ch *N* Slot and Ch *N* Prt/Grp parameters, you can assign a switched channel to a slot or slot/port combination for a digital modem, AIM port, or Ethernet. This configuration affects both inbound call routing and outbound calls. In effect, it reserves the channel for calls to and from the specified slot or port. (For details, see “Configuring call routing” on page 2-51.)

If the channel is nailed, Ch *N* Prt/Grp is a Group number. To make use of this nailed connection, the Group number is referenced in a Connection or Call profile.

Assigning the channel to a trunk group

You can assign trunk group numbers 4–9 to channels to make them available for outbound calls. For details, see “Routing outbound calls” on page 2-60.

Examples of T1 configurations

This section provides examples of configuring T1 lines for ISDN PRI services, robbed-bit signaling, and NFAS signaling. the examples do not include names for the slot profiles (which are in the menu that appears when you select Line Config), because you can assign any name. To apply the settings in a slot profile, however, you must activate the profile. See “Activating a profile” on page 1-11 for these procedures.

Enabling the internal CSU for a T1 port

To enable the internal CSU for a T1 port, proceed as follows:

1 Open the Net/T1 > Line Config > *any slot profile* > Line *N* menu.

2 Set Front End to CSU.
(To disable the internal CSU you would set Front End to DSX.)

3 Exit and save your change.

Configuring a line for ISDN PRI service

When configuring ISDN PRI service for your MAX units, you must configure ISDN signaling for the line. Optionally, you can also configure the MAX to send either ISDN code 16 (Normal call clearing) or code 17 (User busy) when the PRI switch servicing the MAX triggers the T310 timer.

Example of configuring ISDN signaling

This example applies to switched channels with ISDN signaling on a T1 line:

1 Open Net/T1 > Line Config > *any slot profile* > and set the 1st Line to Trunk:

```
Net/T1
   Line Config
     any slot profile
         Name=
         1st Line=Trunk
        2nd Line=Disabled
```

2 Open the Line 1 subprofile and set the signaling mode to ISDN:

```
      Line 1...
         Sig Mode=ISDN
```

3 Specify the framing and encoding values to ESF and B8ZS, respectively (for example):

```
         Framing Mode=ESF
         Encoding=B8ZS
```

4 Close the T1 profile.

Example of configuring Pre-T310 Timer

The ISDN Pre-T310 timer enables users calling into a MAX to get better clarification of call disconnects during the initial setup of the call. If a call is presented to the MAX, and there is an extended period of delay while the call is being set up (for example a lot of local Ethernet traffic slowing down RADIUS requests or DNS lookups) you might want your users to get a disconnect indication other than the generic Normal call clearing.

In compliance with CCITT Specification Q.931, the MAX sends a Call Proceeding message to the network switch for every call it accepts.

The network switch sets its T310 timer as it awaits further messages from the MAX. The switch tears down the call if the T310 timer expires. When this happens, the switch reports ISDN code 16 (Normal call clearing) to the calling device.

The ISDN Pre-T310 timer adds a MAX-specific timer which must be set to a time period less than that of the T310 timer on the switch. Then, after the MAX-specific timer expires but before the T310 timer expires, the MAX sends ISDN code 17 (User Busy) and clears the call.

Note: Only calls presented on T1/PRI lines support the Pre-T310 timer feature.

To configure the Pre-T310 timer:

1 Open the Net/T1 > Line Config > *slot profile* > Line *N* menu.

2 Set the Send Disc parameter to a value of from 0 to 60 seconds.

The parameter must be set to a value less than the T310 timer value, so that it expires (and the MAX sends its ISDN disconnect) before the T310 timer.

3. Open the Ethernet > Mod Config > Auth menu.
4. Set the Timeout Busy=Yes if you would like User Busy sent when the Send Disc timer expires. Set Timeout Busy=No if you would like Normal call clearing sent.

   Note: The Timeout Busy parameter replaces the CLID Timeout Busy parameter.

Overlap Receiving for the MAX

By adding the Overlap Receiving feature, the Ascend unit can gather the complete called-party number from network switch, enabling the usage of features such as called-number authentication.

Overlap Receiving affects the incoming-call establishment procedure at the Ascend unit. According to ITU's Q.931 specifications, the user can use either the en-bloc receiving procedure or the Overlap Receiving procedure to handle the incoming call. If en-bloc receiving is in use, the Setup message contains all the information required by the called user to process the call. If you enable the Overlap Receiving parameter, the received Setup message might contain incomplete called number information. After it receives the Setup Acknowledge message, the network sends the remainder of the call information (if any) in one or more Information messages.

Configuring robbed-bit signaling

The following configuration shows a T1 line using all switched channels and the default inband (*robbed-bit*) signaling mode. To configure a T1 line for robbed-bit:

1. Open Net/T1 > Line Config > *any slot profile* and set the 2nd Line to Trunk (for example):

```
Net/T1
   Line Config
      any slot profile
        Name=
        1st Line=Trunk
       2nd Line=Trunk
```

2. Open the Line 2 subprofile and set the signaling mode to Inband:

```
     Line 2...
        Sig Mode=Inband
```

3. Specify the robbed-bit call control mechanism:

```
        Rob Ctl=Wink-Start
```

4. Close the T1 profile.

Using NFAS signaling

When you configure two T1 lines for NFAS signaling, they share a D channel. Configure one line with a primary D channel, and the other with a secondary D channel. Use the secondary D channel only if the primary line goes down or if it receives a signal commanding a change to the other D channel.

Note: Both lines must reside in the same slot.

To configure two T1 lines for NFAS:

1 Open Net/T1 > Line Config > *any slot profile* and set both lines to Trunk service.

```
Net/T1
   Line Config
      any slot profile
        Name=
        1st Line=Trunk
       2nd Line=Trunk
```

2 Open the Line 1 subprofile and set the signaling mode to NFAS:

```
      Line 1...
         Sig Mode=ISDN_NFAS
```

3 Keep the default NFAS ID.

```
         NFAS ID num=1
```

4 Configure Channel 24 as the primary NFAS D channel:

```
         Ch 24=NFAS-Prime
```

5 Close the Line 1 subprofile.

6 Open the Line 2 subprofile and set the signaling mode to NFAS:

```
      Line 2...
         Sig Mode=ISDN_NFAS
```

7 Keep the default NFAS ID:

```
         NFAS ID num=2
```

8 Configure Channel 24 as the secondary NFAS D channel:

```
         Ch 24=NFAS-Second
```

9 Close the T1 profile.

Enabling a robbed-bit PBX with PRI access lines (PRI-to-T1 Conversion)

Apply this section if you have PRI lines from the WAN and need to convert to T1 signaling for support of T1 PBXs. In most cases, you cannot use this feature in combination with digital modems.

The following sample configuration uses line 1 to send and receive calls on the WAN and line 2 to handle a PBX for voice service. The MAX emulates a WAN switch, so the PBX on line 2 simulates connection to an AT&T or other carrier switch. For detailed information about each parameter, see the *MAX Reference Guide*.

Note: The PBX must use 2-state inband with DTMF signaling and must support Senderized (en bloc) digit transmission, because the MAX has a preset time limit on received dialing digits. In addition, the called-party number should be available from the switch; that is, you need Dialed Number Identification Service (DNIS) or called-party information element.

To configure a pair of T1 lines to support a PBX:

1 Open 20-000 Net/T1 > Line Config > *any slot profile*, and select a slot profile. That is, select a profile for the second of the two Net/T1 slots.

```
Net/T1
   Line Config
      Name=
```

```
1st Line=Trunk
2nd Line=Disabled
```

Note: For the MAX 2000 which has only one pair of T1 lines, these steps apply to the profile for lines 1 and 2 in slot 1 (the 10-100 menu).

Note: On the MAX 1600, PRI-to-T1 conversion is available only if you install the Net/T1 slot card, and these steps apply to the profile for those lines.

2 Set the 2nd Line parameter to Trunk:

```
2nd Line=Trunk
```

3 Open the Line 1 subprofile and set the Sig Mode parameter to ISDN:

```
Line 1...
   Sig Mode=ISDN
```

On the MAX 1600, this step applies to line #1 of the Net/T1 slot card.

Note: On the MAX 4000 and 1600, you can also set the first pair of T1 lines (slot 1) for ISDN (PRI) signaling. In that case they become available for outgoing calls from the PBX and can switch incoming calls to the PBX.

4 Close the Line 1 subprofile.

5 Open the Line 2 subprofile and set the Sig Mode parameter to PBX T1:

```
Line 2...
   Sig Mode=PBX T1
```

On the MAX 1600, this step applies to line #2 of the Net/T1 slot card.

6 Set the Rob Ctl parameter as required by the PBX. For example:

```
Line 2...
   Rob Ctl=Wink-Start
```

7 Set the T1-PRI:PRI # Type parameter as allowed by the provide of your PRI lines as appropriate for the calls placed by your PBX. For example:

```
Line 2...
   T1-PRI:PRI # Type=National
```

8 Set the T1-PRI:NumPlanID parameter as required by the provider of your PRI lines. For example:

```
Line 2...
   T1-PRI:NumPlanID=ISDN
```

9 The PBX Type parameter tells the MAX what type of service the PBX expects on its T1 line. In most installations the PBX expects voice-service calls with call progress tones. The Data setting does not supply call progress tones or information messages to the user.

```
Line 2...
   PBX Type=Voice
```

10 The Ans Service parameter tells the MAX whether to convert a call coming in on the PRI line(s) to robbed-bit T1 signaling or to answer the call and perform normal incoming call routing. Most installations select Voice:

```
Line 2...
   Ans Service=Voice
```

Note: If you set Ans Svc=Voice, the MAX converts incoming voice-service calls on PRI line(s) to T1 signaling on the outgoing line to the PBX. The MAX routes data-service calls according to the MAX unit's normal incoming call routing. The calls do not go to the PBX and are not converted.

Note: If you set Ans Svc=Voice, you cannot configure the MAX for both digital modem operation and PBX-T1 support, because the MAX switches all incoming voice service calls to the PBX and none ever reach the digital modems.

11 Most installations leave the Ans # parameter blank.

```
Line 2...
   Ans #=
```

12 Set the Delete Digits and Add Number parameters, which convert the phone number dialed at the PBX to an ISDN PRI format. For example:

```
Line 2...
   Delete Digits=2
  Add Number=923
```

13 Set the Call-by-Call parameter, which adds the appropriate ISDN PRI call-setup request for calls dialed out from the PBX. For example:

```
Line 2...
   Call-by-Call=2
```

14 Close the Line 2 subprofile.

15 Close the T1 profile.

16 If you have not already set the Modem:NumPlanID parameter in the System Profile (Sys Config menu), set it now. It determines the numbering plan on outgoing calls. It applies not only to calls the PBX places, but to all outgoing call the MAX places.

Note: On MAX models with multiple lines configured for ISDN (that is, PRI), outgoing calls from the PBX use the first available channel on any line configured for ISDN signaling. If you wish to select a PRI line for outgoing calls, the number dialed by the PBX must be prefaced by a dialing prefix set up in the Ch *N* Trnk Grp Line profile parameter, and you must enable trunk groups (by setting the System profile's Use Trunk Grps parameter to Yes).

Note: When the MAX forwards an incoming call to the PBX, it does not forward the called-party number.

Assigning bandwidth to a nailed link

A nailed link is up permanently. Both ends of the link must assign the same number of channels to the link. However, channel assignments do not have to match. For example, Channel 1 might be switched at the local end and nailed at the remote end. To designate certain channels for a nailed line:

1 Open Net/T1 > Line Config > *any slot profile* > Line 1.

```
Net/T1
   Line Config
     any slot profile
        Name=
        1st Line=Trunk
        2nd Line=Disabled
        Line 1...
```

2 Configure the nailed channels. For example, to assign channels 1–5 to the same nailed connection:

```
Ch 1=Nailed
Ch 1 Prt/Grp=3
Ch 2=Nailed
Ch 2 Prt/Grp=3
Ch 3=Nailed
Ch 3 Prt/Grp=3
Ch 4=Nailed
Ch 4 Prt/Grp=3
Ch 5=Nailed
Ch 5 Prt/Grp=3
```

3 Close the T1 profile.

Note: A Connection profile can use this permanent link by specifying the nailed channels' group number in the Group parameter. A Frame Relay profile uses a permanent nailed link by specifying the group number in its Nailed Grp parameter.

Performing T1 line diagnostics

The MAX provides the following T1 diagnostic commands:

```
Net/T1
   Line Diag
      Line LB1
      Line LB2
      Switch D Chan
      Clr Err1
      Clr Perf1
      Clr Err2
      Clr Perf2
```

You can use these commands to test the line configuration. For detailed information about each command, see the *MAX Reference Guide*.

Configuring E1 lines

Each built-in E1 line contains 32 channels, each of which can support one single-channel connection. Depending on the signaling mode used on the line, all 32 channels are available for user data, or 31 channels are available for data and the 32nd channel is reserved for signaling. E1 line configuration parameters are in the slot profiles listed in the menu that appears when you select Line Config, as shown in the following example:

```
Net/E1
   Line Config
     any slot profile
        Name=myPTT_line1
        1st Line=Trunk
        2nd Line=Trunk
        Back-to-Back=No
        Line 1...
           Sig Mode=DPNSS
           Switch Type=Net 5
           Framing Mode=G.703
           # Complete=N/A
           Grp B Signal=N/A
```

```
 Grp II Signal=N/A
 L3 End=X END
 L2 End=B END
 NL Value=64
 LoopAvoidance=7
 Clock Source=Yes
 Ch 1=Switched
 Ch 1 #=1212
 Ch 1 Slot=3
 Ch 1Prt/Grp=1
 Ch 1 TrnkGrp=5
Ch 2=Switched
```

Note: The Line *N* profile includes a set of Ch *N* parameters for each channel in the line (31 channels if PRI signaling is used, or 32 channels for robbed-bit signaling).

You can configure multiple slot profiles and assign each a different name. Then, you can apply a different configuration to the slot by activating a different slot profile. To activate a slot profile, see "Activating a profile" on page 1-11.

In a slot profile, you can set Line 1 and Line 2 to Trunk service (indicating a standard E1 interface with signaling information) or Disabled.

The ETSI series of standards does not include a specification for how a CPE unit disables a NET5 line. Therefore, if you disable an E1 line, the switch to which your MAX is connected does not take the line out of service when you save the profile. The MAX disables outgoing call requests for a disabled line, but the switch still delivers incoming calls to the MAX. If you need to disable incoming calls, contact your carrier.

Note: If you have not configured any CLID profiles, you can use a workaround instead of contacting the carrier. Set Ethernet > Answer > ID Auth to Required. The MAX then does not accept any incoming calls on *any* E1 line. The MAX does not answer the call (go off-hook), so the caller is not charged for the call.

For lines configured with a DPNSS switch type, you can make a test connection to another DPNSS unit, without using an intervening switch, by setting Back-to-Back to Yes.

Understanding the line interface parameters

This section provides background information about the E1 line interface parameters. For detailed information about each parameter, see the *MAX Reference Guide.*

E1 signaling mode

An E1 line's signaling mode (Sig Mode) can be None (leased) or one of the following:

- ISDN—ISDN signaling using the D channel. You must designate the 32nd channel of the E1 line as the D channel.
- DPNSS—The interface supports DPNSS or DASS 2 signaling.
- R2—R2 signaling.
- Metered—Metered R2 signaling protocol, used in Brazil and South Africa.
- Chinese—A version of the R2 signaling protocol, used in China.

- CLID processing for the Philippines uses an inband A-5 MFR2 register signal to initiate and proceed with CLID processing.)
- Argentina—A version of the R2 signaling protocol, used in Argentina. (CLID processing for Argentina uses an inband A-5 MFR2 register signal to initiate and proceed with CLID processing.)
- Brazil—A version of the R2 signaling protocol, used in Brazil. (CLID processing for Brazil uses an inband A-5 MFR2 register signal to initiate and proceed with CLID processing.)
- India—A version of the R2 signaling protocol, for use in India. (CLID processing for India uses an inband A-5 MFR2 register signal to initiate and proceed with CLID processing.)

Note: The default bandwidth for data calls across R2 lines is 64 Kbps, so set Ethernet > Connections > *any Connection profile* > Telco Options > Force 56 to Yes in any Connection profile that should use 56 kbps over R2 lines.

Switch type

The Switch Type parameter specifies the type of network switch the carrier uses for providing ISDN service on your E1/PRI line. Switch types for E1/PRI lines include:

- GloBanD—(Q.931W GloBanD data service.
- NI-1—National IDSN-1.
- Net 5—Euro ISDN services in Belgium, the Netherlands, Switzerland, Sweden, Denmark, and Singapore.
- Danish—Conforms to the Danish E1-TB91020, July 1991 specification. Is a variation of Net5 PRI E1.
- DASS 2—U.K. only.
- ISLX—DPNSS switch type.
- ISDX—DPNSS switch type.
- Mercury—DPNSS switch type.
- Australian—Australia only.
- French—VN3 ISDN PRI.
- German—1TR6.
- CAS—New Zealand.

Framing Mode

The physical layer of the E1 line uses G.703 framing, which is the standard framing mode used by most E1 ISDN and DASS 2 providers. Most E1 DPNSS providers in the U.K require 2Ds, which is a variant of G.703. If you select G.703, the MAX provides CRC-4 checking. If you select 2DS, it does not.

Complete

The # Complete parameter specifies are in the number received for an incoming call using R2 signaling. You can specify end-of-pulsing to indicate that the MAX should keep on receiving digits until the caller stops sending them, or you can specify a fixed number of digits (up to 10).

Group signaling parameters

Grp B Signal and Grp II Signal specify the group signal to send before answering a call.

Required settings for DPNSS or DASS 2 switches

- L3 End and L2 End—Specify CCITT Layer 2 and CCITT Layer 3, respectively.
- NL value—The default value specifies 64 transmissions.
- Loop avoidance—The default value is 7.

For more details, contact the carrier. These settings are not applicable for ISDN.

Clock Source

The Clock Source parameter determines whether the E1 line can be used as the master clock source for synchronous connections. In synchronous transmission, both the sending device and the receiving device must maintain synchronization in order to determine where one block of data ends and the next begins.

Understanding the channel configuration parameters

This section provides background information about the E1 channel configuration parameters. For complete information, see the *Network Configuration Guide* for your MAX.

Ch N

For each of the 32 channels of an E1 line, the Ch *N* parameter specifies how the channel is used. Select one of the following values.

- Switched—The default. Supports switched connections. Can be robbed-bit or a B channel, depending on the line's signal mode.
- Nailed—A clear-channel 64K circuit.
- D channel—The channel used for ISDN D-channel signaling. Assigned automatically to channel number 16 when ISDN signaling is in use.
- Unused—Unavailable for use.

Ch N #

The Ch *N* # parameter specifies the add-on number associated with each switched channel. For details, see "Add-on numbers" on page 2-3.

Ch N Slot and Ch N Port

In the Ch *N* Slot and Ch *N* Prt/Grp parameters, you can assign a switched channel to a slot or slot/port combination for a digital modem, AIM port, or Ethernet. This configuration affects both inbound call routing and outbound calls. In effect, it reserves the channel for calls to and from the specified slot or port. For details, see "Configuring call routing" on page 2-51.

If the channel is nailed, Ch *N* Prt/Grp is a Group number. To make use of the nailed connection, the Group number is referenced in a Connection or Call profile.

Ch N Trnk Grp

You can assign trunk group numbers 4–9 to channels to make them available for outbound calls. For details, see "Routing outbound calls" on page 2-60.

Examples of E1 configuration

This section provides some examples of configuring for E1 lines for ISDN signaling, for DPNSS signaling, and for nailed connections.

Using ISDN signaling

To configure an E1 PRI line for ISDN signaling in Belgium, the Netherlands, Switzerland, Sweden, Denmark, or Singapore:

1. Open Net/E1 > Line Config > *any slot profile* > Line 1 and specify ISDN signaling:

   ```
   Net/E1
      Line Config
        any slot profile
           Line 1...
              Sig Mode=ISDN
   ```

2. Set the Switch Type parameter to Net 5 (the standard used in these countries):

   ```
   Switch Type=Net 5
   ```

3. Specify G.703 framing (the standard used by most E1 ISDN providers):

   ```
   Framing Mode=G.703
   ```

   Note: If you select G.703, the MAX provides CRC-4 checking. If you select 2 DS, it does not.

4. Close the E1 profile.

Using DPNSS signaling

To configure the E1 line for DPNSS signaling:

1. Open Net/E1 > Line Config > *any slot profile* > Line 1.
2. Set the DPNSS signaling mode and compatible switch type. For example:

   ```
   Net/E1
      Line Config
         any slot profile
           Line 1...
              Sig Mode=DPNSS
             Switch Type=Mercury
   ```

   Mercury is a variant of DPNSS.

3. Set the framing mode. For example:

   ```
   Framing Mode=2DS
   ```

   Most E1 DPNSS providers in the U.K. require 2DS, which is a variant of G.703. If you select G.703, the MAX provides CRC-4 checking. If you select 2DS, it does not.

4 When you set the DPNSS signaling mode, the following parameters show the appropriate default value.

```
L3 End=X END
L2 End=B END
NL Value=64
LoopAvoidance=7
```

5 Close the E1 profile.

Setting up a nailed connection

The number of nailed channels must be the same at both ends of the connection but the channel assignments do not have to match. For example, if there are five nailed channels at the local end, there must be five nailed channels at the remote end but Channel 1 could be switched at the local end and nailed at the remote end.

Note: To use nailed channels, a Connection or Call profile references the group number specified by each channel's Prt/Grp parameter. A total of 64 nailed connections can be defined over nailed channels.

To configure nailed channels on Line 1 of either of the two E1 slots, open the Line 1 profile:

1 Open Net/E1 > Line Config > *any slot profile* > Line 1 (for example):

```
Net/E1
   Line Config
      any slot profile
        Name=
        1st Line=Trunk
        2nd Line=Disabled
        Line 1...
           Sig Mode=Inband
           NFAS ID num=N/A
          Rob Ctl=Wink-Start
```

2 Scroll to the Ch *N* parameters, and configure the nailed channels. For example, to assign channels 1–5 to the same nailed connection:

```
Ch 1=Nailed
Ch 1 Prt/Grp=3
Ch 2=Nailed
Ch 2 Prt/Grp=3
Ch 3=Nailed
Ch 3 Prt/Grp=3
Ch 4=Nailed
Ch 4 Prt/Grp=3
Ch 5=Nailed
Ch 5 Prt/Grp=3
```

3 Close the E1 profile.

Performing E1 line diagnostics

The MAX provides the following E1 diagnostic commands:

```
Net/E1
   Line Diag
      Line LB1
      Line LB2
```

You can use these commands to test the line configuration. For detailed information about each parameter, see the *MAX Reference Guide.*

ISDN call information

If the E1 PRI line switch type is German 1TR6 or Japan NTT, you can display information about ISDN calls by invoking the terminal-server command line and entering the Show Calls command. For example:

```
ascend% show calls
```

The command displays statistics about current calls. For example:

```
Call ID  Called Party ID Calling Party ID InOctets OutOctets

3        5104563434      4191234567        0        0
4        4197654321      5108888888        888888   99999
```

The Call ID column contains an index number specific to the call.

Called Party ID and Calling Party ID show the telephone number of the answering device and calling device, respectively.

InOctets and OutOctets show the number of bytes received by the answering device and transmitted by the calling device, respectively.

Note: When an ISDN call disconnects from either a German 1TR6 switch or a Japan NTT switch, the switch sends call billing information to the call originator as part of the call tear-down process. This information is written to the eventCallCharge (eventEntry 17) SNMP object in the Ascend Enterprise MIB events group (10). An SNMP manager can then read this object to determine the cost of the call. The eventCallCharge object is a read-only integer and is applicable only if eventType is callCleared (3). Otherwise, 0 is returned.

Configuring the serial WAN port

The MAX has a built-in V.35 serial WAN DB-44 port. A serial WAN port provides a V.35/RS-449 WAN interface that typically connects to a Frame Relay switch. The clock speed received from the link determines the serial WAN data rate. The maximum acceptable clock is 8 Mbps. The clock speed at the serial WAN port has no effect on the bandwidth of other WAN interfaces in the MAX.

Serial WAN configuration includes the following parameters (shown with sample settings):

```
Serial WAN
   Mod Config
      Module Name=serial
      Nailed Grp=3
      Activation=Static
```

Understanding the serial WAN parameters

This section provides some background information about the serial WAN configuration. For detailed information about each parameter, see the *MAX Reference Guide*.

Nailed Grp

The Nailed Grp parameter assigns a number that can be referenced as the Group in a Connection profile as the Nailed Grp in a Frame Relay profile. If Group is specified in a Connection profile, the MAX bridges or routes packets to another unit across that nailed connection. If a Frame Relay profile references the parameters, the MAX has a nailed connection to a Frame Relay switch, and the DLCI number in each frame determines which frames the MAX sends over the link.

The number you assign must be unique in the MAX configuration. Do not use a group number that is already in use for a nailed connection on another interface.

Activation

The Activation parameter tells the MAX which signals control the data flow through the serial WAN port. The DCE that connects to the serial WAN port (for example, a Frame Relay switch) determines how to set the value. The Clear To Send (CTS) signal handles flow control.

Example serial WAN configuration

To configure the serial WAN interface to connect to a Frame Relay switch that uses Static data flow:

1 Open Serial WAN > Mod Config.

2 Assign a module name and a group number. For example:

```
Serial WAN
   Mod Config
      Module Name=wan-serial
      Nailed Grp=3
```

3 Set the Activation parameter to Static:

```
      Activation=Static
```

4 Close the Serial WAN profile.

5 Configure a Frame Relay profile and specify the Nailed Grp number assigned to this port. For example:

```
Frame Relay
   Name=NNI
   Active=Yes
   Call Type=Nailed
   FR Type=NNI
   LinkUp=Yes
   Nailed Grp=3
   ...
```

For more information about Frame Relay, see Chapter 4, “Configuring Frame Relay.”

Configuring digital modems

A digital modem is a device that can communicate over a digital line (such as an ISDN line) with a station that uses a modem connected to an analog line. Incoming modem calls and incoming digital calls come over the same digital line to the MAX unit's integrated digital modem. The MAX can also make an outgoing call over a digital line to a modem on an analog line.

A digital modem accepts an incoming call as a Pulse Coded Modulation (PCM) encoded digital stream that contains a digitized version of the analog waveform sent by a caller attached to a modem. The digital modem also converts outgoing data to a PCM-encoded digital stream for transmission across the WAN to an analog modem.

Following are the digital-modem-configuration parameters for a V.34 modem slot card with eight digital modems:

```
V.34 Modem
   Mod Config
      Ans 1#=12
      Ans 2#=13
      Ans 3#=14
      Ans 4#=15
```

```
V.34 Modem
   Modem Diag
      ModemSlot=enable slot
      Modem #1=enable modem
      Modem #2=enable modem
      Modem #3=enable modem
      Modem #4=enable modem
      Modem #5=enable modem
      Modem #6=enable modem
      Modem #7=enable modem
      Modem #8=enable modem
```

If you have a V.32bis modem installed in your MAX, the interface displays `LAN Modem` instead of V.34 Modem. If you have a K56Flex modem installed, the interface displays `K56 Modem`. Also, there can be 8, 12, or 16 modems per modem slot card. The Modem Diag menu displays 8, 12, or 16 Modem #N parameters corresponding to the number of modems on the slot card.

For detailed information about each parameter, see the *MAX Reference Guide*.

56k Modem Numbering

K56Flex modem cards are not numbered sequentially. The numbering does not affect functionality.

8-MOD modem numbering

Modems in the 8-MOD modem card are numbered 0, 1, 2, 3, 6, 7, 10, 11.

For example, if you have an 8-MOD modem card in slot 3 in a MAX 2000, the Show Modems command in the terminal-server displays the following output:

```
ascend% show modems

slot:item   modem  status
3:0         1      idle
3:1         2      idle
3:2         3      idle
3:3         4      idle
3:6         5      idle
3:7         6      idle
3:10        7      idle
3:11        8      idle
```

12-MOD modem numbering

Modems in the 12-MOD K56Flex modem card are numbered 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 13

For example, if you have a 12-MOD K56Flex modem card in slot 2 in a MAX 2000, the Show Modems command in the terminal-server displays the following output:

```
ascend% show modems

slot:item   modem  status
2:0         1      idle
2:1         2      idle
2:2         3      idle
2:3         4      idle
2:4         5      idle
2:5         6      idle
2:6         7      idle
2:7         8      idle
2:8         9      idle
2:9        10      idle
2:12       11      idle
2:13       12      idle
```

Understanding the digital modem parameters

Asynchronous data calls initiated by analog modems requires digital-modem processing, so all incoming analog modem calls must be routed first to a digital modem. The Answer numbers are add-on numbers assigned to some of the MAX unit’s WAN lines as described in “Configuring call routing” on page 2-51).

After the digital modems process the call, they send it to the MAX unit’s terminal-server software. If it does not contain PPP encapsulation, it is handled as a login call that can be routed transparently to a Telnet host on the local network. PPP-encapsulated modem calls pass to the bridge/router as regular PPP connections.

For information about the terminal-server, see "Configuring terminal-server connections" on page 3-51.

Note: 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 these calls do not require digital-modem processing. For information about processing V.110 calls, see"Configuring V.110 modems" on page 2-26.

Sample configuration

To configure digital modems:

1 Open V.34 Modem > Mod Config (or V.42 Modem > Mod Config).

2 Specify the unique digits of the phone numbers to be routed to digital modems. For example:

```
V.34 Modem
   Mod Config
      Ans 1#=12
      Ans 2#=13
      Ans 3#=14
      Ans 4#=15
```

3 Close the Modem profile.

Quiescing digital modems and returning them to service

A digital modem that has been temporarily disabled without disrupting existing connections is *quiesced*. When an active call disconnects, that modem is added to the disabled modem list and is not available for use. If all modems are on the disabled list, incoming callers receive a busy signal until the modems have been restored for service. When you re-enable a quiesced modem, a delay of up to 20 seconds might occur before the modem becomes available for service.

Note: Booting the MAX restores all quiesced lines, slots, and ports to service.

For more information about the 1st Line and 2nd Line parameters, see the *MAX Reference Guide*.

Configuring V.110 modems

A V.110 card provides eight V.110 modems that each enable the MAX to communicate with an asynchronous device over synchronous digital lines. An async 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 async session (a terminal server session). For details, see the *MAX Reference Guide*.

The V.110 configuration parameters are:

```
V.110
   Mod Config
      Ans 1#=12
      Ans 2#=13
      Ans 3#=14
      Ans 4#=15
```

For detailed information about each parameter, see the *MAX Reference Guide*.

Understanding the V.110 modem parameters

Asynchronous data calls that use V.110 encapsulation require V.110 modem processing, so incoming calls using V.110 must be routed first to a V.110 modem. The Answer numbers are add-on numbers assigned to some of the MAX unit's WAN lines as described in "Configuring call routing" on page 2-51).

The V.110 modem processes the call and sends it to the MAX unit's terminal-server software. If the call does not contain PPP encapsulation, it is handled as a login call that can be routed transparently to a Telnet host on the local network. PPP-encapsulated modem calls pass to the bridge/router as regular PPP connections.

Note: V.110 terminal adapters make asynchronous calls with CCITT V.110 encapsulation. These calls require V.110 modem processing.

Example of V.110 configuration

To configure V.110 modules:

1 Open V.110 > Mod Config.

2 Specify the dial-in phone numbers to be routed to V.110 as a terminal-server call.
For example:

```
V.110
   Mod Config
      Ans 1#=12
      Ans 2#=13
      Ans 3#=14
      Ans 4#=15
```

3 Close the V.110 profile.

Configuring Personal Handy Phone Service (PHS)

PHS is a mobile phone service currently offered in Japan only. In addition to voice communication, PHS offers data communication at a bandwidth of up to 32 Kbps, thus providing Internet access as well as voice service.

This feature is available through the addition of slot cards, each of which supports 16 concurrent PHS users. You can install up to two cards.

You need to enable the software functionality on the MAX through a hash code upgrade. When you have this hash code, the System Options menu displays `PHS Installed.` Otherwise, the System Options menu displays `PHS Not Installed`.

When you boot up the MAX with a PHS card in slot 4 and the software enabled, the following menu appears:

```
Main Edit Menu
   00-000 System
   10-000 Net/T1
   20-000 PIAFS-16
   30-000 Empty
   40-000 Serial WAN
   50-000 Ethernet
```

PIAFS stands for Personal Internet Access Forum Standard. PIAFS is a protocol designed to support connection negotiation, data transfers, and error correction. The -16 refers to the slot card's support of 16 concurrent PHS users.

Configuring ISDN BRI network cards

An ISDN Basic Rate Interface (BRI) network interface card has eight BRI lines. These lines can provide lower-cost connections to sites that do not require or have access to the higher-bandwidth T1 or E1 lines. There are two types of BRI network cards: the U and the S cards, functionally they are the same. The BRI network configuration involve the following parameters (shown with sample settings):

```
Net/BRI
   Line Config
      any slot profile
         Name=bri-net
         Switch Type=AT&T
         BRI Analog Encode=Mu-Law
         Line 1...
            Enabled=Yes
            Link Type=P_T_P
            B1 Usage=Switched
            B1 Slot=3
            B2 Prt/Grp=1
            B1 Trnk Grp=5
            B2 Usage=Switched
            B2 Slot=3
            B2 Prt/Grp=2
            B2 Trnk Grp=5
            Pri Num=555-1212
```

```
Pri SPID=01555121200
Sec Num=555-1213
Sec SPID=01555121300
```

For detailed information about each parameter, see the *MAX Reference Guide*.

Note: After you have configured the line, you might need to configure the card for outbound calls (as described in "Configuring the Net BRI line for outbound calls" on page 2-30).

Understanding the Net BRI parameters

This section provides some background information about the Net BRI parameters. For detailed information about each parameter, see the *MAX Reference Guide.*

Name

You can configure several profiles in a Net/BRI slot and activate a profile when it is needed. Each profile's name should be descriptive.

Switch Type

The Switch Type parameter specifies the central network switch that provides ISDN service to the MAX. (For details about supported switch types, see the *MAX Reference Guide*.)

BRI Analog Encode

If you are going to receive modem calls, you can set the BRI Analog Encode parameter to specify the encoding type.

Link Type

The Link Type parameter specifies whether the switch operates in point-to-point or multipoint mode. In point-to-point mode, MAX requires one phone number and no Service Profile Identifiers (SPIDs). In multipoint mode, the MAX requires two phone numbers and two SPIDs. All international switch types except DBP Telecom, and all U.S. switch types except AT&T 5ESS, operate in multipoint mode.

Using the BRI line for switched or nailed connections

Each BRI line has two B channels for user data and one D channel for signaling. The B1 and B2 Usage parameters specify how to use the B channels: Switched (the default), Nailed, or Unused (not available for use).

Associating the channel with a slot/port in the MAX

With the B *N* Slot and B *N* Prt/Grp parameters, you can assign a switched channel to a slot or slot/port combination for a digital modem, AIM port, or Ethernet. The slot or slot/port-combination configuration affects both inbound call routing and outbound calls. In effect, it reserves the channel for calls to and from the specified slot or port. For details, see "Configuring call routing" on page 2-51.

Note: You cannot control whether an incoming call rings on the first or second B channel, so set the the B1 Slot and B2 Slot parameters to identical values.

If the channel is nailed, B *N* Prt/Grp is a Group number. To make use of this nailed connection, the Group number is referenced in a Connection or Call profile.

Assigning the channel to a trunk group

You can assign trunk group numbers 4–9 to channels to make them available for outbound calls. You cannot combine PRI channels with BRI channels in the same trunk group. For details, see "Routing outbound calls" on page 2-60.

Phone number and Service Profile Identifier (SPID) assignments

The Pri Num parameter is the primary add-on number for the Net BRI line. If you configure the line for point-to-point service, this is the only number associated with the line.

The Sec Num parameter is the secondary add-on number for the Net BRI line. If you configure the line for point-to-point service, Sec Num is not applicable.

Pri SPID and Sec SPID are the SPIDs associated with the Primary and Secondary numbers, respectively. (For more information, see "SPIDS (for Net BRI lines)" on page 2-4.)

Examples of Net BRI configuration

This section provides examples of configuring Net BRI lines for incoming switched connections and for outbound calls.

Configuring incoming switched connections

The following example shows how to configure the BRI lines in multipoint mode with an NI-1 switch. Configure the lines for switched incoming connections.

1 Open Net/BRI > Line Config > *any slot profile*.

2 Assign a name to the profile and specify the carrier's switch type.

```
Net/BRI
   Line Config
     any slot profile
        Name=bri-net
        Switch Type=NI-1
       BRI Analog Encode=Mu-Law
```

3 Open Line 1, enable the line, and specify multipoint mode:

```
      Line 1...
         Enabled=Yes
         Link Type=Multi-P
```

4 Configure the B channels for switched usage and for routing to the local network. For example:

```
B1 Usage=Switched
B1 Slot=9
B2 Prt/Grp=0
B1 Trnk Grp=
B2 Usage=Switched
B2 Slot=9
B2 Prt/Grp=0
B2 Trnk Grp=
```

5 Specify the primary and secondary add-on numbers and their associated SPIDs. For example:

```
Pri Num=555-1212
Pri SPID=01555121200
Sec Num=555-1213
Sec SPID=01555121300
```

6 Close the Line 1 subprofile and proceed to configure the other 7 lines.

7 Close the Net BRI profile.

Configuring the Net BRI line for outbound calls

In the following example Net BRI configuration on a MAX 6000, the MAX has two T1 or E1 lines and has a Net BRI card installed in slot 5. To enable local users to use the BRI lines to initiate outbound connections, the MAX must be configured for trunk groups. To enable outbound calls on the Line 1 use trunk groups:

1 Open System > Sys Config and enable trunk groups systemwide:

```
System
   Sys Config
      Use Trunk Grps=Yes
```

2 Close the System profile.

3 Open Net/BRI > Line Config > *any slot profile* > Line 1:

```
Net/BRI
   Line Config
      any slot profile
         Name=bri-net
         Switch Type=NI-1
         BRI Analog Encode=Mu-Law
         Line 1...
             Sig Mode=Inband
             NFAS ID num=N/A
            Rob Ctl-Wink-Start
```

4 Assign both of the line's channels to trunk group 6 (for example):

```
B1 Trnk Grp=6
B2 Trnk Grp=6
```

5 Repeat this trunk group setting for the remaining BRI lines (Lines 2—8), so that all BRI lines are in trunk group 6.

6 Close the Net BRI profile.

To specify that outbound calls initiated by the MAX unit's bridge/router use trunk groups:

1 Open Ethernet > Mod Config > WAN Options and set the Dial Plan parameter to Trunk Grp:

```
Ethernet
   Mod Config
   Wan options...
      Dial Plan=Trunk Grp
```

2 Close the Ethernet profile.

To specify that a connection uses a BRI line:

1 Open the Connection profile.

2 Include the Net BRI trunk group number in the Dial # parameter. For example:

```
Ethernet
   Connections
      Dial #=6-555-1212
```

When the first digit of the Dial # is a trunk group number, the MAX uses the call using the channels in that trunk group to place the call.

3 Close the Connection profile.

Note: For a way to use Destination profiles to specify lines as backup channels if all WAN channels are busy, see "Routing outbound calls" on page 2-60. Instead of explicitly entering the dial number in the Connection profile, you can reference a Destination profile that can specify up to six different dial-out paths to a particular destination.

Displaying information about BRI calls

If the BRI line switch type is German 1TR6, you can display information about ISDN calls from the terminal-server command line by entering the Show Calls command. For example:

```
ascend% show calls
```

The command displays statistics about current calls. For example:

```
Call ID  Called Party ID Calling Party ID InOctets OutOctets
3        5104563434      4191234567        0        0
4        4197654321      5108888888        888888   99999
```

The Call ID column contains an index number specific to the call. Called Party ID and Calling Party ID show the telephone number of the answering device and calling device, respectively.

InOctets and OutOctets show the number of bytes received by the answering device and transmitted by the calling device, respectively.

Note: When an ISDN call disconnects in Germany, the ISDN switch sends call billing information to the call originator as part of the call tear-down process. For lines that use the German 1TR6 switch type, you can access ISDN call charges in the Ascend Enterprise MIB via SNMP management utilities.

Configuring Host BRI lines

The Host BRI module provides up to eight local ISDN BRI lines. The device terminating these local ISDN BRI lines might be a MAX (or any BRI device), on its own local Ethernet segment, or a Desktop video device with its own BRI line and built-in terminal adapter. When connected to a Host BRI line, the MAX appears to be an AT&T switch.

TEs on Host BRI lines can call each other, enabling local net-to-net BRI calls. These local calls never go out to the WAN. They make use of the BRI bandwidth internally. They can also send and receive calls from the WAN. To the actual WAN switch, the MAX appears as the call's endpoint. Routing to the Host BRI line is handled internally.

Host BRI configuration uses the following parameters (shown with sample settings).

```
Host BRI
   Line Config
      any slot profile
         Name=local
         Line 1...
            Enabled=Yes
            Dial Plan=Extended
            Ans 1#=1212
           Ans 2#=
```

For detailed information about each parameter, see the *MAX Reference Guide*.

Understanding the Host BRI parameters

This section provides some background information about the Host BRI configuration parameters. For complete information about the parameters, see the *MAX Reference Guide.*

Name

You can configure several profiles in a Host BRI slot and activate a profile when it is needed. Each profile's name should be descriptive.

Enabled

If you set the Enabled parameter to No, the line is not available for use.

Dial Plan

The Dial Plan parameter specifies how the device terminating a Host BRI line can send and receive calls. The options are to use the extended dial plan or use Trunk Groups. (For details about dial plans, see "Routing outbound calls" on page 2-60.)

Ans 1# and Ans 2#

Set Ans 1# and Ans 2# to route incoming WAN calls to the local BRI lines supplied by the Host BRI. For details, see "Configuring call routing" on page 2-51.

Examples of Host BRI configuration

This section provides examples of routing inbound calls to the terminating device, enabling the device to make outbound calls, and displaying information about BRI calls.

Routing inbound calls to the terminating device

With the configuration shown in this example, the MAX routes inbound WAN calls to the device terminating the Host BRI line. That device does not make outbound calls to the WAN. The inbound caller dials 555-1212 and connects to the terminating equipment that terminates BRI line 1.

1 Open Host/BRI > Line Config > *any slot profile* and assign a name to the profile:

```
Host/BRI
   Line Config
        any slot profile
           Name=local
```

2 Open the Line 1 subprofile, enable the line, and assign an answer number.

```
      Line 1...
         Enabled=Yes
         Dial Plan=Trunk Grp
         Ans 1#=1212
```

3 Close the Host BRI profile.

Enabling the device to make outbound calls

In this sample configuration, the terminating equipment on line 1 can make an outbound call using Trunk Group 5 and Dial Plan profile 2. With this configuration, the caller at the Host BRI terminating equipment dials 502-408-555-1212 and connects to the device whose telephone number is 408-555-1212 (Trunk group 5, Dial Plan 2). To implement the configurations:

1 Open System > Sys Config and enable trunk groups systemwide:

```
System
   Sys Config
      Use Trunk Grps=Yes
```

2 Close the System profile.

3 Open a Net/T1 (or Net/E1) profile and make sure that some of the line's channels are assigned to trunk group 5. Then, close the profile.

4 Open Dial Plan 02.

5 Specify the Inherit setting for the Data Service and PRI # Type parameters:

```
Dial Plan
   Name=Boston
   Call-by-Call=6
   Data Svc=Inherit
   PRI # Type=Inherit
```

For details, see "Routing outbound calls" on page 2-60.

6 Close the Dial Plan profile.

Configure the Host BRI module for outbound calls using the Dial Plan:

1 Open Host/BRI > Line Config > *any slot profile* > Line 1.
2 Set Dial Plan to Extended

```
Host/BRI
   Line Config
     any slot profile
        Name=local
        Line 1...
           Enabled=Yes
           Dial Plan=Extended
           Ans 1#=1212
          Ans 2#=
```

3 Close the Host BRI profile.

Configuring a local BRI-to-BRI call

With the configuration in this example, the terminating equipment on one Host BRI line can connect to the terminating equipment on another Host BRI by using a Dial Plan profile and going out on line 5, slot 4. To make the connection the caller dials:

```
345
```

This number, in a special 3-digit format references a Dial Plan profile. The first digit, called the dialing prefix, is 3. The second digit, 4, represents expansion slot 4, and the third digit is the host port on that card.

To enable outbound calls using trunk groups:

1 Open System > Sys Config and enable trunk groups systemwide:

```
System
   Sys Config
      Use Trunk Grps=Yes
```

2 Close the System profile.

To configure Line 3 for a local BRI-to-BRI call that is never seen by the telephone company:

1 Open Host/BRI > Line Config > *any slot profile* and specify the use of trunk groups.

```
Host/BRI
   Line Config
      any slot profile
         Line 3...
            Enabled=Yes
           Dial Plan=Trunk Grp
```

2 Close the Host BRI profile.

Configuring BRI/LT lines

The BRI/LT provides up to 8 BRI lines just like the Host BRI card. Typically, the BRI lines provide end-users with IDSL services. The end-user terminates their BRI line with an IDSL TA such as a Pipeline 85. BRI/LT configuration uses the following parameters (shown with sample settings):

```
BRI/LT
   Line Config
      any slot profile
         Name=idsl
         Line 1...
            Enabled=Yes
            Dial Plan=N/A
            B1 Usage=Switched
            B1 Slot=3
            B1 Prt/Grp=N/A
            B1 Trnk Grp=0
            B2 Usage=Switched
            B2 Slot=4
            B2 Prt/Grp=N/A
            B2 Trnk Grp=0
            Ans 1#=1212
           Ans 2#=
```

Understanding the BRI/LT parameters

This section provides some background information about the Net BRI parameters. For detailed information about each parameter, see the *MAX Reference Guide*.

Name

You can configure several profiles in a BRI/LT slot and activate a profile when it is needed. Each profile's name should be descriptive.

Enabled

If you set the Enabled parameter to No, the line is not available for use.

Dial Plan

The Dial Plan parameter specifies how the device terminating a BRI/LT line can send and receive calls. The options are to use the extended dial plan or use Trunk Groups. For details about dial plans, see "Routing outbound calls" on page 2-60.

B1 Usage and B2 Usage

Each BRI line has two B channels for user data and one D channel for signaling. The B1 and B2 Usage parameters specify how to use the B channels: Switched (the default), Nailed, or Unused (not available for use).

B N Slot and B N Prt/Grp

In the B *N* Slot and B *N* Prt/Grp parameters, you can assign a switched channel to a slot or slot/port combination for a digital modem, AIM port, or Ethernet. This configuration affects both inbound call routing and placing calls. In effect, it reserves the channel for calls to and from the specified slot or port. For details, see “Configuring call routing” on page 2-51.

Note: You cannot control whether an incoming call rings on the first or second B channel, so the B1 Slot and B2 Slot parameters should be set to identical values.

If the channel is nailed, B N Prt/Grp is a Group number, is referenced in a Connection or Call profile to make use of this nailed connection.

B N Trnk Grp

B *N* Trnk Grp allows you to configure trunk group dialing for outgoing calls on BRI lines provided by the BRI/LT card. Trunk group numbers 4–9 can be assigned to channels to make them available for outbound calls. You cannot combine PRI channels with BRI channels in the same trunk group. For details, see “Routing outbound calls” on page 2-60 for details.

Phone number and Service Profile Identifier (SPID) assignments

The Pri Num parameter specifies is the primary add-on number for the Net BRI line. If you configure the line for point-to-point service, it is the only number associated with the line.

Sec Num is the secondary add-on number for the Net BRI line. If you configure the line for point-to-point service, the parameter is not applicable.

Pri SPID and Sec SPID are the SPIDs associated with the Primary and Secondary numbers, respectively. For details, see “SPIDS (for Net BRI lines)” on page 2-4.

Ans 1# and Ans 2#

Set Ans 1# and Ans 2# to route incoming WAN calls to the local BRI lines supplied by the Host BRI. For details, see “Configuring call routing” on page 2-51.

Example of BRI/LT configuration

This section provides a sample configuration for a BRI/LT line. In this configuration, the MAX routes calls received on the phone number 555-1212 to the device terminating the BRI/LT line. To implement the configuration:

1 Open a BRI/LT > Line Config profile and assign a name to it. For example:

```
Host/BRI
   Line Config
      40-1** idsl
         Name=idsl
         Switch Type=
         Line 1 ...
         Line 2 ...
        Line 3....
```

2 Open the Line 1 subprofile, enable the line, and assign an answer number.

```
Line 1...
   Enabled=Yes
   Dial Plan=Trunk Grp
  Ans 1#=1212
```

3 Close the BRI/LT profile.

BRI/LT diagnostics

The MAX provides the following BRI/LT diagnostics:

```
BRI/LT
   Line Diag
      Line N...
         EOC Address=
         Line LoopBack
         Corrupt CRC
         UnCorrupt CRC
         Rq Corrupt CRC
         UnRq Corrupt CRC
         Clr NEBE
         Clr FEBE
        Sealing Current
```

For detailed information about each parameter, see the *MAX Reference Guide*.

Configuring IDSL voice-call support

Ascend's ISDN Digital Subscriber Line (IDSL) card supports incoming and outgoing voice calls. To support outgoing voice calls, the connected Terminal Equipment (TE) must send digits to the MAX by means of Q.931 en-bloc dialing (sends all dialed digits to the MAX in one block (the ISDN Call Setup message) rather than one digit at a time).

The MAX receives outgoing call requests from the attached ISDN TE and routes voice calls to the Public Switched Telephone Network (PSTN) over a T1 line or ISDN PRI line. The MAX receives incoming voice calls and to route the calls to TEs connected to IDSL cards uses Dialed Number Identification Service (DNIS).

Configuring the MAX IDSL card for outgoing voice calls

To configure the MAX to accept voice calls from ISDN TEs connected to the IDSL slot card and route them to the PSTN:

1 Open the System > Sys Config menu.

2 Set Use Trunk Groups to Yes.

3 Exit and save the System profile.

Use the following steps if you want voice call requests routed to a T1/PRI line:

1. Open the Net/T1 > Line Config > *any slot profile* Line *N* menu.
2. Set Ch *N* TrnkGrp to a value from 4 to 9.

   where *N* specifies the channel of the T1/PRI line you want to make available to the IDSL card.

   You must prepend this value to the phone number the TE dials. When the MAX receives a voice-call request from the TE, the MAX uses the trunk-group number to route the call to a T1 channel with a matching trunk-group number. If trunk groups are not used, the call request terminates at the MAX and is not forwarded to the PSTN.
3. Exit and save the Line *N* profile.

For details of configuring your T1/PRI line, see "Configuring T1 lines" on page 2-5.

Configuring the MAX IDSL card for incoming voice calls

You can use two different methods to configure the MAX to accept voice calls from the PSTN and route them to TEs connected to the IDSL slot cards.

To instruct the MAX to route calls to the IDSL card on the basis of the called number:

1. Open the BRI/LT > Line Config > *any slot profile* Line *N* menu.
2. Set Ans 1#, Ans 2#, or both, to the called number that is dialed to reach the end user's TE.

   The Central Office (CO) switch must support DNIS, because the MAX matches the DNIS number of the incoming call to numbers specified by Ans *N*# parameters.

To instruct the MAX to route calls to the IDSL card on the basis of the T1 channel on which the MAX receives calls:

1. Open the Net/T1 > Line Config > *any slot profile* Line *N* menu.
2. If a MAX should route calls received on a specific channel to the IDSL card, set the appropriate Ch *N* Slot parameter to the IDSL card's slot number.

   For example, if the MAX is to route all calls received on channel 1 to an IDSL card in slot 7, set Ch 1 Slot to seven.

Configuring a Pipeline for outgoing voice calls over IDSL

You can configure a Pipeline to support outgoing voice calls when they are connected to a MAX IDSL slot card for routing to the PSTN. If you use a TE other than a Pipeline, make sure it supports en-bloc dialing. To configure the Pipeline, proceed as follows:

1. Open the Ethernet > Answer > PPP Options menu.
2. Set Encaps to MPP.

   MPP supports data-call preemption as described in the Note on page 2-39.
3. Open the Configure menu.
4. Set Switch Type to IDSL.

   The IDSL selection is an AT&T 5ESS Point-to-Point configuration with en-bloc dialing support.

When you dial out from a phone connected to the analog port of the Pipeline or TE, you must prepend the Trunk group number (configured on the MAX) to the phone number you dial. This is similar to dialing from an ISDN Centrex System, where you must prepend an additional digit to get an outside line.

For example, if you configure the MAX with Trunk Group set to 9 and you are dialing 555-5555, dial 9-555-5555 to instruct the MAX to dial 555-5555 on the channels (T1 or PRI) configured with a Trunk Group setting of 9.

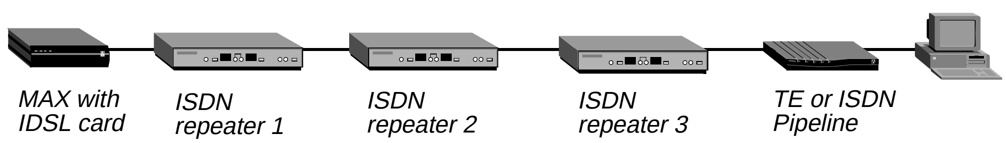
If you omit the trunk group, the call terminates at the MAX. It is not routed to the PSTN.

Note: Data call preemption is also supported with IDSL voice call support. If you use two channels for a single MPP data call, and dial your analog phone, the MAX reallocates one channel to the voice call, leaving one channel for the data call. When you hang up, the MAX reallocates the channel to the data call if throughput load warrants it.

Performing loopback diagnostics for IDSL

The MAX supports loopback tests from itself to any device on the IDSL connection. For example, you can loop back the signal from the IDSL card to the remote TE or Pipeline, or from the IDSL card to any intermediate repeater (see Figure 2-1).

Figure 2-1. IDSL connection with repeaters



In Figure 2-1, you could set up a loopback test from the MAX to any of the ISDN repeaters, or from the MAX all the way to the remote device at the end of the connection. This ability enables you to isolate trouble anywhere in the connection.

To configure a loopback test on the BRI lines provided by the IDSL slot card:

1 Select BRI/LT > Line Diag > *any slot profile* > Line *N*, where *N* is the number of the line you want to loopback.

2 Specify the EOC Address of the device that is the terminating point for the loopback test. Or set the EOC Address parameter to one of the following values:

- 0—Specifies the remote TA or MAX
- 1—Specifies the repeater nearest the MAX
- 7—Specifies all devices

3 Select Line Loopback and press Enter.

4 In the confirmation dialog that appears, select 1=Line *N* LB.

While the line loops back, normal data transfer is disrupted.

5 Press Escape to cancel the loopback.

For more details, see the *MAX Reference Guide.* In a local loopback test, data originating at the local site loops back to its originating port without going out over the WAN. It is as though a *data mirror* were held up to the data at the WAN interface, and the data reflected back to the originator. The WAN interface is the port on the MAX that connects to a WAN line.

New status messages

Select the BRI/LT > Line Diag > Line *N* > Sealing Current parameter to toggle loop sealing current between On and Off. If you toggle it on, the following message appears in the Edit window:

```
Message #242
  Loop Sealing Current
     now ON
```

If you toggle it off, the following message appears in the Edit window:

```
Message #243
  Loop Sealing Current
     now OFF
```

Configuring Host/6 (Host/Dual) AIM ports

You can connect a videoconferencing codec (coder/decoder) to an Ascend Inverse Multiplexing (AIM) port to communicate over a point-to-point link. An AIM *port* is the V.35, RS-499, or X.21 port on the MAX. Typically, inverse-multiplexed calls are between video codecs and other devices that might need high bandwidth serial data over the WAN.

An AIM port uses pins for controlling the data flow through the port. A device sends a signal through a pin and over the line to another device. The signal being sent determines the control-line state, for example, when a device sends a signal to another party, indicating that it has data to send, the control-line state is RTS (Request to Send). If the other device sends a signal to indicate that it is ready to receive data, the control-line state is DTR (Data Transmit Ready). The process of sending these synchronization signals between AIM ports is called *handshaking*.

Note: When you install an AIM-port card in the MAX, the AIM ports become the default route for inbound data calls, taking precedence over the bridge/router software. Make sure that your call-routing configuration accommodates calls defined for the local Ethernet. (See “Configuring call routing” on page 2-51.)

An AIM port requires three levels of configuration:

- The Port profile, to configure the AIM port itself
- The Host interface profile, to configure the interface to the codec
- The Call profile, to configure WAN connections on the port

Configuring the AIM port

The Port profile sets protocol and routing parameters for the port itself. The profile includes the following parameters (shown with sample settings):

```
Host/6 (or Host/Dual)
   PortN Menu
      Port Config
         Port Name=Port1
         Dial Plan=Trunk Grp
         Ans 1#=1212
```

```
Ans 2#=1213
Ans 3#=
Ans 4#=
Idle=None
Dial=Terminal
Answer=Auto
Clear=Terminal
Port Password=Ascend
Term Timing=No
RS-366 Esc=N/A
Early CD=None
DS0 Min Rst=Off
MAX DS0 Mins=N/A
MAX Call Mins=0
```

This section provides some background information about AIM-port configuration. For detailed information about each parameter, see the *MAX Reference Guide.*

Dial Plan

The Dial Plan parameter specifies how to place calls from this port. The choices are to use trunk groups or to use the extended dial plan. (For details, see "Routing outbound calls" on page 2-60.)

Ans N#

The Ans *N#* parameters specify add-on numbers assigned to a WAN line. Using them is one way of routing inbound calls received on those numbers to the AIM port. (For details, see "Configuring call routing" on page 2-51.)

Idle

The Idle parameter specifies the action the port takes when you turn on the power, or when no call is active. You can specify None (the port waits for a user to establish a call), or Call (the port dials the call).

Dial

The Dial parameter specifies how the codec dials an outbound call. The settings are as follows:

- Terminal—Dial manually by using DO Dial.
- DTR Active—Dial only if DTR is asserted at the port, indicating that the codec is ready to send data.
- RS-366 ext1—Dial through an RS-366 dialing service.
- RS-366 ext2—Same as RS-366 ext 1 but with different message protocols.
- V.25bis—Dial direct according to V.25 bis hardware handshaking.
- V.25bis-C —Same as V.25bis, but the CTS signal cannot change state during a call.
- X.21 ext1—Dial as described in the CCITT Blue Book Rec. X.21.
- X.21 ext2—Same as X.21 ext1, but with different message protocols.
- X.21 ext1-P—Same as X.21 ext1, but used for a PictureTel X.21 dialer.

Answer

The Answer parameter specifies how the codec answers a call. The settings are as follows:

- Terminal—Answer manually by using DO Answer.
- DTR Active—Answer only if DTR is asserted at the port, indicating that the codec is ready to receive data.
- DTR+Ring—Answer after one ring if DTR is asserted at the port, for codecs configured to answer manually.
- P-Tel Man—Same as DTR+Ring, but used for a Picture Tel codec configured to answer calls manually.
- V.25bis—Answer according to V.25 bis hardware handshaking.
- V.25bis-C—Same as V.25bis, but the CTS signal cannot change state during a call.
- X.21—Answer according to X.21 hardware handshaking.
- Auto—Answer every call automatically, regardless of the control-line state.
- None—Use the port for outgoing calls only.

Clear

The Clear parameter specifies how the control-line state determines when the MAX clears a call.

Port Password

The receiving unit compares the Port Password setting to compare the Call Password the caller sends upon initial connection of the first channel of an AIM or BONDING call. If the user's password matches the Port Password, the session establishes normally for the remainder of the call. If it does not match, the authenticating unit sends a message back to the originator and drops the session. The port-status screen indicates that the call failed authentication. If the Port profile does not specify a Port Password, the units connect without authentication, even though the originating unit might have sent a password.

Note that the MAX only authenticates AIM and BONDING calls. The MAX does not authenticate dual-port calls. (See "This section provides some background information on Call profile parameters. For detailed information about each parameter, see the Reference Guide for your MAX." on page 2-45.)

Term Timing

The Term Timing parameter enables a clock signal that compensates for the phase difference between Send Data and Send Timing. If the codec uses this signal, set the Term Timing parameter to yes. Otherwise, it uses the Send Timing signal from the codec.

Esc

If the Dial parameter specifies RS-366 ext2, the default escape character is #. You can set RS-366 Esc to specify a different escape character if you wish.

Early CD

By default, the MAX raises Carrier Detect (CD) after the completion of handshaking and an additional short delay. If the local or remote codec times out waiting for CD, you can set Early CD to raise CD without waiting for handshaking.

DS0 Min Rst

A DS0 minute is the online usage of a single 56-Kbps or 64-Kbps switched channel for one minute. When the usage exceeds the maximum (MAX DS0 Mins), the MAX cannot place any more calls, and it takes any existing calls offline. The DS0 Min Rst parameter resets accumulated DS0 minutes to zero after a specified time, or disables the timer.

Sample Port profile configuration

To configure the port for RS-366 dialing:

1 Open Host/6 > Port 1 Menu > Port Config.

2 Assign the profile a name, and configure call routing. For example:

```
Host/6
   Port 1 Menu
      Port Config
         Port Name=Port1
         Dial Plan=Trunk Grp
         Ans 1#=1212
         Ans 2#=1213
         Ans 3#=1214
         Ans 4#=1215
```

3 Set the Dial, Answer, and Clear parameters appropriately for the codec. For example:

```
Dial=RS-366 ext1.
Answer=Auto
Clear=Terminal
```

4 Leave the default values for the remaining parameters, or modify them as needed.

5 Close the Port profile.

Port diagnostics

After configuring the port, you can perform a loopback test to verify the configuration. The Port Diagnostics menu contains only the loopback command:

```
Host/6
   Port N Menu
      Port Diag
         Local LB
```

For detailed information about the Local LB command, see the *MAX 6000 Series Administration Guide*. In a local loopback test, data originating at the local site loops back to its originating port without going out over the WAN. It is as though a *data mirror* were held up to the data at the WAN interface, and the data reflected back to the originator. The WAN interface is the port on the MAX that connects to a WAN line. The AIM port on the MAX must be idle when you run the local loopback test. It can have no calls online.

Configuring the Host interface

A Host interface profile defines how the port or pair of ports interfaces with the codec. Following are the related host-interface parameters (shown with sample settings):

```
Host/6
   Mod Config
      Module Name=dualport
      Port 1/2 Dual=Yes
      Port 3/4 Dual=Yes
      Port 5/6 Dual=No
      Palmtop=Full
      Palmtop Port #=N/A
      Palmtop Menus=Standard
```

```
Host/Dual
   Mod Config
      Module Name=nodual
      Dual Ports=No Dual
      Palmtop=Full
      Palmtop Port #=N/A
      Palmtop Menus=Standard
```

This section provides some background information about configuring the interface to the codec. For detailed information about each parameter, see the *MAX Reference Guide*.

Pairing ports for dual-port calls

If you are configuring the interface to an older model codec that does not support AIM, you can pair two AIM ports to provide double the bandwidth for the videoconferencing call. A dual-port call requires a dual-interface on the codec.

In a dual-port call, the codec performs its own inverse multiplexing on two channels so that a call can achieve twice the bandwidth of a single channel. A pair of AIM ports on the MAX connects to the codec. The pair includes a primary and secondary port. Because the MAX places the two calls in tandem and clears the calls in tandem, it considers them a single call.

Creating a dual-port configuration does not prevent you from dialing any other type of call from the primary host port of the pair, or from using either port for receiving type of call. Pairing ports does not disable RS-366 dialing at the secondary port.

Enabling dual-port calls

The following configuration pairs the first two AIM ports in a Host 6 card:

1 Open Host/6 > Mod Config.

2 Assign a name (optional).

3 Set the Dual Port parameter to pair two ports. For example:

```
Host/6
   Mod Config
      Module Name=pair-one
      Port 1/2 Dual=Yes
      Port 3/4 Dual=No
      Port 5/6 Dual=No
```

4 Close the Host interface profile.

For more information, see "Configuring a two-channel dual-port call" on page 2-50.

Configuring WAN connections between serial hosts

A Call profile defines a WAN connection on the AIM port. Following are the profile's parameters (shown with sample settings):

```
Host/6 (or Host/Dual)
   Port1 Menu
      Directory
         Name=bonding
         Dial #=212-555-1212
         Call Type=bonding
         Call Mgm=Mode 1
         Data Svc=56K
         Force 56=No
         Base Ch Count=3
         Inc Ch Count=2
         Dec Ch Count=1
         Bill #=212-555-1213
         Auto-BERT=120
         Bit Inversion=No
         Fail Action=Disc
         PRI # Type=Intl
         Transit #=222
         Group=N/A
         FT1 Caller=N/A
         B&O Restore=N/A
         Flag Idle=Yes
         Dyn Alg=N/A
         Sec History=N/A
         Add Pers=N/A
         Sub Pers=N/A
         Call Password=Ascend
         Time Period 1...
            Activ=N/A
            Beg Time=N/A
            Min Ch Cnt=2
            MAX Ch Cnt=12
            Target Util=N/A
```

This section provides some background information on Call profile parameters. For detailed information about each parameter, see the *MAX Reference Guide*.

Dial#

The Dial# parameter specifies the far-end number and can specify the method of placing the call. It can include up to 24 characters. On a two channel call, it can contain up to 49 characters, or two phone numbers containing up to 24 characters each and separated by an exclamation point. For details about specifying the method of placing the call, see “Routing outbound calls” on page 2-60.

Note: The V.25bis protocol implementation in the MAX includes extensions that enable you to use the V.25bis CRS command to specify a phone number. In the CRS command you can specify a BONDING or other profile, followed by a phone number that is stored in the Dial# parameter. For such usage, the phone number has a limit of 20 characters.

Connection type and bandwidth management

The Call type parameter specifies the type of connection between the local and remote codecs. The available settings are:

- 1 Chnl—Single channel call
- 2 Chnl—Dual-port call
- FT1-B&O—Provides automatic backup and overflow protection of nailed-up circuits)
- FT1—Fractional T1 nailed channels
- AIM—Uses Ascend Inverse Multiplexing to combine channels.
- FT1-AIM—Combines nailed and switched channels by means of the AIM protocol.
- BONDING—Uses the Bandwidth On Demand Interoperability Group September 1992 1.0 specification.

  When you select an AIM or BONDING call type, you must also specify a management method by setting the Call Mgm parameter. For more complete information, see the *MAX Reference Guide*.

Bandwidth issues

The Base Ch Count parameter specifies the base number of channels to use when setting up the call. Inc Ch Count and Dec Ch Count specify the number of channels the MAX can add and subtract at one time, respectively.

The Data Svc parameter affects how much bandwidth is available for a particular session, and how channels may be allocated to the call. For example, if Data Svc is set to 384K, then the channel count parameters such as Dec Ch Count should be divisible by 6 (namely, 6, 12, 18, or 24), because 384 Kbps is 6x64 Kbps. Operational problems can result if you do not specify a multiple of 6. The Inc Ch Count parameter’s setting should equal the number of B channels in the service or a integer multiple of that service’s B channels.

Similarly, if the data service is MultiRate or GloBanD (a multiple of 64 Kbps), then be sure to make Inc Ch Count and Dec Ch Count divisible by the same multiple. Again, the Inc Ch Count parameter’s setting should equal the number of B channels in the service or a integer multiple of that service’s B channels.

Action upon failure to establish base channels of a connection

The Fail Action parameter specifies whether the MAX disconnects, reduces the bandwidth request, or establishes a lower bandwidth call and retries for the additional bandwidth when it cannot establish a call with the number of channels specified by the Base Ch Count parameter.

Telco options

You can configure a set of Telco options for the call, including a billing number, automatic byte-error test (Auto-BERT), PRI # Type, Transit #, a trunk group or nailed group number, and FT1 caller (whether the local codec originates the call).

B & O Restore and Flag Idle

When the call type is FT1-B&O, the B&O Restore parameter specifies the number of seconds to wait before restoring a nailed channel that has been dropped because of quality problems.

When the call management type is Dynamic, Flag Idle specifies whether the port looks for a flag pattern (01111110) or a mark pattern (11111111) as the idle indicator.

Dynamic bandwidth allocation issues

The MAX can use its proprietary dynamic bandwidth allocation algorithms, for calls that have AIM- or BONDING-compatible equipment on both ends.

The MAX connects to the remote end over a single channel and then dials multiple channels to the same destination on the basis of the total amount of bandwidth requested. When adding bandwidth, the MAX adds the number of channels specified in the Inc Ch Count parameter. When subtracting bandwidth, it subtracts the number of channels specified in the Dec Ch Count parameter. The following settings determine when bandwidth is added or subtracted:

- Dyn Alg specifies the algorithm to use for calculating ALU during the time period specified by the Sec History parameter.
- Sec History specifies a time period, in seconds that the MAX uses as the basis for calculating average line utilization (ALU). The MAX compare the ALU to a target percentage threshold (Target Util). When the ALU exceeds the threshold for a specified time, the MAX attempts to add channels. When ALU falls below the threshold for a specified time period, the MAX attempts to remove channels.
- Add Pers specifies the time, in seconds for which the ALU must exceed the Target Util before the MAX adds bandwidth.
- Sub Pers specifies the number of seconds for which the ALU must fall below the Target Util before the MAX subtracts bandwidth.
- Time period *N* opens a submenu of parameters for a specifying a time period. You can divide an AIM call that specifies Dynamic call management into time periods, each characterized by separate Activ, Beg Time, Max Ch Cnt, Min Ch Cnt, and Target Util parameters.

Call Password

The calling unit sends the Call Password setting when the base channel of the call connects. The receiving unit compares the value to its Port Password. If the password received matches the stored password, the session establishes 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 sends a *Password Mismatch* message to indicate that the call failed authentication.

For additional information, see “This section provides some background information about AIM-port configuration. For detailed information about each parameter, see the Reference Guide for your MAX.” on page 2-41.

Example of AIM call configuration

To configure an AIM call that uses dynamic bandwidth allocation algorithms to manage the call dynamically:

1 Open a Host/6 Directory profile, such as Host/6 > Port 1 Menu > Directory.

2 Specify the dial number to reach the remote device, and set the call type to AIM. For example:

```
Host/6
   Port 1 Menu
      Directory
         Name=aim
         Dial #=6-212-555-1212
         Call Type=aim
```

3 Specify Dynamic call management:

```
         Call Mgm=Dynamic
```

4 Set the base channels and the number of channels to be added or subtracted when bandwidth requirements change. For example:

```
         Base Ch Count=3
         Inc Ch Count=2
         Dec Ch Count=1
```

5 Set the DBA parameters. For example:

```
         Dyn Alg=Quadratic
         Sec History=60
         Add Pers=20
         Sub Pers=20
         Time Period 1...
            Activ=Enabled
            Beg Time=00:00:00
            Min Ch Cnt=1
            MAX Ch Cnt=12
            Target Util=70
```

6 Close the Call profile.

Example FT1-B&O call configuration

While FT1 calls use nailed channels, FT1-AIM and FT1-B&O calls can combine switched channels with nailed channels. For FT1-B&O calls, you must also specify B&O Restore.

Note: For FT1-AIM or FT1-B&O, you must set the Idle and Dial parameters in the Port profile at both the local and remote ends of the call. For the MAX to connect the switched channels when you turn it on, choose Idle=Call and Dial=Terminal. For the MAX to connect the switched channels when the host equipment at both ends sets DTR active, set Idle=None and Dial=DTR.In this latter configuration, the hosts at both ends of the connection must establish DTR active to make the MAX connect the switched channels.

To configure an FT1-B&O call:

1. Open a Host/6 Directory profile, such as Host/6 > Port 1 Menu > Directory.
2. Set the call type to FT1-B&O.

```
Host/6
   Port 1 Menu
      Directory
         Name=ft1-bo
         Call Type=FT1-B&O
```

3. Set call management to Dynamic. This is required in the device that initiates the FT1-B&O call.

```
         Call Mgm=Dynamic
```

4. Specify the Group number for the nailed channels. For example:

```
         Group=3
```

5. Specify that the MAX initiates the call:

```
         FT1 Caller=Yes
```

   If the other end of the link initiates the call, set this parameter to No. Only one side of the link can initiate the call for FT1-AIM or FT1-B&O calls.

6. Close the Call profile.
7. Open the Port Config profile, which in this case is Host/6 > Port 1 Menu > Port Config.
8. Specify how the switched channels connect. For example:

```
Host/6
   Port 1 Menu
      Port Config
         Idle=None
         Dial=DTR
```

   These settings must be the same in the devices at both ends of the link. The settings shown above connect the switched channels when the host equipment at both ends sets DTR active. As an alternative, the following settings connect the channels at power-up:

```
Host/6
   Port 2 Menu
      Port Config
         Idle=Call
         Dial=Terminal
```

9. Close the Port profile.

Configuring a single-channel call

This example shows how to configure a connection between two terminal adaptors connected to two AIM ports in the MAX. A call between AIM ports on the same MAX remains entirely local; the MAX does not use any WAN channels. To configure a single-channel port-to-port call:

1. Open a Host/6 Directory profile, such as Host/6 > Port 3 Menu > Directory.
2. Set the Dial # parameter in a special 3-digit format. For example:

```
Host/6
   Port 3 Menu
      Directory
```

```
Name=terminal-adaptors
Dial #=241
```

For more information, see “Routing outbound calls” on page 2-60.

3 Specify a single-channel call type:

```
Call Type=1 Chnl
```

4 Close the Call profile.

Configuring a two-channel dual-port call

In a dual-port call, two AIM ports on the MAX connect the call to the serial host. The two ports are a primary port and a secondary port. However, the MAX places the two calls in tandem and clears the calls in tandem, and considers them a single call. The following restrictions apply for dual-port connections:

- The selected data service must be available end-to-end.
- The dialing method cannot be V.25 bis.
- The Answer number must be the same for both ports.
- If trunk groups are in use, both channels of the call must be in the same trunk group.

In this example, the Host interface profile must enable port pairing for dual-port calls. (For details, see “Enabling dual-port calls” on page 2-44.) In addition, a T1 or E1 line has two of its channels configured with the phone number 1212 (a hunt group). To route the call answered on the 1212 hunt group to the paired ports for a dual-port call:

1 Open Host/Dual > Port 1 Menu > Port Config.

This is the Port profile for the primary port (Port 1).

2 Specify the hunt-group answer number. For example:

```
Host/Dual
   Port 1 Menu
      Port Config
         Port Name=Port1
         Ans 1#=1212
```

Note: Do not set the Ans # parameter for the secondary host port (Port 2).

3 Close the Port profile.

To configure the dual-port call:

1 Open Host/Dual > Port 1 Menu > Directory.

This is the Call profile for the primary port (Port 1).

2 Specify the dial number of the remote codec. For example:

```
Host/Dual
   Port 1 Menu
      Directory
         Name=hunt-groups
         Dial #=6-201-555-7878
```

If the dual-port call requires two dial numbers, specify both numbers. Separate them with by an exclamation mark. For example:

```
Dial #=6-201-555-7878!6-201-555-7879
```

3 Set Call Type to 2 Chnl:

```
Call Type=2 Chnl
```

4 Close the Call profile.

Configuring call routing

This section describes how to configure incoming and outgoing call routing on the MAX. If you have a mixture of incoming calls, such as modem and digital, this section answers your questions about routing those calls to the proper modules in the MAX. This section also includes a state diagram illustrating incoming call routing. The last part of the section describes how the MAX handles outbound calls.

Routing inbound calls

When the MAX receives a call on a WAN line, it performs CLID or DNIS authentication (if appropriate), answers the call, and determines which slot should receive the call. It then finds the caller's profile, authenticates the call, builds a session, and passes the data stream to the appropriate module or host. If a call is routed to the Ethernet port, the bridge/router software forwards it to a host or hosts according to packet addresses.

Specifying answer numbers for destination host ports

The MAX then checks for answer-number specifications. If it finds a matching answer number, it uses that to route the call. If not, it goes on to the next comparison.

Specifying host ports' slot and port numbers in WAN channel configurations

The MAX then checks for slot and port number specifications. If it finds a matching slot number, it uses that to route the call. (If it also finds a port number, if routes to that specific port on the slot number.) If not, it goes on to the next comparison.

Exclusive port routing

Unless you turn on exclusive port routing, if the call comes in on an ISDN line, the MAX can route the call by means of bearer service information if it finds no explicit call-routing information.

Setting up ISDN subaddressing

The MAX first checks for an ISDN subaddress in the dialed number. If it finds one, it uses that to route the call. If not, it goes on to the next comparison.

To set up ISDN subaddressing, set the following parameters (shown with sample settings):

```
System
   Sys Config
      Sub-Adr=Routing
      Serial=1
      LAN=2
```

```
DM=3
V.110=4
```

Assign single-digit settings to the AIM ports (Serial), Ethernet (LAN), digital modems (DM), and V.110 slots. When you use ISDN subaddressing in routing mode, incoming calls include a subaddress number as part of the phone number. With the configuration in this configuration, the caller would dial 510-555-1212,3 to reach the digital modems. The subaddress “3” follows the dialed number and is separated from it by a comma.

Specifying answer numbers for destination host ports

Each host port can specify one or more answer numbers. When the MAX receives an inbound call and no subaddress is in use, it matches the called number to these answer numbers and routes the call to the port with the matching number. Following are the related parameters (shown with sample settings):

```
V.34 Modem (or V.42 Modem)
   Mod Config
      Ans 1#=1213
      Ans 2#=1214
      Ans 3#=1215
      Ans 4#=1216

V.110
   Mod Config
      Ans 1#=1217
      Ans 2#=1218
      Ans 3#=1219
      Ans 4#=1220

Host/BRI
   Line Config
      Line N...
         Ans 1#=1230
         Ans 2#=1231

BRI/LT
   Line Config
      Line N...
         Ans 1#=1240
         Ans 2#=1241

   Port N Menu
      Port Config
         Ans 1#=1232
         Ans 2#=1233
         Ans 3#=1234
         Ans 4#=1235

Ethernet
   Mod Config
      WAN options...
         Ans 1#=1236
         Ans 2#=1237
         Ans 3#=1238
         Ans 4#=1239
```

Note: When a MAX has more than one digital modem slot card installed, the cards and modems form a pool, and any modem can answer a call routed to any digital modem slot.

Slot and port specifications

In the configuration of WAN lines, you can assign one or more channels to a slot card. In the case of an AIM slot card, you can assign channels to a port on the card. This channel configuration affects both inbound call routing and the placement of calls. In effect, the configuration reserves the channel for calls to and from the specified slot or port.

Configure slot and port routing only when answer number and ISDN subaddress routing are not specified. Following are the related parameters (shown with sample settings):

```
Net/T1
   Line Config
       Line N...
         Ch N=Switched
         Ch N Slot=3
         Ch N Prt/Grp=1
Net/E1
   Line Config
      Line N...
         Ch N=Switched
         Ch N Slot=3
         Ch N Prt/Grp=1
Net/BRI
   Line Config
      Line N...
         BN Usage=Switched
         BN Slot=3
         BN Prt/Grp=1
```

When the MAX receives an inbound call and no subaddress is in use or no matching answer number is found, it evaluates the slot and port specifications and routes the call to the specified destination. In the MAX 2000 model:

- 0 (Zero, the default) specifies that this parameter is not used to route incoming calls.
- 1 is an invalid setting, because it represents the built-in slot for T1 or E1 lines.
- 2-3 represent expansion slots. When looking at the back panel of the MAX unit, slot 2 is the left-hand slot and slot 3 is the right-hand slot.
- 4 represents the LAN. The MAX routes calls to the bridge/router module.

Note: When a MAX has more than one digital modem slot card installed, the cards and modems form a pool, and any modem can answer a call routed to any digital modem slot.

Exclusive port routing

Exclusive port routing prevents the MAX from accepting calls for which it has no explicit routing destination. If you set the System > Sys Config > parameter Excl Routing to No (the default), it routes the call on the basis of bearer service. The MAX routes voice calls to a digital modem, it routes V.110 calls to a V.110 module, and data calls to an AIM port or, if no AIM ports are available, to the bridge/router. If you set Excl Routing to Yes and none of the specified call-routing comparisons are successful, the MAX drops the call.

Limiting incoming calls using DNIS-related methods

You can limit the number of incoming calls that the MAX accepts to sixteen specific dialed numbers, or from modem callers, V.110 callers, or HDLC callers. Also, there are three terminal-server commands to display DNIS sessions and statistics.

Overview

You can configure the MAX to limit the number of incoming calls on the basis of:

- Called number ID (DNIS) presented by calls
- MAX resource that answers the call: modem, HDLC, or V.110
- Combined maximum number of calls to modem, HDLC, and V.110 resources

Note: The MAX considers a call to be an HDLC call if it is not a modem call or a V.110 call.

The MAX returns the cause `Busy` for rejected calls.

If the MAX receives a call that does not specify a dialed number or provides a dialed number not specified in the DNIS #*N* parameters, the MAX considers the call as having an *Unspecified* DNIS.

Call routing

When you set Ethernet > Mod Config > DNIS options > DNIS Limitation to Yes, and the MAX receives a call that provides a DNIS number specified in Ethernet > Mod Config > DNIS options > DNIS #*N*, the MAX routes the call as follows:

1 The MAX compares DNIS #*N* max calls to the number of active calls made to the called number.
If the maximum has been reached, the MAX rejects the call.

2 If the call is a modem call, the MAX compares DNIS #*N* max Modem to the number of active modem calls made to the called number.
If the maximum has been reached, the MAX rejects the call.

3 If the call is an V.110 call, the MAX compares DNIS #*N* max V110 to the number of active V.110 calls made to the called number.
If the maximum has been reached, the MAX rejects the call.

4 If the call is not a modem or V.110 call, the MAX considers it an HDLC call and compares DNIS #*N* max HDLC to the number of active HDLC calls made to the called number.
If the maximum has been reached, the MAX rejects the call.

The MAX answers the call if no maximum has been reached.

If the call does not provide DNIS, or no specified DNIS #*N* matches the provided DNIS number, the MAX proceeds as follows:

1 The MAX compares Unspecified max calls to the number of unspecified active calls.
If the maximum has been reached, the MAX rejects the call.

2 If the call is a modem call, the MAX compares Unspecified max Modem to the number of unspecified active modem calls.
If the maximum has been reached, the MAX rejects the call.

3 If the call is an V.110 call, the MAX compares Unspecified max V110 to the number of unspecified active V.110 calls.

If the maximum has been reached, the MAX rejects the call.

4 If the call is not a modem or V.110 call, the MAX considers it an HDLC call and compares Unspecified max HDLC to the number of unspecified active HDLC calls.

If the maximum has been reached, the MAX rejects the call.

The MAX answers the call if no maximum has been reached.

Limiting calls to specific dialed numbers

To limit calls to specific dialed numbers, proceed as follows:

1 Open the Ethernet > Mod Config > DNIS options submenu.

2 Set DNIS Limitation to Yes.

3 Set DNIS #*N* to a called number.

The MAX compares the called number to DNIS #*N* digit-by-digit, right to left. A match occurs when all the digits specified in DNIS #*N* match the same number of rightmost digits of the called number. For example, if you set DNIS #*N* to 1235, then the called number 8761235 matches, but 1235876 does not match.

4 Set DNIS #*N* max calls to specify the total of simultaneous V.110, HDLC, and modem calls to the called number specified in DNIS #*N*.

Note: You must set DNIS #*N* max calls even if you configure the MAX to limit calls on the basis of modem, V.110, or HDLC calls.

5 Set DNIS #*N* Modem if you want to limit the number of simultaneous modem calls to the called number specified in DNIS #*N*.

6 Set DNIS #*N* HDLC if you want to limit the number of simultaneous synchronous calls to the called number specified in DNIS #*N*.

7 Set DNIS #*N* V110 if you want to limit the number of simultaneous V.110 calls to the called number specified in DNIS #*N*.

8 Exit and save the changes.

You can configure up to sixteen DNIS numbers with unique limiting configurations for each DNIS number.

Limiting calls to unspecified dialed numbers

Similar to specified dialed numbers, you can limit the number of simultaneous modem, HDLC, or V.110 calls. Proceed as follows:

1 Open the Ethernet > Mod Config > DNIS options submenu.

2 Set DNIS Limitation to Yes.

3 Set Unspecified max calls if you want to limit the total of simultaneous V.110, HDLC, and modem calls to called numbers that do not match any specified in DNIS #*N*.

Note: You must set Unspecified max calls even if you configure the MAX to limit calls on the basis of modem, V.110, or HDLC calls.

4 Set Unspecified max Modem if you want to limit the number of simultaneous modem calls to called numbers that do not match any specified in DNIS #*N*.

5 Set Unspecified max HDLC if you want to limit the number of simultaneous synchronous calls to called numbers that do not match any specified in DNIS #*N*.

6 Set Unspecified max V110 if you want to limit the number of simultaneous V.110 calls to called numbers that do not match any specified in DNIS #*N*.

7 Exit and save the changes.

Example of call routing

This section shows three sample configurations to limit incoming calls on the basis of DNIS values.

Limiting all modem calls that do not specify a DNIS number

To specify that the MAX accepts ten simultaneous modem calls that do not specify a DNIS number, configure the following parameters as shown:

- Unspecified max calls = 10
- Unspecified modem calls = 10
- Unspecified V110 calls = 0
- Unspecified HDLC calls = 0

Limiting all calls that do not specify a DNIS number

To specify that the MAX accepts twenty calls of any type that do not specify a DNIS number, configure the following parameters as shown:

- Unspecified max calls = 20
- Unspecified modem calls = 20
- Unspecified V110 calls = 20
- Unspecified HDLC calls = 20

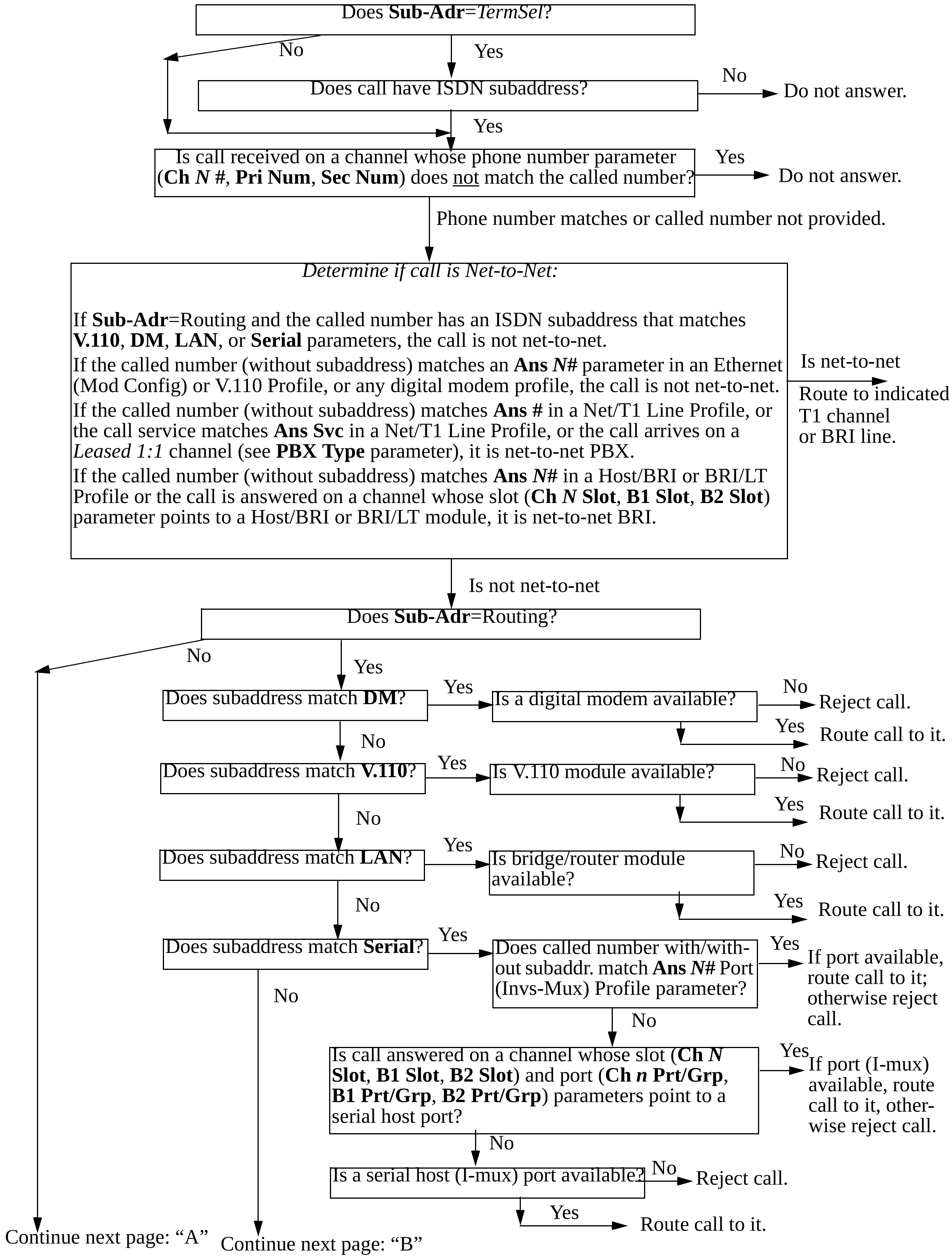
Limiting V.110 calls to a specific DNIS number

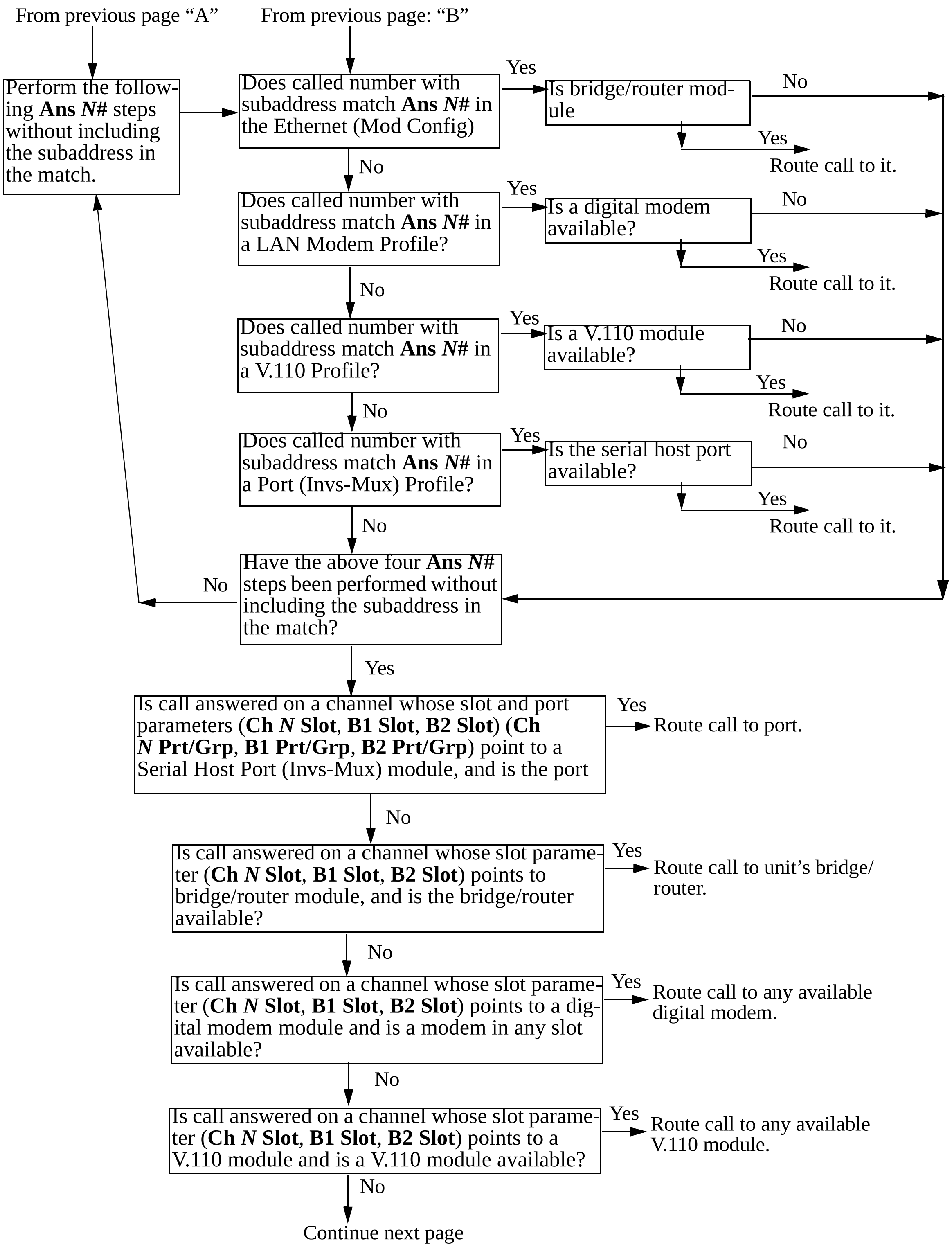
To specify that the MAX accepts fifteen simultaneous V.110 calls that specify a DNIS number of 1212, and allowing 100 simultaneous calls to any DNIS number (except 1212), configure the following parameters as shown:

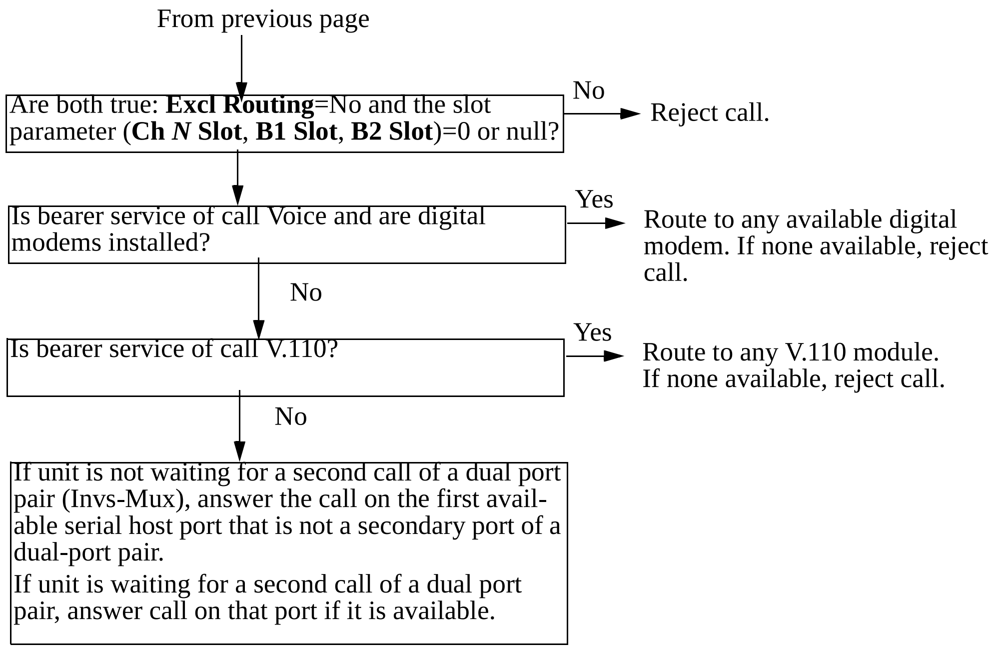
- DNIS #1 max calls = 15
- DNIS #1 modem calls = 0
- DNIS #1 V110 calls = 15
- DNIS #1 HDLC calls = 0
- Unspecified max calls = 100
- Unspecified modem calls = 100
- Unspecified V110 calls = 0
- Unspecified HDLC calls = 0

Incoming call routing state diagram

The following pages show detailed state information about inbound call routing in the MAX. To understand these charts, you should be familiar with the parameters referenced in many of the steps.


Does Sub-Adr=TermSel?
No
Yes
Does call have ISDN subaddress?
No
Do not answer.
Yes
Is call received on a channel whose phone number parameter (Ch N #, Pri Num, Sec Num) does not match the called number?
Yes
Do not answer.
Phone number matches or called number not provided.
Determine if call is Net-to-Net:
If Sub-Adr=Routing and the called number has an ISDN subaddress that matches V.110, DM, LAN, or Serial parameters, the call is not net-to-net.
If the called number (without subaddress) matches an Ans N# parameter in an Ethernet (Mod Config) or V.110 Profile, or any digital modem profile, the call is not net-to-net.
If the called number (without subaddress) matches Ans # in a Net/T1 Line Profile, or the call service matches Ans Svc in a Net/T1 Line Profile, or the call arrives on a Leased 1:1 channel (see PBX Type parameter), it is net-to-net PBX.
If the called number (without subaddress) matches Ans N# in a Host/BRI or BRI/LT Profile or the call is answered on a channel whose slot (Ch N Slot, B1 Slot, B2 Slot) parameter points to a Host/BRI or BRI/LT module, it is net-to-net BRI.
Is net-to-net
Route to indicated T1 channel or BRI line.
Is not net-to-net
Does Sub-Adr=Routing?
No
Yes
Does subaddress match DM?
Yes
Is a digital modem available?
No
Reject call.
Yes
Route call to it.
No
Does subaddress match V.110?
Yes
Is V.110 module available?
No
Reject call.
Yes
Route call to it.
No
Does subaddress match LAN?
Yes
Is bridge/router module available?
No
Reject call.
Yes
Route call to it.
No
Does subaddress match Serial?
Yes
Does called number with/without subaddr. match Ans N# Port (Invs-Mux) Profile parameter?
Yes
If port available, route call to it; otherwise reject call.
No
No
Is call answered on a channel whose slot (Ch N Slot, B1 Slot, B2 Slot) and port (Ch n Prt/Grp, B1 Prt/Grp, B2 Prt/Grp) parameters point to a serial host port?
Yes
If port (I-mux) available, route call to it, otherwise reject call.
No
Is a serial host (I-mux) port available?
No
Reject call.
Yes
Route call to it.
Continue next page: “A”
Continue next page: “B”


From previous page "A"
From previous page: "B"
Perform the following Ans N# steps without including the subaddress in the match.
Does called number with subaddress match Ans N# in the Ethernet (Mod Config)
Yes
Is bridge/router module
No
Yes
Route call to it.
No
Does called number with subaddress match Ans N# in a LAN Modem Profile?
Yes
Is a digital modem available?
No
Yes
Route call to it.
No
Does called number with subaddress match Ans N# in a V.110 Profile?
Yes
Is a V.110 module available?
No
Yes
Route call to it.
No
Does called number with subaddress match Ans N# in a Port (Invs-Mux) Profile?
Yes
Is the serial host port available?
No
Yes
Route call to it.
No
Have the above four Ans N# steps been performed without including the subaddress in the match?
No
Yes
Is call answered on a channel whose slot and port parameters (Ch N Slot, B1 Slot, B2 Slot) (Ch N Prt/Grp, B1 Prt/Grp, B2 Prt/Grp) point to a Serial Host Port (Invs-Mux) module, and is the port
Yes
Route call to port.
No
Is call answered on a channel whose slot parameter (Ch N Slot, B1 Slot, B2 Slot) points to bridge/router module, and is the bridge/router available?
Yes
Route call to unit's bridge/ router.
No
Is call answered on a channel whose slot parameter (Ch N Slot, B1 Slot, B2 Slot) points to a digital modem module and is a modem in any slot available?
Yes
Route call to any available digital modem.
No
Is call answered on a channel whose slot parameter (Ch N Slot, B1 Slot, B2 Slot) points to a V.110 module and is a V.110 module available?
Yes
Route call to any available V.110 module.
No
Continue next page



Routing outbound calls

When the MAX dials out, it routes the outbound call from the originating slot to a WAN channel to place the call. It looks for channels whose Ch N Trn Grp (or B1 Trnk Grp or B2 Trnk Grp) parameter matches the trunk group prefix in the number dialed; that is, in the Dial # parameter of the Call Profile placing the call.

(Note that, invs-mux calls have priority over other types of outgoing calls on those channels whose Ch N Slot parameters point to invs-mux modules.) If no trunks have available channels, the call is not placed.

Note: An available channel within the trunk group is one that is not assigned to any port (its slot/port numbers are zero) or is assigned to the port that originated the call. Channels assigned to another port are not available.

Enabling trunk groups

If you enable trunk groups, dial-out numbers must include a trunk group number as a dialing prefix, and all switched channels to be available for outbound calls must be assigned to a trunk group.

A trunk group is a group of channels that has been assigned a number. Once you have enabled trunk groups, all switched channels must be assigned a trunk group number if they are to be available for outbound calls.

The following setting enables trunk groups:

```
System
   Sys Config
      Use Trunk Grps=Yes
```

Note: Trunk group numbers 2 and 3 have special meaning, as described in the next two sections. Only trunk groups 4–9 are available for assignment to channels.

Dialing through trunk group 2 (local port-to-port calls)

Use trunk group 2 for port-to-port calls within the MAX system. Trunk group 2 is the first digit in a 3-digit dialing prefix in which the next 2 digits are interpreted as the slot and port number of the called port.

When 2 is the first digit in a three-digit dial number, the MAX places a call to the slot and port specified in the next two digits. Following are the related parameters (shown with sample settings):

```
Host/6 (or Host/Dual)
   PortN Menu
      Directory
         Name=bonding
         Dial #=241
```

With Dial# set to 241, the MAX places a call to the first port of a Host 6 or Host Dual card in slot 4. The second digit can be 0 or any number from 3 to 8. If it is zero, the call goes to any available AIM port (the third digit is ignored in this case). Digits 3–8 represent an expansion slot number, and the third digit is the host port on that card.

Dialing through trunk group 3 (Destination profiles)

Trunk group 3 is the first digit in a three-digit dialing prefix in which the next two digits are interpreted as the number of a Destination profile.

When three is the first digit in a three-digit dialing prefix, the MAX interprets the next two digits as the number of a Destination profile. Following are the related parameters (shown with sample settings):

```
Destinations
   Name=outdial-1
   Option=1st Avail
   Dial 1#=4-212-555-1212
Dial Plan
   Call-by-Call 1=1
   Dial 2#=5-212-555-1212
   PRI # Type=National
   Transit #=
   Bill #=

Host/6 (or Host/Dual)
   Port N Menu
      Directory
         Dial #=312

Ethernet
   Connections
      Dial #=312
```

With Dial# set to 312, the MAX reads Destination profile 12. Destination profiles let you instruct the MAX to use the first available channels to place the call, or to try one trunk group first, followed by another if the first in unavailable. For example, if the Destination profile sets Option=1st Avail, the MAX takes the first available channels for the call. If the dial numbers specify different trunk groups, the MAX can use bandwidth from one switch as backup for another. For example, trunk group four might contain channels serviced by Sprint while trunk group five might be serviced by AT&T.

Dialing through trunk groups 4–9

You can assign a trunk group to any channel that the MAX uses for placing the call. If the specified group has no available channels, the call is not placed.

There are six available trunk groups. Trunk group numbers 4–9 can be assigned to WAN channels to group those channels. Trunk-group assignments limit the number of channels available to multichannel calls, because only channels within the same trunk group can be aggregated. The MAX uses trunk-group assignments to group the channels from different types of lines. For example, when more than one carrier services the MAX lines, you can assign trunk group four to a line serviced by one carrier and trunk group five to a line serviced by another.

Note: A trunk group cannot include both BRI and PRI channels.

Following are the related parameters (shown with sample settings):

```
Net/T1
   Line Config
      Line N...
         Ch N=Switched
         Ch N TrnkGrp=4
         ...
Net/E1
   Line Config
      Line N...
         Ch N=Switched
         Ch N TrnkGrp=4
         ...
Net/BRI
   Line Config
      Line N...
         BN Usage=Switched
         BN TrnkGrp=5
Ethernet
   Mod Config
      WAN options...
         Dial Plan=Trnk Grp
Ethernet
   Connections
      Dial #=5-555-1212
Host/6 (or Host/Dual)
   Port N Menu
      Directory
         Dial Plan=Trunk Grp
         Dial #=4-555-1217
```

```
Host/BRI
   Line Config
      Line N...
         Dial Plan=Trnk Grp
```

If Dial Plan=Trunk Grp and a single-digit dialing prefix from 4 to 9, the MAX places the call through using channels in that trunk group.

Dialing through the extended dial plan

When the extended dial plan is specified for a particular port, the trunk-group number is the first digit in a three-digit dialing prefix in which the next two digits are interpreted as the number of a Dial Plan profile.

The extended dial plan relates only to PRI lines. It uses a specified trunk group, but accesses a Dial Plan profile to obtain PRI parameters for the outbound call. The extended dial plan is typically used to route calls from a terminating device on a Host BRI line out to the WAN over PRI channels. However, it can also be used to set up the PRI parameters for other outbound calls. Following are the related parameters (shown with sample settings):

```
Dial Plan
   Name=host1
   Call-by-Call=8
   Data Svc=56KR
   PRI # Type=National
   Transit #=222
   Bill #=

Host/BRI
   Line Config
      Line N...
         Dial Plan=Extended
```

To use the extended dial plan from an AIM port or Ethernet:

```
Host/6 (or Host/Dual)
   Port N Menu
      Port Config
         Dial Plan=Extended
         Dial #=806-212-555-1217

Ethernet
   Mod Config
      WAN options...
         Dial Plan=Extended

Ethernet
   Connections
      Dial #=806-212-555-1212
```

With the dialing prefix 806, the first digit is a trunk-group number and the next two digits instruct the MAX to read Dial Plan profile 6. Placement of the call uses channels in trunk group 8 and the PRI settings in that Dial Plan profile.

Matching slot and port specifications (reserved channels)

Whether or not you enable trunk groups, the MAX relies on slot/port specifications to place outbound calls if you specify any slot/port numbers. When a channel configuration specifies a slot or slot/port combination, it effectively reserves the channel for calls to and from the specified slot or port. Calls originating from a different slot or port do not find the channel available.

Specifying a slot and port number in a channel configuration reserves the channel for calls to and from the specified slot or port. Following are the related parameters (shown with sample settings):

```
Net/T1
   Line Config
       Line N...
         Ch N=Switched
         Ch N Slot=3
         Ch N Prt/Grp=1
Net/E1
   Line Config
      Line N...
         Ch N=Switched
         Ch N Slot=3
         Ch N Prt/Grp=1
Net/BRI
   Line Config
      Line N...
         BN Usage=Switched
         BN Slot=3
         BN Prt/Grp=1
```

If the outbound call originates from a host on Ethernet, the destination address in the packets brings up a Connection profile or RADIUS user profile that dials the call. If the call does not go out through a digital modem, it originates from slot 5.

If the outbound call originates from a device connected to an AIM port, the Call profile associated with that port dials the call. This type of call originates from the slot and port of the AIM card.

If the outbound call originates from a terminal adapter connected to a Host/BRI or BRI/LT port, the call originates from the slot and port of the Host/BRI or BRI/LT card.

If the outbound call originates from a terminal-server user dialing out through a digital modem, the digital modem slot is the source of the call. (No matter where the call originates, if it goes out through a digital modem, the digital modem slot is the source of the call.)

When the MAX receives an outbound call, it evaluates the slot and port specifications as part of identifying the channels available for placing the call:

- If you set the slot and port specifications for a channel to zero (the default), the channel is available for all outbound calls that specify the trunk group assigned to the channel in the Ch N Trnk Grp parameter.
- If the slot is non-zero and the port is zero, the channel is available to outbound calls originating on that slot.

- If you set both the slot and port numbers to non-zero, the channel is available only to outbound calls originating on that port.

Configuring WAN Links

3

Introduction to WAN links

This chapter describes configuring various types of links across the WAN. It focuses on the encapsulation issues for the following types of connections:

Connection type	**Description**
Point-to-Point Protocol (PPP)	PPP and its multilink variants (MP and MP+) enable dial-in connections, from modems or ISDN devices, using one or more channels. The remote devices must have PPP software.
Combinet	Combinet bridges two network segments at the link level, using one or two channels. The remote device is another Combinet bridge.

Connection type	Description
EU-UI and EU-RAW	UI and RAW are two different types of EU encapsulation. The MAX uses EU-UI when the equipment on the other side of the connection requires the DCE and DTE address fields in the EU header. When the connection does not require these address fields, the MAX uses EU-RAW. EU connections can be dial-in or dial-out. EU encapsulation does not support an authentication protocol. Use CLID authentication to match incoming calls to the proper Connection profile when, for example, you apply special filters to certain callers, or some callers route IP and others bridge.
AppleTalk Remote Access (ARA)	ARA enables a Macintosh user to access AppleTalk devices or IP hosts via modem. The remote Mac must have ARA client software and (if applicable) TCP/IP software.
Terminal-server connections	The MAX terminal server processes asynchronous calls from modems, ISDN modems (V.120 terminal adapters), or raw TCP. You can log those calls into the terminal-server interface or, if they contain PPP, pass the asynchronous calls to the router.

This chapter does not describe RADIUS user profiles that serve the same function as resident Connection profiles. If you are using a RADIUS authentication server, see the *MAX RADIUS Configuration Guide*. For details about WAN connection security, see the *MAX Security Supplement*.

The Answer profile

The Answer profile determines whether the MAX answers or drops an incoming call. If the call does not comply with the specifications in the Answer profile, the MAX drops the call without answering it.

Most administrators set up the Answer profile to reject calls that do not match a Connection profile. When a call matches a Connection profile, the MAX uses the connection-specific settings instead of the related encapsulation and session options in the Answer profile. However, if you configure a Name/Password profile, the MAX can use the settings in the Answer profile to build the session. Following are the Answer profile parameters:

```
Ethernet
   Answer
      Use Answer as Default=No
      Force 56=No
      Profile Reqd=Yes
      Id Auth=None
      Assign Adrs=No

      Encaps...
         MPP=Yes
         MP=Yes
         PPP=Yes
         COMB=Yes
         FR=Yes
         X25/PAD=Yes
         EU-RAW=Yes
         EU-UI=Yes
```

```
   V.120=Yes
   X.75=Yes
   TCP-CLEAR=Yes
   ARA=Yes

IP options...
   Metric=7

PPP options...
   Route IP=Yes
   Route IPX=Yes
   Bridge=Yes
   Route AppleTalk=Yes
   AppleTalk options...
   Recv Auth=Either
   MRU=1524
   LQM=No
   LQM Min=600
   LQM Max=600
   Link Comp=Stac
   VJ Comp=Yes
   CBCP Enable=No
   BACP=No
   Dyn Alg=Quadratic
   Sec History=15
   Add Pers=5
   Sub Pers=10
   Min Ch Count=1
   Max Ch Count=1
   Target Util=70
   Idle Pct=0
   Disc on Auth Timeout=Yes

COMB options...
   Password Reqd=Yes
   Interval=10
   Compression=Yes

V.120 options...
   Frame Length=260

X.75 options...
   K Window Size=7
   N2 Retran Count=10
   T1 Retran Timer=1000
   Frame Length=2048

Session options...
   RIP=Off
   Data Filter=5
   Call Filter=3
   Filter Persistence=No
   Idle=120
   TS Idle Mode=N/A
   TS Idle=N/A
   IPX SAP Filter=1
   Max Call Duration=0
   Preempt=N/A
   Framed Only
```

```
DHCP options...
   Reply Enabled=No
   Pool Number=N/A
   Max Leases=N/A
```

Understanding the Answer profile parameters

This section provides some background information on the Answer profile. For detailed information about each parameter, see the *MAX Reference Guide*.

Use Answer as Default

The Use Answer as Default parameter specifies whether the Answer Profile should override the factory defaults when the MAX uses RADIUS or TACACS to validate an incoming call.

Force 56

If you set Force 56 to Yes, the MAX uses only 56 Kbps of a channel's bandwidth, even when all 64 Kbps appears to be available. The parameter is useful within North America for answering calls from European or Pacific Rim countries when the complete path cannot distinguish between the Switched-56 and Switched-64 data services. It is not needed for calls within North America.

Note: Because the default bandwidth for data calls across R2 lines is 64 Kbps, set Force 56 to Yes in any Connection profile that use 56 Kbps over R2 lines.

Profile Reqd

If you do not require a Connection profile for every caller, the MAX builds a temporary profile for an unknown caller. Many sites consider this situation (Profile Reqd=No) a security breach.

Note: Defining the Setting Profile Reqd parameter to Yes disables Guest access for ARA connections.

ID-Auth

The called number (typically the number dialed by the far end) and CLID (the far-end device's number) can be presented by the phone company as part of the call information and used in a first-level authentication process occurring before the MAX answers a call. See "Understanding Connection profile parameters" on page 3-8 for details. See the *MAX Security Supplement* for background information about authentication.

Encaps subprofile

The Encaps subprofile contains settings for each type of link encapsulation that the MAX supports. If you set an encapsulation type to No in this menu, the MAX does not accept calls of that type.

IP options

In the Answer profile, the Metric parameter determines the virtual hop count of the IP link when the MAX uses RADIUS or TACACS to validate an incoming call and you set the Use Answer as Default.

Encapsulation-specific options

For the details about PPP, Combinet, and other encapsulation options, see the sections later in this chapter, about configuring specific types of connections. The Answer profile uses these options only when you have not set corresponding options in the caller’s configured profile.

X.75 options

The X.75 options enable dial-in access to the terminal server, using the X.75 protocol. See the CCITT Blue Book Recommendation X series 1988 for full technical specifications for X.75.

Session options

In the Answer profile, session options set default filters and timers to build connections that use RADIUS (if you enable Use Answer as Defaults) or Name/Password profiles. The Framed Only option limits terminal server access per user.

DHCP options

In the Answer profile, Dynamic Host Configuration Protocol (DHCP) options enable the MAX to act as a DHCP server for a local Pipeline unit for connections that use RADIUS (if you enable Use Answer as Defaults) or Name/Password profiles.

Example of Answer profile configuration

When a call first comes in, it is unauthenticated. The Answer profile lets you negotiate the PPP, authentication, and encapsulation methods; in addition whether the call will route or bridge. After the connection authenticates, the MAX uses the appropriate Connection profile or, if RADIUS is configured, the MAX uses the appropriate User profile.

To set up the profile:

1. Open the Answer profile and set Profile Reqd to Yes.
2. Set up Calling Line ID (CLID) or Called Number authentication, if required.
3. Enable dynamic assignment of IP addresses to callers, if appropriate.

```
Ethernet
   Answer
      Profile Reqd=Yes
      Id Auth=None
      Assign Adrs=No
```

4. Make sure you enable the encapsulation types you intend to support. For example:

```
Encaps...
   MPP=Yes
   MP=Yes
   PPP=Yes
```

```
COMB=Yes
FR=Yes
X25/PAD=Yes
EU-RAW=Yes
EU-UI=Yes
V.120=Yes
X.75=Yes
TCP-CLEAR=Yes
ARA=Yes
```

5 Enable routing and bridging and specify authentication requirements, as appropriate. For example:

```
PPP options...
   Route IP=Yes
   Route IPX=Yes
   Route AppleTalk=Yes
   Bridge=Yes
   Recv Auth=Either
```

6 Set AppleTalk PPP dial-in options in the AppleTalk Options menu, if required.

7
```
COMB options...
  Password Reqd=Yes
```

8 Close the Answer profile.

Connection profiles

Connection profiles define individual connections. For a given encapsulation type, the Connection profile contains many of the same options as the Answer profile.

Note: Settings in a Connection profile always override similar settings in the Answer profile.

Following are the Connection profile parameters (shown with sample settings):

```
Ethernet
   Connections
     any Connection profile
       Station=device-name
       Active=Yes
       PRI # Type=National
       Dial #=555-1212
       Calling #=555-2323
       Called #=555-1212
       Route IP=Yes
       Route IPX=No
       Route AppleTalk=Yes
       Bridge=No
      Dial brdcast=N/A

       Encaps=encapsulation-protocol
       Encaps options...
         parameters for selected encapsulation-protocol
       IP options...
         LAN Adrs=0.0.0.0/0
         WAN Alias=0.0.0.0/0
         IF Adrs=0.0.0.0/0
         Metric=7
         Preference=100
```

```
   Private=No
   RIP=Off
   Pool=0
   Multicast Client=No
   Multicast Rate Limit=5
   Client Pri DNS=0.0.0.0
   Client Sec DNS=0.0.0.0
   Client Assign DNS=Yes
   Client Gateway=0.0.0.0

IPX options...
   Peer=Router
   IPX RIP=None
   IPX SAP=Send
   Dial Query=No
   IPX Net#=cfff0003
   IPX Alias#=00000000
   Handle IPX=None
   Netware t/o=30

AppleTalk options...
    Peer=Dialin
    Zone Name=ENGINEERING
    Net Start=2001
    Net End=2010
    Default Zone=
    Zone Name #1=
    Zone Name #2=
    Zone Name #3=
    Zone Name #4=

Session options...
   Data Filter=5
   Call Filter=3
   Filter Persistence=No
   Idle=120
   TS Idle Mode=N/A
   TS Idle=N/A
   Max Call Duration=0
   Preempt=N/A
   IPX SAP Filter=0
   BackUp=
   IP Direct=0.0.0.0
   FR Direct=No
   FR Prof=N/A
   FR DLCI=N/A
   Framed Only

OSPF options…
   RunOSPF=Yes
   Area=0.0.0.0
   AreaType=Normal
   StubAreaDefaultCost=N/A
   HelloInterval=40
   DeadInterval=120
   Priority=5
   AuthType=Simple
   AuthKey=ascend0
   Cost=10
```

```
   ASE-type=N/A
   ASE-tag=N/A
   TransitDelay=5
   RetransmitInterval=20
Telco options...
   AnsOrig=Both
   Callback=Yes
   Exp Callback=No
   Call Type=Switched
   Group=N/A
   FT1 Caller=N/A
   Data Svc=56KR
   Force 56=N/A
   Bill #=555-1212
   Call-by-Call=N/A
   Transit #=222
   Dialout OK=No
Accounting...
   Acct Type=None
   Acct Host=N/A
   Acct Port=N/A
   Acct Timeout=N/A
   Acct Key=N/A
   Acct-ID Base=N/A
DHCP options...
   Reply Enabled=No
   Pool Number=N/A
   Max Leases=N/A
```

Note: After you select an encapsulation method in the Encaps option, the Encaps Options subprofile contains settings related to the selected type.

For information on IP, IPX, bridging, OSPF, and AppleTalk configuration, see the appropriate chapter in this guide. For detailed information about each parameter, see the *MAX Reference Guide*.

Understanding Connection profile parameters

This section provides some background information about Connection profile parameters.

Station

The station name is the name of the remote device. Make sure the name matches the remote device's name exactly, including case changes.

PRI # Type

PRI # Type enables an AT&T switch to use your dial number when you make a call using T1 channels and ISDN signaling. You can specify National (inside the U.S.), Intl (outside the U.S.) or Local (within your Centrex group).

Dial #

Dial # is the phone number the MAX dials when an outbound caller attempts to establish a connection. The number can contain up to 24 characters including a dialing prefix that directs the connection to use a trunk group or dial plan (for example: 6-1-212-555-1212). For more details, see Chapter 2, “Configuring the MAX for WAN Access.”

Calling #

Many carriers include the calling number (the phone number of the far-end device placing the call in each call. Calling # is the caller ID number that appears on some phones. The MAX also uses Calling # for Calling Line ID (CLID) authentication.

CLID authentication prevents the MAX from answering a connection unless it originates at the specified phone number. The number you specify can also be used for callback security if you configure callback in the per-connection telco options.

Called #

Called # (typically the number dialed by the far end) appears in an ISDN message as part of the call when Dial Number Information Service (DNIS) is in use. In some cases, the phone company can present a modified called number for DNIS. Authentication uses this number to direct inbound calls to a particular device from a central rotary switch or PBX. For details, see the *MAX Security Supplement* for details.

Encaps and Encaps Options

An encapsulation protocol must be specified for each connection, and its accompanying options configured in the Encaps options subprofile. These are described in separate sections in this chapter.

Route IP, Route IPX, Route AppleTalk

Each connection can be configured for IP routing, IPX routing, OSPF routing (that requires IP routing), or AppleTalk routing. Each of these routing setups has a separate subprofile within a Connection profile.

Bridge

Link-level bridging forwards packets to and from remote networks on the basis of the hardware-level address, not a logical network address. Bridge and Dial Brdcast are related parameters.

Connection profile Session options

A Connection profile has the following Session Options parameters (shown with sample settings):

```
Ethernet
   Connections
      Session options...
         Data Filter=5
```

```
Call Filter=3
Filter Persistence=No
Idle=120
TS Idle Mode=N/A
TS Idle=N/A
Max Call Duration=0
Preempt=N/A
IPX SAP Filter=0
BackUp=
IP Direct=0.0.0.0
FR Direct=No
FR Prof=N/A
FR DLCI=N/A
Block calls after=0
Blocked duration
Framed Only
```

This section provides a brief overview. For detailed information about each parameter, see the *MAX Reference Guide*.

Data Filter, Call Filter

Ascend filters define packet conditions. Data filters drop specific packets, and are often used for security purposes. Call filters monitor inactive sessions and bring them down to avoid unnecessary connection costs. When a filter is in use, the MAX examines every packet in the packet stream and takes action if the defined filter conditions are present. The action the MAX takes depends both on the conditions specified within the filter and how the filter is applied. (For more information, see Chapter 7, "Defining Static Filters.")

Idle, TS Idle Mode, TS Idle

The Idle parameter is a timer setting that specifies how long the connection remains idle before the MAX drops it. The TS Idle Mode and TS Idle parameters apply to terminal-server sessions. TS Idle Mode specifies whether the MAX uses the terminal-server idle timer (TS Idle) and, if so, whether it monitors traffic in one or both directions to determine when the session is idle. TS Idle is the timer that specifies how long the terminal-server session can remain idle before the MAX logs out the user and terminates the connection.

Max Call Duration

The MAX Call Duration parameter sets the maximum duration of an incoming call (1-1440 minutes). The default (zero) turns off this function. The MAX checks the connection once a minute, so the actual time of the call can be slightly longer than the number of minutes you set.

Preempt

Preempt specifies the number of idle seconds the MAX waits before it can use one of the channels of an idle link for a new call.

Backup

The Backup parameter specifies the name of a Connection profile to use when a nailed connection goes down. For example, if a nailed connection to corporate net #1 is out of service, you can use a backup switched connection to corporate net #2. You cannot use this parameter to provide alternative lines to a single destination.

IP Direct

An IP direct connection channels all inbound packets to a specified local host as explained in Chapter 10, "Configuring IP Routing."

Frame Relay parameters

A Frame Relay redirect connection channels all inbound packets out to a Frame Relay switch as described in Chapter 4, "Configuring Frame Relay."

Block Calls After

You can specify the number of unsuccessful attempts to place a call that an Ascend unit can make before blocking further attempts to make that connection. After the specified number of attempts have been made and failed, the blocking timer starts. For detailed information about each parameter, see the *MAX Reference Guide*.

Connection profile telco options

A Connection profile has the following Telco Options parameters (shown with sample settings):

```
Ethernet
   Connections
     any Connection profile
      Telco options...
         AnsOrig=Both
         Callback=Yes
         Exp Callback=No
         Callback Delay=
         Call Type=Switched
         Group=N/A
         FT1 Caller=N/A
         Data Svc=56KR
         Force 56=N/A
         Bill #=555-1212
         Call-by-Call=N/A
         Transit #=222
         Dialout OK=No
```

For detailed information about each parameter, see the *MAX Reference Guide*. This section provides a brief overview.

AnsOrig and FTI Caller

The AnsOrig parameter specifies whether the MAX can answer incoming calls, dial out, or both. FT1 Caller specifies whether this MAX initiates calls on fractional T1 to add switched channels to a nailed MP+ connection (only one side of the connection should have this parameter set to Yes).

Callback

With Callback set to Yes, the MAX hangs up on the caller and dials back immediately, using the dial number in this profile. When you set Expect Callback to Yes, the MAX expects the far end to hang up and dial back (recommended when CLID is required on the far end unit and Ping or Telnet is in use).

Callback Delay

Callback is a feature in which Host A calls Host B, Host B disconnects the call, and then dials back to Host A. On switch types in Japan and Germany, the switch holds onto the DISCONNECT message from Host B to Host A. Since the disconnect has not been delivered, the return call is not accepted because Host A still has the connection up. The Callback Delay parameter allows you to specify a time delay until the DISCONNECT message has been delivered and to configure the callback delay on a per connection basis. You can specify a value from 0 to 60, which indicates the number of seconds for the time delay.

Call Type

The `Call Type=Switched` setting is the default. The other options are for nailed, nailed-MP+, and permanent switched connections.

A nailed connection is a permanent link that is always up as long as the physical connection persists. For a nailed connection, you must specify the group number of the nailed channels. You can even combine groups of nailed channels to create a single high-speed nailed connection. For example:

```
Call Type=Nailed
Group=3, 4
```

A nailed/MP+ connection combines nailed and switched channels. When you choose this Call Type, you need to set the FT1 Caller parameter to specify which side of the link can add switched channels. (For details about the Nailed/MP+ call type, see “Example of MP connection without BACP” on page 3-26.)

A permanent switched connection is an outbound switched call that attempts to remain up at all times. If the unit or central switch resets, or if the link terminates, the permanent switched connection attempts to restore the link at 10-second intervals, similar to the way in which the MAX maintains a nailed connection. A permanent switch connection conserves connection attempts but results in a long connection time. The combination can be cost effective for some customers. For details, see the *MAX Reference Guide*.

Data Svc

The Data Svc parameter specifies the type of data service the link uses, such as 56K or modem.

Bill #

Bill # specifies a billing number for charges incurred on the line. If appropriate, your carrier can provide a billing number that you can use to sort your bill. For example, each department might require its own billing number. The billing number can contain up to 24 characters.

Transit

The Transit # parameter specifies a string for use in the *transit network IE* for PRI line calling through an Interexchange Carrier (IEC). The default (null) causes the MAX to use any available IEC for long-distance calls. You can specify one of the following dialing prefixes:

288 (AT&T)
222 (MCI)
333 (Sprint)

This parameter does not apply to nailed connections.

Dialout OK

The Dialout OK parameter specifies whether you can use the Connection profile for dialing out on one of the MAX unit's digital modems. Only if you set Dialout OK to Yes is the local user allowed access to the immediate modem feature.

Connection profile accounting options

A Connection profile includes the following accounting parameters (shown with default or sample settings:)

```
Ethernet
   Connections
      Accounting...
         Acct Type=None
         Acct Host=N/A
         Acct Port=N/A
         Acct Timeout=N/A
         Acct Key=N/A
         Acct-ID Base=N/A
```

For detailed information about each parameter, see the *MAX Reference Guide*. This section provides a brief overview.

Acct Type

You can set Acct Type to specify whether this connection uses the default accounting setup (specified in the Ethernet profile), no accounting at all, or the user-specific setup specified here. The MAX supports both RADIUS and TACACS+ accounting.

Acct Host and Acct Port

If Acct Type specifies use of a connection-specific accounting server, set Acct Host and Acct Port to specify the IP address of the server and the UDP port number to use in accounting requests.

Acct Timeout and Acct Key

The Acct Timeout parameter specifies how long to wait for a response to a RADIUS accounting request. TACACS+ has its own timeout method.The accounting key is a shared secret (a password shared with the accounting server).

Acct-ID Base

The Acct-ID Base parameter applies to RADIUS accounting. It specifies the numeric base (base 10 or base 16) for the session ID.

Connection profile DHCP options

A Connection profile includes the following DHCP parameters (shown sample settings):

```
Ethernet
   Connections
      DHCP options...
         Reply Enabled=No
         Pool Number=N/A
         Max Leases=N/A
```

For detailed information about each parameter, see the *MAX Reference Guide*. This section provides a brief overview.

Reply Enabled

The Reply Enabled parameter is specifies whether the MAX processes DHCP packets and acts as a DHCP server on this connection. If you set the parameter to Yes and the connection is bridged, the MAX responds to all DHCP requests. If you set Reply Enabled to Yes and the connection uses routing, the MAX responds only to Network Address Translation (NAT) DHCP packets from a Pipeline unit. If you set Reply Enabled to No, the MAX does not respond to DHCP requests.

Pool Number

The Pool Number parameter specifies the IP address pool to use to assign addresses to NAT clients. It is not applicable if you set Reply Enabled to No.

Max Leases

The Max Leases parameter restricts the number of dynamic IP addresses to be given out through this connection, thus limiting the number of clients on the remote LAN who can access the Internet. This parameter is not applicable if you set Reply Enabled to No.

Name/Password profiles

Name/Password profiles provide simple name and password authentication for incoming calls. They are used only if authentication is required in the Answer profile (Recv Auth). In that case, the MAX prompts dial-in users for a name and password, matches the input to a Name/Password profile, accepts the call, and uses the settings in the Answer profile or a specified Connection profile to build the connection.

Name/Password profiles include the following parameters (shown with sample settings):

```
Ethernet
   Names / Passwords
      Name=Brian
      Active=Yes
```

```
Recv PW=brianpw
Template Connection #=0
```

Understanding the Name/Password profile parameters

This section provides some background information about Name/Password profiles. (For detailed information, see the *MAX Reference Guide*.

Name

The name must exactly match the name specified by a dial-in user, including case changes. Ascend does not recommend that you specify a name that is already in use in a Connection profile. The name can be up to 31 characters.

Active

To enable a Name/Password profile for use, set Active to Yes. If you are using a *template* Connection profile to build the session, that profile must also be active. (The Template Connection parameter specifies the template profile.)

Rec PW

Specify a password that exactly matches the one entered by the dial-in user, including case changes. The password can be up to 20 characters.

Template Connection

To use a *template* Connection profile rather than the Answer profile settings to build the session for this Name/Password profile, specify the unique portion of the profile's number here. The default of zero instructs the MAX to use the Answer profile settings. Any other number denotes a Connection profile. The specified Connection profile must be active.

Template connections can be used to enable or disable group logins. For example, you can specify a Connection profile for the Sales group to use when dialing in, then configure a Name/Password profile for each individual salesperson. You can prevent a single salesperson from dialing in by setting Active to No in the Name/Password profile, or you can prevent the entire group from logging in by setting Active to No in the Connection profile.

Example Name/Password profile configuration

To configure a Name/Password profile that uses the Answer profile settings:

1 Open a Name/Password profile.

2 Specify the user's name and password, and activate the profile. For example:

```
Ethernet
   Names / Passwords
      Name=Brian
      Active=Yes
      Recv PW=brianpw
      Template Connection #=0
```

3 Leave the Template Connection # set to **0** (zero) to use Answer profile settings.

4 Close the profile.

Note: To set up a dial-in AppleTalk PPP connection using a Name/Password profile, you also need to set the Peer parameter in the AppleTalk Options profile to Dialin.

Configuring PPP connections

A PPP connection can be one of the following types:

- PPP—a single-channel connection to any remote device running PPP software.
- Multilink PPP (MP)—a multilink connection to an MP-compliant device from any vendor.
- MP with Bandwidth Allocation Control Protocol (MP with BACP)—an MP call that uses BACP to increase or decrease bandwidth on demand.
- Multilink Protocol Plus (MP+)—a multilink connection to another Ascend unit, that uses Ascend dynamic bandwidth allocation to increase or decrease bandwidth on demand.

Note: MP+ supersedes MPP.

A multilink connection begins by authenticating a base channel. If the connection allows additional bandwidth, the local or remote unit dials another link. For example, if a dial-in Ascend Pipeline unit has a single-channel session at 56 Kbps or 64 Kbps and multilink PPP is configured, a second call can combine the first B channel with the second for a transmission rate of 112 Kbps or 128 Kbps.

MAX units can be *stacked* to distribute the bandwidth required for connections across multiple units (as described in “Configuring multichannel calls across a stack of units” on page 3-31).

Note: If a connection configured for multilink PPP fails to establish multiple channels, it falls back to a single-channel PPP session. In either case, you can use the PPP parameters as part of the connection negotiation. Use the MP, BACP, and MP+ settings *in addition to* the single-channel PPP settings.

Configuring single-channel PPP connections

This section describes how to set the parameters used for PPP negotiation for establishing a single-channel PPP call or the base channel of a multilink PPP call. Following are the related parameters (shown with sample settings):

```
Ethernet
   Answer
      Encaps...
         PPP=Yes

      PPP options...
         Route IP=Yes
         Route IPX=Yes
         Route AppleTalk=Yes
         Bridge=Yes
         Recv Auth=Either
         MRU=1524
         LQM=No
         LQM Min=600
         LQM Max=600
         Link Comp=Stac
         VJ Comp=Yes
         CBCP Enable=No
         BACP=
         Dyn Alg=
         Sec History=
         Add Pers=
         Sub Pers=


Ethernet
   Connections
    any Connection profile
      Encaps=PPP
      Encaps options...
         Send Auth=None
         Send Name=N/A
         Send PW=N/A
         Recv PW=
         MRU=1524
         LQM=No
         LQM Min=600
         LQM Max=600
         Link Comp=Stac
         VJ Comp=Yes
         CBCP Mode=N/A
         CBCP Trunk Group=N/A
         Split Code.User=N/A--not in params
```

Understanding the PPP parameters

This section provides some background information about the PPP parameters. For detailed information about each parameter, see the *MAX Reference Guide*.

Routing and bridging parameters

You must enable routing or bridging in the Answer profile for the MAX to pass the data stream from an answered call to its internal bridge/router software.

Revc Auth and Send Auth

The Recv Auth parameter specifies the protocol to use for authenticating the password sent by the far end during PPP negotiation. You can specify None, PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MS-CHAP (Microsoft Challenge Handshake Authentication Protocol format supported by Windows NT systems), or Either. The Either setting allows any of the above.The far end must also support the specified protocol. In the Connection profile's Encaps Options subprofile, the Send Auth parameter specifies that protocol to use for the password sent to the far end during PPP negotiation.

Send PW and Recv PW

In the Connection's profile's Encaps Options subprofile, the Send PW parameter is the password sent to the remote device. It must match the password expected from the MAX. The Recv PW is the password sent to the MAX from the remote device. It is used to match up the caller to a profile when IP routing is not in use.

Send Name

The Send Name parameter specifies the name that the MAX sends to the far-end device during PPP authentication. Authentication fails if the name does not match what the far-end device expects. Also, authentication fails if either the password or IP address (for IP-routed connections) for the Connection profile does not match what the far-end device expects. You can specify up to 16 characters. The default is null.

Maximum receive units (MRU)

In the Answer's profiles's PPP Options, the MRU parameter specifies the maximum number of bytes the MAX can receive in a single packet on a PPP link. Usually the default of 1524 is the right setting, unless the far end device requires a lower number.

Link quality monitoring (LQM)

The LQM parameters specify whether the MAX monitors the quality of the link. If LQM is set to Yes, you can specify the minimum and maximum duration between reports, measured in tenths of a second.

LQM counts the number of packets sent across the link and periodically asks the remote end how many packets it has received. Discrepancies are evidence of packet loss and indicate link quality problems.

For a connection that has a Connection profile, that profile's LQM settings take precedence over the LQM settings in the Answer profile.

Link Comp and VJ Comp

In the Answer profile and in Connection profiles, the Link Comp parameter specifies the type of link compression for the connection, and VJ Comp specifies the type of TCP/IP header compression.

For data compression to take effect, both sides of a connection must support it. The MAX supports Stac and MS-Stac compression for PPP-encapsulated calls.

Stac compression refers to the Stacker LZS compression algorithm, developed by STAC Electronics, Inc., that modifies the standard LZS compression algorithm to optimize for speed (as opposed to optimizing for compression). Stac compression is one of the parameters negotiated when setting up a PPP connection.

MS-Stac refers to Microsoft LZS Coherency compression for Windows 95. This is a proprietary compression scheme for Windows 95 only (not for Windows NT).

Note: If the caller requests MS-Stac and the matching profile does not specify MS-Stac compression, the connection seems to come up correctly but no data is routed. If the profile is configured with MS-Stac and the caller does not acknowledge that compression scheme, the MAX attempts to use standard Stac compression, and if that does not work, it uses no compression.

On a related topic, Novell's NetWare relies on the Data Link layer (also called Layer 2) to validate and guarantee data integrity. STAC link compression, if specified, generates an eight-bit checksum, which is inadequate for NetWare data.

If your MAX supports NetWare (either routed or bridged), and you require link compression, you should configure your MAX in one of the following ways:

- Configure either STAC-9 or MS-STAC link compression, which use a more robust error-checking method, for any connection profile supporting IPX data. Configure link compression in the Ethernet > Answer > PPP Options > Link Comp parameter and Ethernet > Connections > *Any Connection profile* > Encaps Options > Link Comp parameter.
- Enable IPX-checksums on your NetWare servers and clients. (Both server and client must support IPX-checksums. If you enable checksums on your servers but your clients do not support checksums, they will fail to log in successfully.)
- Disable link compression completely by setting Ethernet > Answer > PPP Options > Link Comp = None and Ethernet > Connections > *Any Connection profile* > Encaps Options > Link Comp = None. By disabling link compression, the MAX validates and guarantees data integrity by means of PPP.

VJ Comp applies only to packets in TCP applications, such as Telnet. When you turn it on, the MAX applies TCP/IP header compression for both ends of the link.

CBCP Enable

The Answer profile's CBCP Enable parameter specifies how the MAX responds to caller requests to support CBCP (Callback Control Protocol). If CBCP Enable is set to Yes, the MAX positively acknowledges, during LCP negotiations, support for CBCP. If this parameter is set to No, the MAX rejects any request to support CBCP. (For more information about CBCP, see "Microsoft's Callback Control Protocol (CBCP)" in Chapter 3 of the *MAX Security Supplement*.)

CBCP Mode

The (Connection profile) CBCP mode parameter specifies what method of callback the MAX offers the incoming caller.

CBCP Trunk Group

The (Connection profile) CBCP Trunk Group parameter assigns the callback to a MAX trunk group. This parameter is used only when the caller is specifying the phone number the MAX uses for the callback. The value in CBCP Trunk Group is prepended to the caller-supplied number when the MAX calls back.

BACP

The BACP parameter enables the Bandwidth Allocation Control Protocol. The MAX encapsulates connections in MP (RFC 1990) and uses BACP to manage dynamic bandwidth on demand. Both sides of the connection must support BACP. BACP uses the same criteria for managing bandwidth dynamically as MP+ connections. Specify either Yes to enable BACP or No to disable BACP. No is the default.

Dyn Alg

The Dyn Alg parameter specifies the algorithm that the MAX uses to calculate average line utilization (ALU). You can specify one of the following values:

- Quadratic—Specifies that the MAX gives preference to recent samples of bandwidth usage than to older samples taken in the number of seconds specified in Sec History. The preference grows at a quadratic rate. The default is Quadratic.
- Linear—Specifies that the MAX gives preference to recent samples of bandwidth usage than to older samples taken in the number of seconds specified in Sec History. The weighting grows at a linear rate.
- Constant—Specifies that the MAX does not give greater preference to recent samples.

Sec History

The Sec History parameter specifies a number of seconds to use as the basis for calculating average line utilization (ALU). The ALU is used in calculating when to add or subtract bandwidth from a multi-channel call that supports dynamic bandwidth management.

Add Pers

The Add Pers parameter specifies the number of seconds that a call must maintain Average Line Utilization (ALU) above the target utilization threshold you specified in Target Util before the MAX adds bandwidth from available channels. When adding bandwidth, the MAX adds the number of channels that you specify in the Inc Ch Count parameter. You can specify a number from 1 to 300. The default for MP+ calls is 5. The default for AIM calls with dynamic call management is 20.

Sub Pers

The Sub Pers parameter specifies a number of seconds that a connection maintains an Average Link Utilization (ALU) equal to (or less than) the Target Util threshold before the MAX subtracts bandwidth.

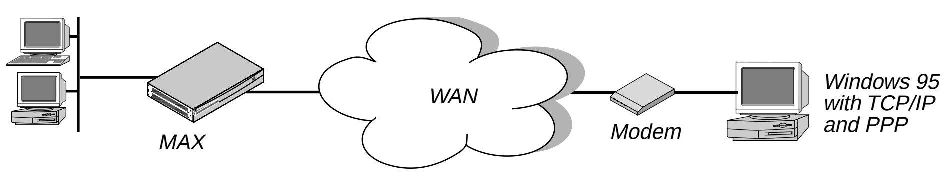
Split Code.User

The Split Code.User parameter divides the PIN and CODE of a user and their USERNAME by a period. If the CHAP field cannot accommodate the full PIN+CODE.USER, you can enable this feature. The MAX splits the passcode into two pieces with the information following the period becoming the CHAP Name, overriding the name of the router. You can specify Yes, to enable the PIN, CODE and USERNAME to be divided, or you can specify No to disable the feature. No is the default.

Example of a PPP connection

Figure 3-1 shows the MAX with a PPP connection with a remote user who is running Windows 95 with the TCP/IP stack and PPP dialup software. The dial-in user has a modem, so the call is asynchronous and uses only one channel.

Figure 3-1. A PPP connection



To configure this PPP connection:

1 Make sure the Answer profile enables PPP encapsulation and has the appropriate routing, bridging, and authentication settings. For example:

```
Ethernet
   Answer
      Encaps...
         PPP=Yes

      PPP options...
         Route IP=Yes
         Route IPX=Yes
         Bridge=Yes
         Recv Auth=Either
```

2. Close the Answer profile.
3. Open a Connection profile.
4. Specify the name of the remote device and activate the profile. For example:

```
Ethernet
   Connections
      Station=tommy
      Active=Yes
```

Note: Make sure that you specify the Station name exactly, including case changes.

5. Select PPP encapsulation and set the appropriate PPP options. For example:

```
      Encaps=PPP
      Encaps options...
         Send Auth=CHAP
         Send PW=remotepw/A
         Recv PW=localpw
```

The Send Auth parameter should be set to CHAP or PAP. Both sides of the connection must support the selected authentication protocol and the selected compression methods.

6. Close the Connection profile.

Enabling PPP dial-out for V.110 modems

The MAX can make outgoing calls to a v.110 terminal-adapter client, using the PPP protocol. This feature also supports the callback feature via V.110 for the MAX Link Client software product.

For information about enabling dial-out that uses the MAX unit's digital modems, see "Configuring dial-out options" on page 3-66.

To enable PPP dial-out for V.110 modems:

1. Open a Connection profile configured for async PPP.
2. Open the Telco Options subprofile and specify the following data service:

```
Ethernet
   Connections
      Telco options...
         Data Svc=v110 19.2 56K
```

3. Close the Connection profile.

In the Data Svc settings, `v110` is the V110, which tells the MAX to communicate with a V.110 terminal-adapter (through the V.100 modems.) The other two settings are the bit rate for the connection and the data service to use, respectively.

```
v110 19.2 56k
```

In this case, the connection to the remote terminal adapter (TA) uses a bit rate of 19.2 Kbps over a line using the Switched-56 data service. If the MAX cannot sync up with the remote TA at the specified bit rate, it attempts to use one of the other bit rates. For more detailed information about the Data Svc parameter, see the *MAX Reference Guide*.

.

Configuring MP and BACP connections

Multilink PPP (MP) uses the encapsulation defined in RFC 1717. It enables the MAX to interact with MP-compliant equipment from other vendors to use multiple channels for a call. MP parameters include the PPP parameters described in "Understanding the PPP parameters" on page 3-18. MP without Bandwidth Allocation Control Protocol (BACP) requires setting a few additional parameters. If you use MP with BACP, you have to set a number of additional parameters. Following are the additional parameters requires for MP with BACP:

```
Ethernet
   Answer
      Encaps...
         MP=Yes
         PPP=Yes

      PPP options...
         Min Ch Count=1
         Max Ch Count=1

Ethernet
   Connections
     any Connection profile
       Encaps=MP
       Encaps options...
         Base Ch Count=1
```

If BACP is enabled, MP connections use that protocol to manage dynamic bandwidth on demand. Both sides of the connection must support BACP. In addition to the PPP parameters, MP connections with BACP use the following parameters:

```
Ethernet
   Answer
      Encaps...
         MP=Yes
         PPP=Yes

      PPP options...
         BACP=Yes
         Dyn Alg=Quadratic
         Sec History=15
         Add Pers=5
         Sub Pers=10
         Min Ch Count=1
         Max Ch Count=1
         Target Util=70

Ethernet
   Connections
     any Connection profile
       Encaps=MP
       Encaps options...
         BACP=Yes
         Base Ch Count=1
         Min Ch Count=1
         Max Ch Count=2
         Inc Ch Count=1
         Dec Ch Count=1
         Dyn Alg=Quadratic
         Sec History=15
```

```
Add Pers=5
Sub Pers=10
Target Util=70
```

Understanding the MP and BACP parameters

This section provides some background information about MP and BACP configuration. For detailed information about each parameter, see the *MAX Reference Guide*.

MP without BACP

For MP connections without BACP, you can specify the base channel count, which must be greater than or equal to the minimum count and less than or equal to the maximum count specified in the Answer profile. The base channel count specifies the number of channels to use to establish the connection, and this number of channels remains fixed for the whole session. You can ignore the rest of the parameters discussed in this section.

Enabling BACP for MP connections

Enable BACP in the Answer profile and the Connection profile for each connection that should use it. Open the PPP Options subprofile from the Answer profile and set BACP to Yes. Open the Encaps Options subprofile from the Answer profile and set BACP to Yes. Both sides of the connection must support BACP.

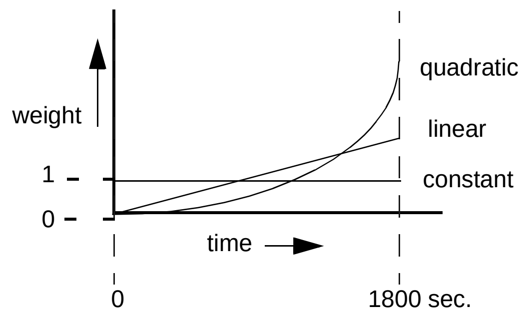
Specifying channel counts

In a Connection profile's Encaps Options subprofile, the base channel count specifies the number of channels to use to establish the call. After the base channel or channels have been established, adding another channel requires dealing another link. Inc Ch Count and Dec Ch Count specify the number of channels the connection can add and subtract at one time, respectively. You can also specify a maximum and minimum number of channels that can be allocated to the call. For additional information, see Parallel Dial in the System profile.

Dynamic algorithm for calculating bandwidth requirements

In an Encaps Options subprofile, the Dyn Alg parameter specifies an algorithm for calculating average line utilization (ALU) during the period specified, in seconds, by the Sec History parameter. Figure 3-2 shows how the available algorithms weight usage samples.

Figure 3-2. Algorithms for weighing bandwidth usage samples



Quadratic (the default) gives more weight to recent samples of bandwidth usage than to older samples taken during the specified period. The weighting grows at a quadratic rate.

Linear gives more weight to recent samples of bandwidth usage than to older samples taken during the specified period. The weighting grows at a linear rate.

Constant gives equal weight to all samples taken during the specified period.

Time period for calculating average line utilization

Sec History specifies a number of seconds to use as the basis for calculating average line utilization (ALU).

Target utilization

Target Util specifies a percentage of line utilization (default 70%) to use as a threshold when determining when to add or subtract bandwidth.

Adding or dropping links (Add Pers)

Add Pers specifies a number of seconds that the ALU must persist beyond the Target Util threshold before the MAX adds bandwidth. Sub Pers specifies a number of seconds that the ALU must persist below the Target Util threshold before the MAX subtracts bandwidth. When adding bandwidth, the MAX adds the number of channels specified in the Inc Ch Count parameter. When subtracting bandwidth, it subtracts the number of channels specified in the Dec Ch Count parameter, dropping the newest channels first.

Guidelines for configuring bandwidth criteria

When configuring dynamic bandwidth allocation, keep the following guidelines in mind:

- The values for the Sec History, Add Pers, and Sub Pers parameters should smooth out spikes in bandwidth utilization that last for a shorter time than it takes to add capacity. Over T1 lines, the MAX can add bandwidth in less than ten seconds. Over ISDN lines, the MAX can add bandwidth in less than five seconds.
- When the MAX adds bandwidth, you typically incur a minimum usage charge. Thereafter, billing is time sensitive. The Sub Pers value should allow the period to which the

minimum duration charge applies plus one or two billing time increments. Typically, billing is done to the next multiple of six seconds, with a minimum charge for the first thirty seconds. Your carrier representative can help you understand the billing structure for the switched tariffs.

- You can add channels one at a time or in multiples. (For additional information, see the Parallel Dial parameter).
- Avoid adding or subtracting channels too quickly (less than 10-20 seconds apart) to reduce the number of short duration calls, each of which incurs the carrier's minimum charge. Adding or subtracting channels too quickly can also affect link efficiency, because the devices on either end have to retransmit data when the link speed changes.

Example of MP connection without BACP

To configure an MP connection without BACP:

1 Open the Answer profile.

2 Enable PPP and MP encapsulation and specify the appropriate routing, bridging, and authentication values. For example:

```
Ethernet
   Answer
      Encaps...
         PPP=Yes
         MP=Yes

      PPP options...
         Route IP=Yes
         Route IPX=Yes
         Bridge=Yes
         Recv Auth=Either
```

3 Close the Answer profile.

4 Open a Connection profile, specify the name of the remote device, and activate the profile. For example:

```
Ethernet
   Connections
      Station=ted
      Active=Yes
```

5 Select MP encapsulation, and open the Encaps Options subprofile.

6 Configure PPP authentication. For example:

```
      Encaps=MP
      Encaps options...
         Send Auth=PAP
         Send PW=remotepw
         Aux Send PW=N/A
         Recv PW=localpw
```

7 Set the base channel count. For example, to use two channels for this call:

```
         Base Ch Count=2
```

Note: Both sides of the connection should specify the same number of channels.

8 Close the Connection profile.

Example MP connection with BACP

To configure an MP connection that uses BACP:

1 Open the Answer profile.

2 Enable PPP and MP encapsulation and specify the appropriate routing, bridging, and authentication values. For example:

```
Ethernet
   Answer
      Encaps...
         MP=Yes
         PPP=Yes

      PPP options...
         Route IP=Yes
         Route IPX=Yes
         Bridge=Yes
         Recv Auth=Either
```

3 Enable BACP to monitor bandwidth requirements on the basis of received packets:

```
         BACP=Yes
```

4 Close the Answer profile.

5 Open a Connection profile, specify the name of the remote device, and activate the profile. For example:

```
Ethernet
   Connections
      Station=clara
      Active=Yes
```

6 Select MP encapsulation and set the MP authentication options. For example:

```
      Encaps=MP
      Encaps options...
         Send Auth=PAP
         Send PW=remotepw
         Aux Send PW=N/A
         Recv PW=localpw
```

7 Enable BACP to monitor bandwidth requirements for packets transmitted on this connection, and configure the Ascend criteria for bandwidth management. For example:

```
         BACP=Yes
         Base Ch Count=1
         Min Ch Count=1
         Max Ch Count=2
         Inc Ch Count=1
         Dec Ch Count=1
         Dyn Alg=Quadratic
         Sec History=15
         Add Pers=5
         Sub Pers=10
         Target Util=70
```

Note: For optimum performance, both sides of a connection must set the channel count parameters to the same values.

8 Close the Connection profile.

Configuring Ascend MP+ connections

Multilink PPP Plus (MP+) uses PPP encapsulation with Ascend extensions. MP+ enables the MAX to use multiple channels for connecting to another Ascend unit. BACP is not required, because the Ascend criteria for adding or dropping a link are part of the MP+ extensions. In addition to the PPP and MP parameters described earlier use the following parameters for MP+ connections: shown with sample settings):

```
Ethernet
   Answer
      Encaps...
         PPP=Yes
         MP=Yes
         MPP=Yes

      PPP options...
         Dyn Alg=Quadratic
         Sec History=15
         Add Pers=5
         Sub Pers=10
         Min Ch Count=1
         Max Ch Count=1
         Target Util=70
         Idle Pct=0

Ethernet
   Connections
     any Connection profile
       Encaps=MPP
       Encaps options...
         Aux Send PW=aux-passwd
         DBA Monitor=Transmit
         Base Ch Count=1
         Min Ch Count=1
         Max Ch Count=2
         Inc Ch Count=1
         Dec Ch Count=1
         Dyn Alg=Quadratic
         Sec History=15
         Add Pers=5
         Sub Pers=10
         Target Util=70
         Idle Pct=0
```

Understanding the MP+ parameters

This section provides some background information about MP+ connections. For detailed information about each parameter, see the *MAX Reference Guide*.

Channel counts and bandwidth allocation parameters

BACP and MP+ use the same criteria for increasing or decreasing bandwidth for a connection. For details about the bandwidth allocation parameters, see “Understanding the MP and BACP parameters” on page 3-24 and “Guidelines for configuring bandwidth criteria” on page 3-25.

Auxiliary password for added channels

The Aux Send PW parameter can specify another password for authenticating subsequent links as they are dialed. For details, see the MAX *Security Supplement* for details.

Bandwidth monitoring

In a Connection profile's Encaps Options subprofile, the DBA Monitor parameter specifies whether bandwidth criteria for adding or dropping links are applied to traffic received across the link, transmitted across the link, or both. If you set DBA Monitor to None on both sides of the link, you disable bandwidth on demand.

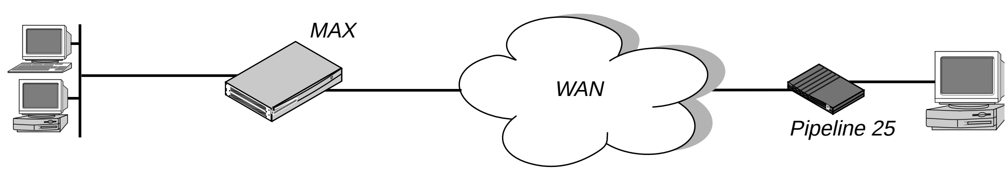
Idle percent

Idle Pct specifies a percentage of utilization below which the MAX drops all channels, including the base channel. Bandwidth utilization must fall below this percentage on *both sides* of the connection before the MAX drops the link. If the device at the remote end of the link enters an Idle Pct setting lower than the value you specify, the MAX does not clear the call until bandwidth utilization falls below the lower percentage. The default value for Idle Pct is 0, causing the MAX to ignore bandwidth utilization when determining whether to clear a call and use the Idle timer instead.

Example of MP+ configuration

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

Figure 3-3. An MP+ connection



To configure an MP+ connection with a remote Ascend unit:

1. Open the Answer profile.
2. Set PPP and MP+ encapsulation to Yes and specify the appropriate routing, bridging, and authentication values. For example:

```
Ethernet
   Answer
      Encaps...
         MPP=Yes
         PPP=Yes

      PPP options...
         Route IP=Yes
         Route IPX=Yes
         Bridge=Yes
         Recv Auth=Either
```

3. Close the Answer profile.

4 Open a Connection profile, specify the name of the remote device, and activate the profile. For example:

```
Ethernet
   Connections
      Station=richard
      Active=Yes
```

5 Select MP+ encapsulation and set the MP+ authentication options. For example:

```
      Encaps=MPP
      Encaps options...
         Send Auth=PAP
         Send PW=remotepw
         Aux Send PW=secondpw
         Recv PW=localpw
```

6 Configure the DBA Monitor and the Ascend criteria for bandwidth management. For example:

```
      Encaps options...
         DBA Monitor=Transmit-Recv
         Base Ch Count=1
         Min Ch Count=1
         Max Ch Count=5
         Inc Ch Count=1
         Dec Ch Count=1
         Dyn Alg=Quadratic
         Sec History=15
         Add Pers=5
         Sub Pers=10
         Target Util=70
         Idle Pct=0
```

Note: For optimum performance, both sides of a connection must set the Base Ch Count, Min Ch Count, and Max Ch Count parameters to the same values.

7 Close the Connection profile.

Configuring a nailed MP+ connection

A Nailed/MP+ connection is a nailed connection that can add switched channels for increased bandwidth. The MAX dials switched channels when it receives an outbound packet for the far end and cannot forward it across the nailed connection, either because those channels are down or because they are being fully utilized.

If both the nailed and switched channels in a Nailed/MP+ connection are down, the connection does not reestablish itself until the nailed channels are brought back up or you dial the switched channels.

The maximum number of channels for the Nailed/MP+ connection is either the Max Ch Count setting or the number of nailed channels in the specified group, whichever is greater. If a nailed channel fails, MAX replaces that channel with a switched channel, even if the call is online with more than the minimum number of channels.

Note: If you modify a Nailed/MP+ Connection profile, most changes become active only after the call is brought down and then back up. However, if you add a group number (for example, changing Group=1,2 to Group=1,2,5) and save the modified profile, the MAX adds the additional channels to the connection without having to bring it down and back up.

To configure a Nailed/MP+ connection:

1 Configure an MP+ connection, as described in the preceding section.

2 Open the Telco Options subprofile of the Connection profile.

3 Specify that the MAX is the designated caller for the switched part of the connection.

```
Ethernet
   Connections
      Telco options...
         AnsOrig=Call Only
         FT1 Caller=Yes
```

Note: On the far end of the connection, set the AnsOrig and FT1 Caller parameters for answering only. Note that the DO Hangup command only works from the caller end of the connection.

4 Specify the Nailed/MP+ call type, and the group number(s) of its nailed channels. For example:

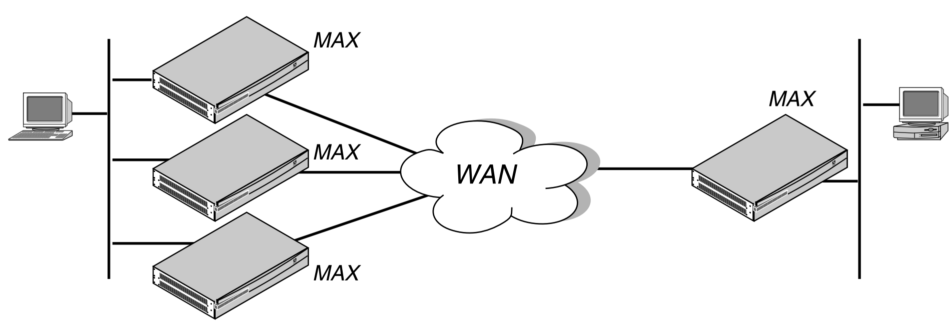
```
         Call Type=Nailed/MPP
         Group=1,2
```

5 Close the Connection profile.

Configuring multichannel calls across a stack of units

If you configure multiple MAX units to form a stack, the multiple channels of a Multilink PPP (MP) or MP+ call can to span (be distributed across) the units in the stack, as shown in “A MAX stack for spanning multilink PPP calls (MP) or MP+” on page 3-31.

Figure 3-4. A MAX stack for spanning multilink PPP calls (MP) or MP+



Call spanning with a stack configuration can be effective when:

- A MAX running MP+ asks for another phone number, and has no available lines.
- A rotary hunt group uses the same phone number to access multiple MAX units, making it impossible to assume that the same MAX that answered the original call answers a subsequent call.

MP/MP+ call spanning is protocol independent and works with all protocols supported by the MAX.

Note: Stacking requires any MP caller to use the MP endpoint discriminator. The same is true of MP+. All Ascend products and most other products that support MP or MP+ use an endpoint discriminator, but the specification for MP does not require it.

How MP/MP+ call spanning works

A stack is a group of MAX units that have the same stack information and are on the same physical LAN. There is no *master* MAX. The MAX units in the stack use a directed-broadcast Ethernet packet to locate each other.

Directed-broadcast packets usually cannot cross a router, so the MAX units in a single stack must be on the same physical LAN. MAX units running in a stack can generate fairly high levels of network traffic which is another reason to keep them on the same physical LAN.

Bundle ownership

Although MAX stacks do not have a master MAX, each bundle of channels in a MP/MP+ configuration has a bundle owner. The MAX that answers the first call in the MP/MP+ bundle is the *bundle owner*. If a bundle spans more than one MAX in a stack, an exchange of information flows between the MAX units in the bundle.

Stacking requires an endpoint discriminator. Every MP/MP+ call that comes to any member of the stack is compared to all existing MP/MP+ calls in the MAX stack to determine whether it is a member of an existing bundle. If the call belongs to an existing bundle, the MAX that answered and the bundle owner exchange information about the bundle. Furthermore, the MAX that answered the call forwards all incoming data packets over the Ethernet to the bundle owner.

Outgoing data

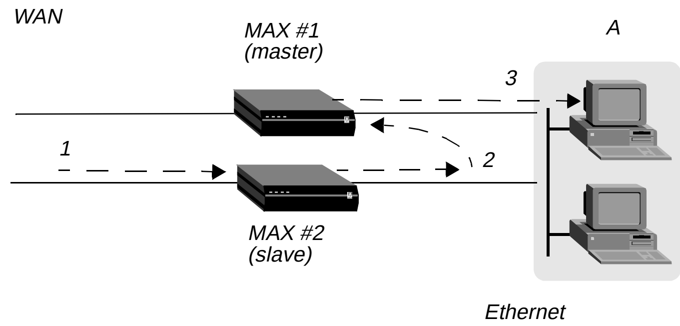
To balance the load among all available WAN channels, outgoing data packets for the WAN are assigned to available channels in a bundle on a rotating basis. If the MAX assigns an outgoing packet to a channel that is not local to the bundle owner, the bundle owner forwards the packet over the Ethernet to the MAX that owns the nonlocal channel.

Real and stacked channels

For the purpose of this description, *real* channels are those channels that connect directly to the MAX that owns the bundle. *Stacked* channels connect to a MAX that transfers the data to or from the MAX that owns the bundle.

For example, assume the initial call through an MP/MP+ bundle connects to MAX #1. This connection is a *real* channel. Next, the second call of the bundle connects to MAX #2. This connection is a *stacked* channel. MAX #1 is the bundle owner, and it manages the traffic for both channels of the bundle. MAX #2 forwards any traffic from the WAN to MAX #1, for distribution to the destination as shown in Figure 3-5.

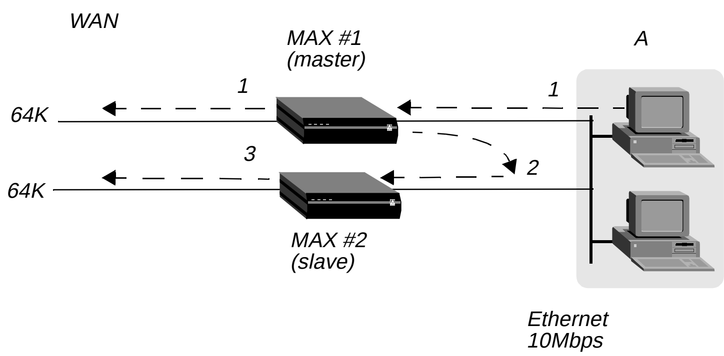
Figure 3-5. Packet flow from the slave channel to the Ethernet



Note: Figure 3-6 does not illustrate traffic from the master MAX. WAN traffic received on the master channel by MAX #1 is forwarded directly to the destination.

Likewise, MAX#1 receives all Ethernet traffic destined for the bundle, and disperses the packets between itself and MAX #2, as shown in Figure 3-6. MAX #1 forwards some of the packets across the WAN through a real channel. MAX #2 sends the rest of them through a stacked channel.

Figure 3-6. Packet flow from the Ethernet



Connection profiles within a stack

A stack does not support sharing of local Connection profiles between the MAX units in the stack. Every MAX that is set up to use internal authentication must retain all authentication information for every call. You can eliminate this requirement by using a centralized authentication server, such as RADIUS.

Phone numbers for new MP+ and MP-with-BACP channels

When a MAX has to add a channel for an MP+ or MP-with-BACP call, it provides a local phone number for the new channel. However, sometimes the MAX that answers the call cannot provide a local phone number for the additional channel because all the channels that connect directly to it are busy. In that case, the MAX requests other members of the stack to supply a phone number for the additional channel.

An MP call does not pass phone numbers when it adds a channel. The originator of the call must know all of the possible phone numbers to begin with.

If each MAX in the stack is accessed through a different phone number, the originator of the call must know all of the possible phone numbers. An alternative in this instance is to use BACP or MP+ to obtain the phone number of a MAX with a free channel.

Performance considerations for MAX stacking

There is no limit to the number of *stacked* channels in single call or in a stack of MAX units, other than the limit for each individual MAX. The MAX 6000, MAX 4000, MAX 2000, and MAX 1800 each support up to 40 stacked channels. The MAX 800 and the MAX 200 Plus support up to three stacked channels. A MAX that can handle *n* real channels can handle *n*/3 stacked channels.

There is no theoretical limit to the number of MAX units in a stack, other than performance considerations. Because all data from stacked channels crosses the LAN, performance could suffer with a large number of MAX units in the stack and many stacked channels in use.

Performance overhead increases when stacked bundles span multiple boxes. In a bundle of 6 channels, 4 of which are real and 2 are stacked, the overhead is the actual bandwidth of the two stacked channels (2 x 64 = 128K). The actual payload data of the 6 channels with a 2:1 data compression is 6 x 2 x 64 = 768K. The overhead is 128 over 768, or 16%. In a two-channel bundle with one real and one stacked channel, with the same compression, the overhead is 25%.

Take into account that you do not know ahead of time how many bundles span the stack, or how many multi- or single-channel calls you are going to get. You can base an estimate on your traffic expectations. But in most situations, the majority of bundles are on a single MAX, for which there is no overhead.

Suggested LAN configurations

Total Ethernet usage is approximately 5116Kbps for a MAX stack handling 82 single-channel calls, 41 two-channel stacked calls, and 41 two-channel nonstacked calls. Because Ethernet capacity generally does not achieve more than 50% utilization, this configuration uses up the available Ethernet bandwidth.

The total number of channels in this configuration is 246. Therefore, a stack of three MAX units, each having three T1 lines with this usage profile, uses all of the Ethernet bandwidth.

The basic limitation from the above examples is the speed of the LAN. One way to increase the speed of your LAN is to attach each MAX to a separate port of a 10/100 Ethernet switch, then use a 100Mbps connection to the backbone LAN. This configuration enables each MAX to utilize up to a full 10Mbps Ethernet bandwidth, and the entire stack combined can generate up to full 100Mbps of Ethernet data. Once again assuming that the 100Mpbs is saturated at 50% usage, you can use up to 51200Kbps of bandwidth, or 10 times more than in the preceding example. The mixed environment of single-channel and two-channel calls now results in a maximum of 2460 channels or 102 T1 lines, or no more than 34 MAX units in a stack. Note that the success of this strategy depends on limiting stacked channels per MAX to the n/3 limit mentioned above.

Suggested hunt group configurations

Whenever you stack MAX units, it is important to limit the number of multichannel calls that are split between the MAX units. The following suggested configurations reduce the overhead for a multichannel call by keeping as many channels as possible on the same MAX.

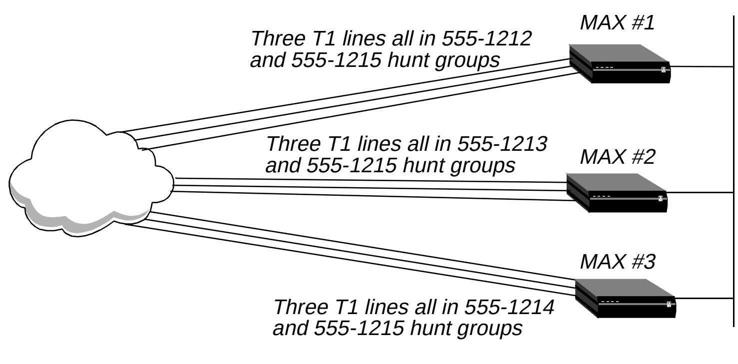
MP+ (MPP)and MP-with-BACP calls

Figure 3-7 shows the suggested hunt group setup for a typical MAX stack that receives only PPP, MP+, or MP-with-BACP calls. Each MAX has three T1 lines. All the T1 lines in a MAX share a common phone number and they are in a hunt group that does not span MAX units. The illustration shows these three local hunt groups with phone numbers 555-1212, 555-1213, 555-1214. In addition, a global hunt group, 555-1215 spans all the T1s of all the MAX units in the stack.

Users that access the MAX dial 555-1215, the global hunt group number. The telephone company sets up the global hunt group to distribute incoming calls equally among the MAX units. Namely, the first call dialing 555-1215 goes to MAX #1, the second call to MAX #2, and so on. If you use this configuration, you must configure each of the MAX unit's Line *N* profiles with the local hunt group numbers. For example, for MAX #1 in Figure 3-7, you would set the Ch *N* # parameters to 12 (the last two digits of the 555-1212 hunt group number).

You can achieve the same distribution without a global hunt group by having one third of the users dial 555-1212, one third dial 555-1213, and one third dial 555-1214. You can leave the Ch *N* # parameters at their default setting (null) if you do not have a global hunt group.

Figure 3-7. Hunt groups for a MAX stack handling both MP and MP+ calls (MAX 6000)



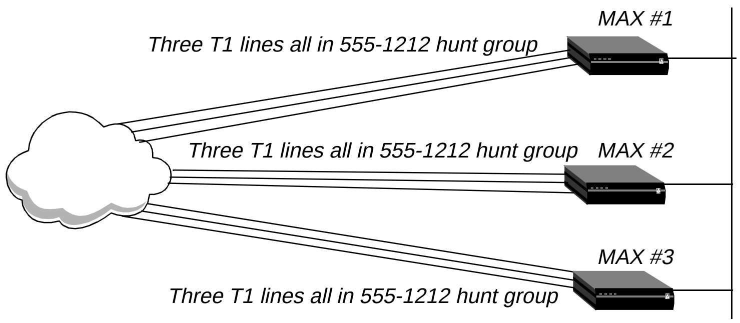
In Figure 3-7, which uses a MAX 6000 as an example, suppose an MP+ call is connected to MAX #1. When that call needs to add a channel, it requests an add-on number from the MAX, and the MAX returns *12* (for 555-1212) as long as a channel in the local T1 lines is available. That is, the bundle does not span multiple MAX units as long as a channel is available in the local hunt group.

The Figure 3-7 configuration tends to break down if MAX units receive MP-without-BACP calls. Spreading the calls across the MAX stack (by dialing the global hunt group) results in the worst possible performance, because MP-without-BACP must know all of the phone numbers before the caller places the first call.

MP-without-BACP calls

Figure 3-8, using a MAX 6000 as an example, shows a site that supports only MP-without-BACP calls. For this site, the telephone company has set up a global hunt group that first completely fills MAX #1, then continues to MAX #2, and so on. This arrangement tends to keep the channels of a call from being split across multiple MAX units, keeping overhead low.

Figure 3-8. Hunt groups for a MAX stack handling only MP-without-BACP calls (MAX 6000)



MP+ calls and MP calls with or without BACP

For a MAX that receives MP+ calls and MP calls with or without BACP, you can use a configuration similar to the one shown in Figure 3-7. In this case, however, you set up the global hunt group differently than explained in “MP+ (MPP)and MP-with-BACP calls.” You set up the global hunt group to help prevent MP-without-BACP calls from being split across multiple MAX units in the stack. As in “MP-without-BACP calls,” calls dialing 555-1215 first completely fill the channels of MAX #1, then continue to MAX #2, and so on.

Both MP+ and MP callers dial the global hunt group number to connect to the stack. “MP-without-BACP calls” on page 3-36 and “MP+ calls and MP calls with or without BACP” on page 3-36 explain how the MAX adds channels to MP+ and MP bundles. Be sure to set the Ch *N* # parameters as explained in “MP+ calls and MP calls with or without BACP” on page 3-36.

MP+ and MP-with-BACP callers do not have to dial the global hunt group numbers to connect. Only the MP-without-BACP callers need to dial the global hunt group. You can achieve an even distribution of MP+ and MP-with-BACP calls by having one third dial 555-1212, one third dial 555-1213, and one third dial 555-1214. You can leave the Ch *N* # parameters at their default setting (null) in this situation.

Understanding the stack parameters

This section provides some background information about the stack parameters. For complete details, see the *MAX Reference Guide*.

Stacking Enabled

The Stacking Enabled parameter enables the MAX to communicate with other members of the same stack. A MAX can belong to only one stack. All members of the stack use the same stack name and UDP port.

Stack Name

The Stack Name parameter specifies a stack name. Add a MAX to an existing stack by specifying that name. Create a new stack by specifying a new stack name.

UDP Port

Stacked MAX units communicate with other members of the stack by using a directed-broadcast Ethernet packet on the specified UDP port. Because directed-broadcast packets are unlikely to cross a router, and because of the high traffic demands created by a multilink call that spans MAX units, all members of a stack must reside on the same physical LAN.

For detailed information about each parameter, see the *MAX Reference Guide*.

Configuring a MAX stack

This section shows how to configure a stack of two MAX units. It does not show the details of configuring hunt groups, which is an important factor for stacked MP connections. For details about hunt groups, see Chapter 2, "Configuring the MAX for WAN Access."

To configure a MAX stack, proceed as follows for each MAX in the stack:

1 Open the Ethernet > Mod Config menu and select Stack Options, as shown in the following sample menu:

```
90-A** Mod Config
 RADIUS Server
 Log
 ATMP
 Modem Ringback=Yes
 AppleTalk
 SNTP Server
 >Stack Options...
 UDP Checksum=No
```

When you press Enter, the Ethernet > Mod Config > Stack Options menu appears. For example:

```
90-A** Mod Config
>Stack Options...
Stacking Enabled=Yes
Stack Name=maxstack-1
UDP Port=6000
```

2 Set Stacking Enabled to Yes (Stacking Enabled=Yes).

3 Set the Stack Name parameter to a unique name for the stack.

A stack name has 16 characters or less. This is the name members of a stack use to identify other members of the same stack. The stack name must be unique among all MAX units that communicate with each other, even if they are not on the same LAN.

If a MAX receives calls from two MAX units on different LANs, and the two units are members of different stacks with the same stack name, the MAX receiving the calls assumes the two MAX units with the same stack name are in the same bundle.

Note: Multiple stacks can exist on the same physical Ethernet LAN if the stacks have different names.

4 Specify the UDP port.

This is a reserved UDP port for intrastack communications. The UDP port must be identical for all members of a stack, but is not required to be unique among all stacks.

Disabling a MAX stack

To disable a stack, specify Stacking Enabled=No for each of the MAX units in the stack.

Adding and removing a MAX

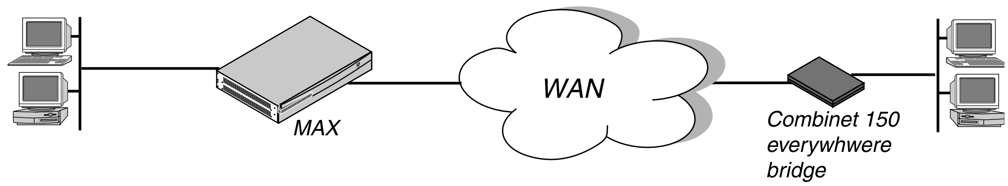
You can add a MAX to an existing stack at any time without rebooting the MAX or affecting stack operation. Because a stack is a collection of peers, none keeps a list of the stack membership. The MAX units in a stack communicate when they need a service from the stack.

Removing a MAX from a stack requires care, because any calls using a channel between the MAX to be removed and another MAX in the stack could be dropped. There is no need to reboot a MAX removed from a stack.

Configuring a Combinet connection

The MAX supports Combinet bridging to link two LANs as if they were one segment. For a Combinet connection to work, bridging must be enabled at the system level (as described in Chapter 8, "Configuring Packet Bridging.") Figure 3-9 shows a Combinet connection.

Figure 3-9. A Combinet connection



Combinet configuration involves the following parameters (shown with sample settings):

```
Ethernet
   Mod Config
      Bridging=Yes

Ethernet
   Answer
      Encaps...
         COMB=Yes

      COMB options...
         Password Reqd=Yes
         Interval=10
         Compression=Yes

Ethernet
   Connections
    any Connection profile
      Station=000145CFCF01
      Encaps=COMB
      Bridge=Yes
      Encaps options...
         Password Reqd=Yes
         Send PW=remotepw
         Recv PW=localpw
         Interval=10
         Base Ch Count=2
         Compression=Yes
```

For detailed information about each parameter, see the *MAX Reference Guide*.

Understanding Combinet bridging parameters

This section provides some background information about a Combinet configuration.

Specifying the hardware address of the remote Combinet bridge

The (Connection profile) Station parameter must specify the Media Access Control (MAC) address of the remote Combinet bridging device.

Enabling bridging

A Combinet connection is always a bridging connection, so the Bridge parameter in the Connection profile must be set to Yes. If the Bridge parameter is N/A, bridging has not been enabled in the Ethernet profile (as described in Chapter 8, “Configuring Packet Bridging”).

Requiring a password from the remote bridge

You can specify that an individual Combinet connection does not require a password exchange, even if the Answer profile specifies that Combinet passwords are required.

Specifying passwords to exchange with the remote bridge

The Send PW parameter is the password sent to the remote device. It must match the password expected from the MAX. The Recv PW parameter is the password sent to the MAX from the remote device.

Configuring line-integrity monitoring

The (Answer profile) Interval parameter specifies the number of seconds between transmissions of Combinet line-integrity packets. You can specify a number between 5 and 50. If the MAX does not receive a Combinet line-integrity packet within the specified interval, it disconnects the call.

Base channel count

The (Connection profile) Base Ch Count parameter specifies the base number of channels to use when setting up the call. It can be set to 1 (for 64 Kbps) or 2 (for 128 Kbps).

Compression

The (Connection profile) Compression parameter enables or disables STACKER LZS compression/decompression. Both sides of the link must enable compression or it is not used.

Example of Combinet configuration

To configure a Combinet connection:

1 Open a Connection profile.

2 Specify the MAC address of the remote device and activate the profile. For example:

```
Ethernet
   Connections
      Station=000145CFCF01
      Active=Yes
```

3 Configure bridging options as follows:

```
      Bridge=Yes
      Dial Brdcast=Yes
```

4 Select Combinet encapsulation and then configure COMB options for this connection. (Leave the default values for Compression and Interval.) For example:

```
   Encaps=COMB
      Encaps options...
         Password Reqd=Yes
         Send PW=*SECURE*
         Recv PW=*SECURE*
         Interval=10
         Base Ch Count=2
         Compression=Yes
```

5 Close the Connection profile.

Configuring EU connections

EU encapsulation is a type of X.75 HDLC encapsulation commonly used in European countries. Like PPP, EU runs over synchronous lines. It has no asynchronous mode for connecting to modems. EU encapsulation differs from a PPP or MP+ connection in that it does not support password authentication, IP/IPX address pools, or dynamic bandwidth allocation (DBA). It does support routing and bridging connections.

EU-RAW and EU-UI do not provide password-authentication of incoming calls, so another mode of authentication is typically used to verify the caller when the call is end-to-end ISDN. For details, see the *MAX Security Supplement*.

EU configuration involves the following parameters (shown with sample settings):

```
Ethernet
   Answer
      Id Auth=Called Reqd
      Encaps...
         EU-UI=Yes
         EU-RAW=Yes

Ethernet
   Connections
     any Connection profile
      Calling #=555-7878
      Called #=555-1212
      Encaps=EU-RAW
```

```
        Encaps options...
           MRU=1524
  Ethernet
     Connections
       any Connection profile
        Calling #=555-7878
        Called #=555-1212
        Encaps=EU-UI
        Encaps options...
           MRU=1524
           DCE Addr=1
           DTE Addr=3
```

Understanding the EU parameters

This section provides some background information on EU parameters. For detailed information about each parameter, see the *MAX Reference Guide*.

EU-RAW and EU-UI

EU-RAW is a type of X.75 encapsulation in which IP packets are HDLC encapsulated together with a CRC field. EU-UI uses the same encapsulation, but contains a smaller header that can contain one value for packets from the caller and another value for packets from the called unit. Most EU connections use EU-RAW.

Maximum Receive Units (MRU)

The MRU parameter in a Connection profile's Encaps Options profile, specifies the maximum number of bytes the MAX can receive in a single packet on an EU link. Usually the default 1524 is the right setting, unless the far end device requires a lower number. If the administrator of the remote network specifies that you must change this value, enter a number lower than 1524.

Data communications equipment address (DCE Addr)

The DCE Addr parameter specifies a value for the calling unit in the EU-UI header. The caller needs to obtain the number you specify and configure the calling unit accordingly.

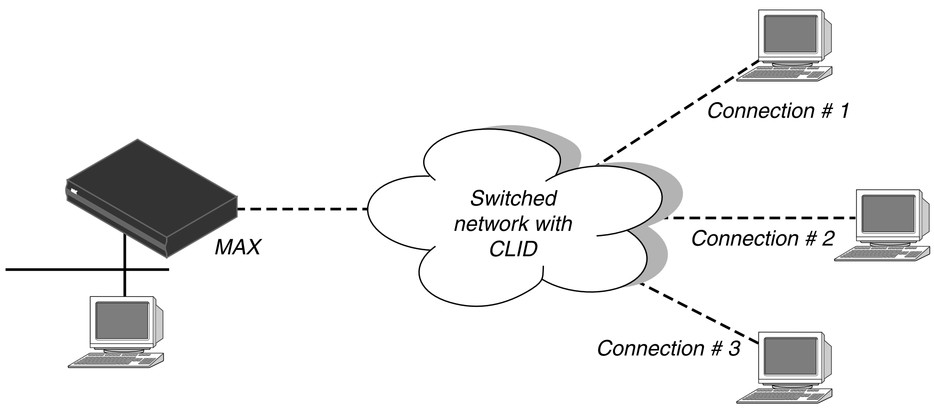
Data terminal equipment address (DTE Addr)

The DTE Addr parameter specifies a value for the called unit in the EU-UI header. The caller must use the same value for the called unit.

Example of an EU configuration

Figure 3-10 shows three connections that use EU encapsulation with ID authentication.

Figure 3-10. EU connection



To configure a connection that uses EU-RAW framing:

1 Open the Answer profile and make sure that EU-RAW encapsulation is enabled.

2 Set Id Auth to Calling Reqd (CLID authentication):

```
Ethernet
   Answer
      Id Auth=Calling Reqd
      Encaps...
         EU-RAW=Yes
```

3 Close the Answer profile.

4 Open a Connection profile and specify the name of the remote device.

5 Activate the profile:

```
Ethernet
   Connections
      Station=remote-device
      Active=Yes
```

6 Specify the calling line number. For example:

```
      Calling #=555-1212
```

7 Select the EU-RAW encapsulation type and, if necessary, configure the MRU in the Encaps Options subprofile. For example:

```
      Encaps=EU-RAW
      Encaps options...
         MRU=1524
```

8 Close the Connection profile.

Example of a EU-UI connection

To configure a connection using EU-UI framing:

1 Open the Answer profile and make sure that EU-UI encapsulation is enabled.

2 Set Id Auth to Calling Reqd (CLID authentication):

```
Ethernet
   Answer
      Id Auth=Calling Reqd
      Encaps...
         EU-UI=Yes
```

3 Close the Answer profile.

4 Open a Connection profile, specify the name of the remote device, and activate the profile. For example:

```
Ethernet
   Connections
      Station=remote-device
      Active=Yes
```

5 Specify the calling line number. For example:

```
      Calling #=555-1212
```

6 Select the EU-UI encapsulation type:

```
      Encaps=EU-UI
```

7 In the Encaps Options subprofile, set the DCE and DTE addresses. For example:

```
      Encaps options...
         MRU=1524
         DCE Addr=1
         DTE Addr=3
```

8 Close the Connection profile.

Configuring an ARA connection

AppleTalk Remote Access (ARA) uses V42 Alternate Procedure as its data link, so ARA can be used only over asynchronous modem connections.

To configure ARA connections, you set the following parameters (shown with sample settings):

```
Ethernet
   Mod Config
      Appletalk=Yes
      AppleTalk...
         Zone Name=*

Ethernet
   Answer
      Profile Reqd=Yes
      Encaps...
         ARA=Yes

Ethernet
   Connections
```

```
  Encaps=ARA
  Encaps options...
     Password=*SECURE*
     Max. Time (min)=0
AppleTalk Options...
  Peer=Dialin
  Zone Name=
  AppleTalk Router=Seed
  Net Start=300
  Net End=309
  Default Zone=
  Zone Name #1=
  Zone Name #2=
  Zone Name #3=
  Zone Name #4=
```

Understanding the ARA parameters

This section provides some background information about ARA parameters. For detailed information about each parameter, see the *MAX Reference Guide*.

AppleTalk and Zone Name

The AppleTalk parameter in the Ethernet Mod Config profile enables the AppleTalk stack in the MAX. If the local Ethernet supports an AppleTalk router with configured zones, the Zone Name parameter in the Mod Config profile should specify the zone in which the MAX unit's resides.

Profile Reqd

When Profile Reqd=Yes in the Answer profile, ARA Guest access is disabled.

Password

The (Connection profile) Password parameter specifies the password sent to the MAX from the ARA client.

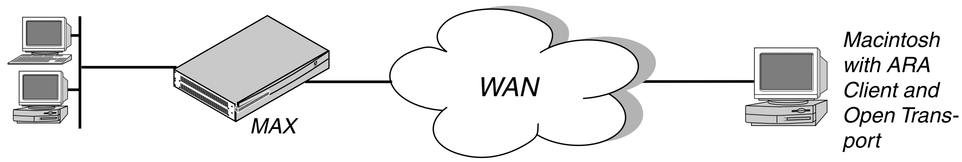
Max. Time

The (Connection Profile) Max. Time parameter specifies the maximum number of minutes an ARA session can remain connected. If it is set to 0 (zero)— (the default), the timer is disabled. The maximum connect time for an ARA connection has nothing to do with the MAX idle timer. If a connection is configured with maximum connect time, the MAX initiates an ARA disconnect when that time is up. The ARA link goes down cleanly, but remote users are not notified. Users find out the ARA link is gone only when they try to access a device.

Example of ARA configuration that enables IP access

This section shows an example of ARA configuration that enables a Macintosh with an internal modem to dial into the MAX by using the ARA Client software to communicate with an IP host on the Ethernet. A connection that does not require IP access would be a subset of this example. Figure 3-11 shows the sample network.

Figure 3-11. An ARA connection enabling IP access



Note: If you do not require IP access, the Connection profile does not need IP routing and the Macintosh client does not need a TCP/IP configuration. For ARA connections that support IP access, the MAX receives IP packets encapsulated in AppleTalk's DDP protocol. It removes the DDP headers and routes the IP packets normally.

Configure the Macintosh ARA Client software as follows:

- Set the appropriate modem parameters in the ARA Client software to enable the user's async modem to establish a connection with the MAX.
- Specify the dial-in number in the ARA Client software.

Configure the Macintosh TCP/IP software as follows:

1 Configure Open Transport

The TCP/IP Control Panel has an option to connect by using MacIP. DDP-IP encapsulation requires MacIP. This Control Panel also has an option to configure its IP address manually, via BOOTP, DHCP, or RARP. If you assign the Macintosh a permanent IP address, choose Manually. If the MAX assigns an address to the Macintosh from a pool of allocated addresses, choose BOOTP.

2 Configure MacTCP

The MacTCP Control Panel should have an icon for ARA. That icon must be selected for DDP-IP encapsulation. This Control Panel also has an option to configure its IP address Manually or from a Server. If you assign the Macintosh a permanent IP address, choose Manually. If you assign the MAX an address to the Macintosh from a pool of allocated addresses, choose Server. Do not choose *Dynamically* in the MacTCP Control Panel. The MAX does not support *Dynamically.*

Note: The MAX must be configured as an IP router. At a minimum, the MAX unit's Ethernet interface should be configured with an IP address and a DNS server address. If the ARA client obtains an IP address from the server, you must also configure the MAX for dynamic IP address assignment. See Chapter 10, "Configuring IP Routing."

If you configure the MAX for IP routing (in the Ethernet profile), you can configure an ARA connection that enables IP access as follows:

1 Open the Ethernet profile and set AppleTalk to Yes.

2 If applicable, specify the AppleTalk zone in which the MAX resides. For example:

```
Ethernet
   Mod Config
      Appletalk=Yes
      AppleTalk...
         Zone Name=Engineering
```

3 Close the Ethernet profile.

4 Open a Connection profile, specify the dial-in user's name, and activate the profile. For example:

```
Ethernet
   Connections
      Station=mac
      Active=Yes
```

5 Select ARA encapsulation and configure the ARA options. For example:

```
      Encaps=ARA
      Encaps options...
         Password=localpw
         Max. Time (min)=0
```

6 Configure the connection for IP routing.

For example, if the Macintosh software has a hard-coded IP address (Manual):

```
      Route IP=Yes
      IP options...
         LAN Adrs=10.2.3.4/24
```

Or, if the Macintosh software expects a dynamic IP address assignment:

```
      Route IP=Yes
      IP options...
         LAN Adrs=0.0.0.0/0
         Pool=1
```

7 Close the Connection profile.

Configuring dial-in PPP for AppleTalk

You can configure an Ascend unit so that individual users can dial into an AppleTalk network using a PPP dialer, such as AppleTalk Remote Access 3.0 and Pacer PPP. The MAX does not need to be set up as an AppleTalk router to support dial-in PPP to AppleTalk.

You can set up a MAX to enable an AppleTalk client to dial in using PPP in two ways:

- With a Connection profile
- With a Name/Password profile

Configuring an AppleTalk PPP connection with a Connection profile

To use a Connection profile to configure an AppleTalk PPP connection:

1 Open the Ethernet > Mod Config menu.

2 Set Appletalk=Yes.

3 Open the appropriate Connection profile.

4 Set Route Appletalk=Yes.

5 Open the AppleTalk Options menu.

```
90-103 apple
  AppleTalk options...
   Peer=Dialin
   Zone Name=N/A
   Net Start=N/A
   Net End=N/A
```

6 Set the Peer parameter to indicate whether the connection for this profile is a single user PPP connection or a router

Peer=Dialin indicates that the profile is for a single user PPP connection. All other fields in the AppleTalk Options menu are N/A.

7 If you select Peer=Dialin, you have completed the configuration. Close the AppleTalk Options menu and save your changes.

Peer=Router indicates that the profile is for a connection with a router (such as an Ascend Pipeline unit). If you select Peer=Router, you need to configure the other fields in the AppleTalk options menu by continuing with step 1 through step 5.

Note: Peer=Router works the same way that AppleTalk routing worked before this feature. The following steps are given here for convenience, and duplicate the existing documentation for AppleTalk routing.

1 Configure the AppleTalk zone name for the Ascend unit in the AppleTalk Options submenu of the Ethernet Configuration profile.

If there are other AppleTalk routers on the network, you must configure the zone names and network ranges to coincide with the other routers on the LAN.

The default for the Zone Name field is blank. Enter up to 33 alphanumeric characters to identify the zone name for the unit you are configuring.

Note: These fields display N/A if you have not enabled AppleTalk in the Ethernet Mod Config menu.

2 Set the AppleTalk Router parameter to specify the Ascend unit is a seed or nonseed router. The default setting is Off disabling AppleTalk routing.

A seed router must be assigned a network range and zone name configuration. There must be at least one seed router on a routed AppleTalk network. Select AppleTalk Router=Seed for this option.

A nonseed router learns network number and zone information from other routers. Select AppleTalk Router=Non-Seed for this option. If you choose Non Seed or Off, then Net Start, Net End, Default Zone, and Zone Name #*n* are N/A.

If you are configuring a nonseed router and are using Name/Password, go to "Configuring an AppleTalk PPP connection with a Name/Password profile" on page 3-49.

3 If you are configuring the Ascend unit as a seed router, specify the network range for the network to which the Ascend unit is attached.

Net Start and Net End define the network range for nodes attached to this network. Valid entries for these fields are in the range from 1 to 65199. If there are other AppleTalk routers on the network, you must configure the network ranges to coincide with the other routers.

4 Specify the default zone name for nodes on the Ascend unit's internet.

Enter up to 33 alphanumeric characters for the default zone name. The default for this field is blank.

The default zone is the one used by a node in the network for which you are configuring the Connection profile, until another zone name is explicitly selected by the node.

5 Specify the zone names that the platform can seed.

The MAX can seed up to 32 zones, the Pipeline can seed up to 5. Enter up to 33 alphanumeric characters in each Zone Name #*n* field.

Configuring an AppleTalk PPP connection with a Name/Password profile

To use a Name/Password profile to configure an AppleTalk PPP connection:

1 Open the Ethernet > Mod Config menu.

2 Set Appletalk to Yes.

3 In the Answer profile, open the PPP Options menu.

4 Set Route Appletalk to Yes.

5 PPP Options menu's Appletalk options submenu. For example:

```
90-103 apple
  AppleTalk options...
   Peer=Dialin
```

6 Set the Peer parameter to indicate whether the connection for this profile is a single user PPP, connection, or a router.

Peer=Dialin indicates that the profile is for a single user PPP connection. All other fields in the AppleTalk options menu are N/A. Peer=Router indicates that the profile is for a connection with a router (such as an Ascend Pipeline unit). If you select Peer=Router, you need to configure the other fields in the AppleTalk Options menu. If you select Peer=Dialin, you have completed the configuration.

7 Close the AppleTalk Options menu and save your changes.

If you selected Peer=Router in step 6 of the preceding procedure:

1 Configure the AppleTalk zone name for the Ascend unit in the AppleTalk Options submenu of the Ethernet Configuration profile.

If there are other AppleTalk routers on the network, you must configure the zone names and network ranges to coincide with the other routers on the LAN.

The default for the Zone Name field is blank. Enter up to 33 alphanumeric characters to identify the zone name for the unit you are configuring.

Note: These fields display N/A if you have not enabled AppleTalk in the Ethernet Mod Config menu.

2 Set the AppleTalk Router parameter to specify the Ascend unit is a seed or nonseed router. The default setting is Off disabling AppleTalk routing.

A seed router must be assigned a network range and zone name configuration. There must be at least one seed router on a routed AppleTalk network. Select AppleTalk Router=Seed for this option.

A nonseed router learns network number and zone information from other routers. Select AppleTalk Router=Non-Seed for this option. If you choose Non Seed or Off, then Net Start, Net End, Default Zone, and Zone Name #*n* are N/A.

If you are configuring a nonseed router and are using Name/Password, go to “Configuring an AppleTalk PPP connection with a Name/Password profile” on page 3-49.

3 If you are configuring the Ascend unit as a seed router, specify the network range for the network to which the Ascend unit is attached.

Net Start and Net End define the network range for nodes attached to this network. Valid entries for these fields are in the range from 1 to 65199. If there are other AppleTalk routers on the network, you must configure the network ranges to coincide with the other routers.

4 Specify the Default Zone name for nodes on the Ascend unit’s internet.

Enter up to 33 alphanumeric characters for the Default Zone name.

The Default Zone is the one used by a node in the network for which you are configuring the Connection profile, until another zone name is explicitly selected by the node.

5 Specify the zone names that the platform can seed.

The MAX can seed up to 32 zones, and the Pipeline can seed up to five. Enter up to 33 alphanumeric characters in each Zone Name #*n* field.

Configuring AppleTalk connections from RADIUS

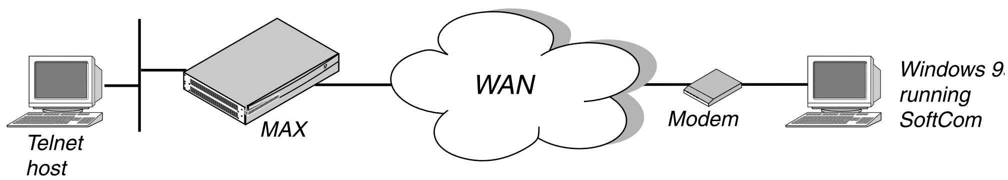
You can set up an AppleTalk connection in a RADIUS user profile and configure static AppleTalk routes in a RADIUS pseudo-user file. For detailed information, see the *MAX RADIUS Configuration Guide*.

Configuring terminal-server connections

Terminal-server connections are host-to-host connections that use an analog modem, ISDN modem (such as a V.120 terminal adapter), or raw TCP. If you use one of these methods to initiate a call but the call contains PPP encapsulation, the terminal server forwards the call to the MAX router. These are asynchronous PPP calls, and aside from the initial processing, the MAX handles asynchronous PPP calls like regular PPP sessions as described in "Configuring PPP connections" on page 3-16.

Figure 3-12 shows a user dialing in via analog modem with dial-up software that does not include PPP. The MAX first routes this type of call to a digital modem, then forwards the call automatically to the terminal server.

Figure 3-12. Terminal-server connection to a local Telnet host



Terminal-server connections can be authenticated via Connection or Name/Password profiles, or through a third-party authentication server such as RADIUS.

Note: Like PPP connections, terminal-server connections rely on the Answer profile for default settings and enabling of the encapsulation type. For information about the telco options in a Connection profile, see "Introduction to WAN links" on page 3-1. These telco options apply equally to PPP or terminal-server calls.

Connection authentication issues

When the terminal server receives a forwarded call, it waits briefly to receive a PPP packet. If the terminal server times out waiting for PPP, it sends its Login prompt. When the terminal server receives a name and password, it authenticates them against the Connection profile.

If the terminal server receives a PPP packet, instead of sending a Login prompt it responds with a PPP packet and LCP negotiation begins, including PAP or CHAP authentication. The terminal server then establishes the connection as a regular PPP session.

Note: If you do not want your users to share profiles, set the Shared Prof parameter to No. This parameter can be set in Ethernet > Mod Config for all users or in Ethernet > Connections > *any Connection profile* for a single user. For more details about the Shared Prof parameter, see the *MAX Reference Guide*. To specify shared profiles per user in RADIUS, see the Ascend-Shared-Profile-Enable attribute in the *MAX RADIUS Reference Guide*.

Recommended settings for callers with modems and terminal adapters depend on the type of device and whether the connection uses PPP.

Analog modems and async PPP connections

If the Connection profile specifies PAP or CHAP authentication for connection through analog modem, the caller's PPP software should not be configured with any expect-send scripts, because the software must start negotiating PPP when the modems connect.

If the Connection profile does not specify PAP or CHAP authentication, configure the caller's PPP software with an expect-send script (expect > *Login:* send <$username> expect *Password:* send <$password:>). When the MAX authenticates the connection, the software starts sending PPP packets.

V.120 terminal adapters and PPP connections

If you configure the V.120 terminal adapter to run the PPP protocol, the V.120 terminal adapter handles PAP or CHAP authentication and whatever other PPP or MP features the terminal adapter supports. Typically, the Connection profile requires PAP or CHAP.

V.120 terminal adapters with PPP turned off

If you configure a V.120 terminal adapter to run without PPP, it does not support PAP or CHAP authentication. If the Connection profile requires PAP or CHAP authentication, the connection fails.

Modem connections

This section shows sample Connection profiles for a terminal server connection established via analog modem. For example, the following profile uses only the required parameters for authenticating a terminal server modem connection:

```
Ethernet
   Connections
      Station=uttam
      Active=Yes
      Encaps=PPP
      Encaps options...
         Recv PW=localpw
```

For detailed information about each parameter, see "Understanding the PPP parameters" on page 3-18.

The next profile shows optional parameters for bringing down the terminal server connection after a specified amount of idle time:

```
Ethernet
   Connections
      Station=uttam
      Active=Yes
      Encaps=PPP
      Encaps options...
         Recv PW=localpw
      Session options...
         TS Idle Mode=Input/Output
         TS Idle=60
```

For information about the parameters, see “Connection profile Session options” on page 3-9 and “Configuring single-channel PPP connections” on page 3-17.

V.120 terminal adapter connections

V.120 terminal adapters (also known as ISDN modems) are asynchronous devices that use CCITT V.120 encapsulation. The values that seem to work best for V.120 operation are:

- Maximum information field size for send and receive packets = 260 bytes
- Maximum number of retransmissions (N200) = 3
- Logical link ID (LLI) = 256
- Idle timer (T203) = 30 seconds
- Maximum number of outstanding frames = 7
- Modulo = 128
- Retransmission timer (T200) = 1.5 seconds
- Types of frames accepted = UI, I. (I-type frames are recommended.)
- Call placement: The MAX can receive V.120 calls, but cannot place them.

Note: If the connection uses PAP or CHAP authentication, the ISDN terminal adapter should be configured for async-to-sync conversion. In this case, V.120 encapsulation is not required in the Connection profile. For more information, see “Connection authentication issues” on page 3-51.

The V.120 device must be correctly configured to place calls to the MAX. The settings required for compatible operation of a V.120 device and the MAX are listed below. For information about entering these settings, see the V.120 manual.

- V.120 maximum transmit frame size = 260 bytes
- V.120 maximum receive frame size = 260 bytes
- Logical link ID = 256
- Modulo = 128
- Line channel speed = Select 56K if the MAX accepts calls from the V.120 device on a T1 line, or if you are not sure that you have 64 Kbps channel speed end-to-end.

After checking the configuration of the V.120 device, make sure you enable V.120 calls in the Answer profile:

```
Ethernet
   Answer
      Encaps...
         V.120=Yes

      V.120 options...
         Frame Length=260
```

To configure a connection that uses a V.120 terminal adapter, create a Connection profile such as the following:

```
Ethernet
   Connections
     Tommy
       Station=tommy
```

```
          Active=Yes
          Encaps=PPP
          Encaps options...
             Recv PW=localpw
          Session options...
             TS Idle Mode=Input
             TS Idle=60
```

For information about the parameter, see "Connection profile Session options" on page 3-9 and "Configuring single-channel PPP connections" on page 3-17.

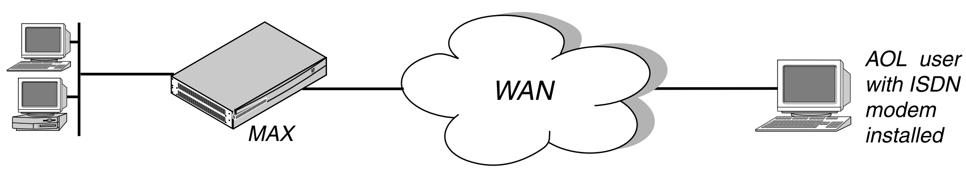
TCP-clear connections

Use a TCP-clear connection for surname logins or TCP modem connections.

Username login

In most cases, use TCP-clear to transport custom-encapsulated data understood by the host and the caller. For example, America Online customers who log in from an ISDN device typically use a TCP-clear connection to *tunnel* their proprietary encapsulation method in raw TCP/IP packets, as shown in Figure 3-13.

Figure 3-13. A TCP-clear connection



Note: A TCP-clear connection is host-to-host. As soon as the MAX authenticates the connection, the host establishes a TCP connection as specified in the Connection profile.

First, make sure you enable TCP-clear calls in the Answer profile:

```
Ethernet
   Answer
      Encaps...
         TCP-CLEAR=Yes
```

To configure a TCP-clear connection, set the parameters shown in the following example:

```
Ethernet
   Connections
     Richard
       Station=richard
       Active=Yes
       Encaps=TCP-CLEAR
       Encaps options...
         Recv PW=localpw
         Login Host=techpubs
         Login Port=23
       Session options...
         TS Idle Mode=Input
         TS Idle=60
```

If you configure DNS, you can enter a hostname for the Login host (such as the *techpubs* example above). Otherwise, specify the host's IP address. The port number is the TCP port, on the host, to use for the connection. A port number of zero means *any port*.

(F or related information, "Connection profile Session options" on page 3-9 and "TCP-modem connections (DNIS Login)" on page 3-55.)

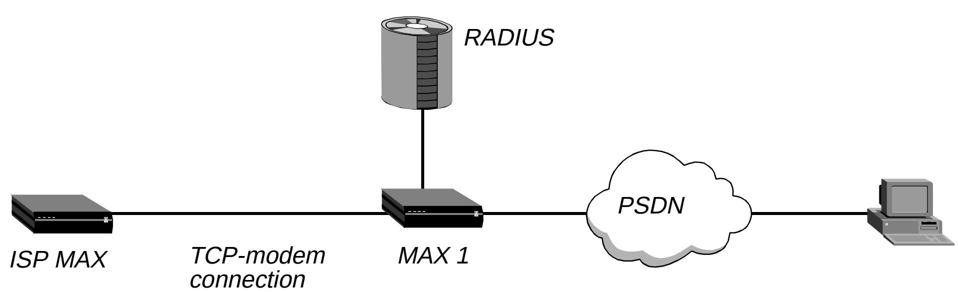
TCP-modem connections (DNIS Login)

The TCP-modem feature enables the MAX to accept connections through the Ethernet interface although the MAX handles the sessions as if they were modem connections. You can enable or disable TCP-modem access to the MAX, and you can configure the default port for TCP modem access.

TCP-modem refers to the way the MAX treats a TCP-encapsulated call between two MAX units over an asynchronous line as if it were a modem. You can disable TCP-modem connections to the MAX. In addition, you can change the TCP port used for these connections. The default port for TCP-modem is 6150.

Figure 3-14 illustrates an example of a TCP modem-setup. A user dialing into an ISP first connects to the telephone switch and then establishes a connection to MAX 1. The MAX 1 has a TCP-Clear connection configured in RADIUS to a MAX at an ISP. Typically, this connection is over Frame Relay. The remote user appears to be directly connected to the ISP MAX. MAX 1 merely passes the data through. The ISP MAX typically authenticates remote users.

Figure 3-14. Sample TCP-modem connection



For detailed information about TCP-modem connections, see the *MAX RADIUS Configuration Guide*.

The terminal-server interface

The terminal server can provide a command-line interface (terminal mode) or a menu of Telnet hosts that dial-in users can log into (menu mode). Or, you can configure an immediate mode to automatically present the user with a login prompt to a host, bypassing the terminal-server interface altogether.

Terminal mode

In terminal mode, users have access to the command line and can see information about your network by using administrative terminal-server commands. You can also enable them to initiate their own Telnet, Rlogin, or TCP connections to hosts.

Menu mode

The menu interface lists up to four local hosts. Users select a hostname to initiate a Telnet session to that host. The menu interface with four hosts looks like this:

```
Up to 16 lines of up to 80 characters each
will be accepted. Long lines will be truncated.
Additional lines will be ignored


         1. host1.abc.com
         2. host2.abc.com
         3. host3.abc.com
         4. host4.abc.com
           Enter Selection (1-4, q)
```

Immediate mode

In immediate mode, the terminal server initiates a Telnet, Rlogin, or TCP connection to one specified host without every giving the dial-in user a choice. The host requires login and password entered by the user, not by the terminal server.

Enabling terminal-server calls and setting security

To enable the MAX units terminal servers, open Ethernet > Mod Config > TServ Options and set TS Enabled to Yes.

Also, the terminal-server Security setting can be None, Partial, or Full. The setting determines whether users are prompted for a login name and password before entering the terminal server. Its meaning is partly dependent on whether users log into menu mode or terminal mode, and whether they are allowed to toggle between these two modes.

- With security set to None, no prompt appears for a login name and password.
- With security set to Partial, a prompt appears for a name and password only when entering terminal mode, not for menu mode.
- With security set to Full, a prompt appears for a name and password upon initial login, no matter what interface appears.

Understanding modem parameters

Calls from analog modems are directed first to the MAX digital modems where the connection must be negotiated before being directed to the terminal-server software.

To influence the outcome for modem negotiation and data packetizing, you can set the following parameters:

```
Ethernet
   Mod Config
      TServ options...
         V42/MNP=Will
         Max Baud=33600
         MDM Trn Level=-13
         MDM Modulation=K56
         Cell First=No
         Cell Level=-18
         7-Even=No
         Packet Wait Time=2
         Packet characters=0
```

This section provides background information about the modem configuration parameters. For complete information, see the *MAX Reference Guide*.

V42/MNP

The digital modems negotiate LAPM/MNP error control with the analog modem at the other end of the connection according to how the V42/MNP parameter is set. The modems can request LAPM/MNP and accept the call anyway if it is not provided, request it and drop the call if it is not provided, or not use LAPM/MNP error control at all.

Max Baud

Typically, the digital modems start with the highest possible baud rate (3360) and negotiate down to the rate accepted by the far end modem. You can adjust the maximum rate to bypass some of the negotiation cycles, provided that no inbound calls use a baud rate higher than what you specify here.

MDM Trn Level

The MDM Trn Level parameter specifies the modem transit level, which is the amount of attenuation in decibels the MAX should apply to the line. When a modem calls the MAX, the unit attempts to connect at the transmit attenuate level you specify. Generally, you do not need to change the transmit level. However, if the carrier becomes aware of line problems or irregularities, you might need to alter the modem transmit level.

Users can change the default settings for their specific connections. Increasing the attentuation, level helps certain modems with near-end-echo problems.

MDM Modulation

You can specify the modulation to use when answering calls on the unit’s 56K modems. The possible settings are K56, V.34 and V.90.

Cell FIrst and Cell Level

The MAX supports cellular modem call, and the user can set the gain level of the modem for cellular communication.

Cell First determines whether the MAX first attempts cellular modem or conventional modem negotiation when answering incoming calls. If the first negotiation fails, the MAX attempts the other negotiation.

Cell Level determines the gain level of the cellular modem.

7-Even

The MAX does not use 7-bit even parity on outbound data unless you set the 7-Even parameter to Yes. Most applications do not use 7-bit even parity.

Packet Wait and Packet Characters

The Packet Wait and Packet Characters parameters support specialized applications on modem connections. Packet Wait specifies the maximum amount of time, in milliseconds, that any received data can wait before being passed up the protocol stack for encapsulation.

Packet Characters specifies the minimum number of bytes of received data that should accumulate before the data is passed up the protocol stack for encapsulation.

Note: Be sure to take into account modem speeds when calculating these values.

Example of modem configuration

To set the maximum negotiable baud rate for incoming calls from analog modems:

1. Open Ethernet > Mod Config > TServ Options.
2. Set the maximum negotiable baud rate to 26400:

```
Ethernet
   Mod Config
      TServ options...
         Max Baud=26400
```

3. Close the Ethernet profile.

Configuring terminal mode

When a user communicates with the terminal server itself (rather than with a host, in immediate mode), the MAX establishes a session between the remote user's PC and the terminal server. The following parameters (shown with sample settings) affect the session the MAX establishes and what commands are available to the user:

```
Ethernet
   Mod Config
      TServ options...
         Silent=No
         Clr Scrn=Yes
         Passwd=
         Banner=** Ascend Terminal Server **
```

```
Login Prompt=Login:
Prompt Format=Yes
Passwd Prompt=Password:
Prompt = ascend%
Term Type= vt100
Login Timeout= 60
...
Telnet=Yes
Rlogin=No
Def Telnet=Yes
Clear Call=No
Telnet mode=ASCII
Local Echo=No
Buffer Chars=Yes
...
3rd Prompt=
3rd Prompt Seq=N/A
IP Addr Msg=N/A
```

Understanding the terminal-mode parameters

This section provides background information on the terminal-mode configuration parameters. For complete information, see the *MAX Reference Guide*.

Silent and Clr Scn

The Silent and Clr Scn parameters specify the appearance of the user's screen during establishment of the connection. Silent determines whether status messages appear while the MAX tries to establish the connection. You can set Clr Scrn to clear the screen when the MAX establishes a connection.

Password

The Passwd parameter specifies a terminal-mode password of up to 15 characters. This is the password terminal-server users will be prompted for when establishing a connection to the terminal server itself.

Banner and prompts for login

When the MAX establishes the terminal-server session, the system displays the banner "**Ascend Terminal Server **" or a different banner you have configured.

Login Prompt and Password Prompt specify what the user sees while logging in. The default prompts are:

Login:

Password:

The Login prompt can be up to 80 characters and consist of more than one line if Prompt Format is set to Yes. To specify a multiline prompt, set Prompt Format to Yes and use `\n` to represent a carriage return/line feed and `\t` to represent a tab.

Prompt

The Prompt parameter specifies the command-line prompt, which by default is:

```
ascend%
```

Be sure to include a trailing space you want one on the user's screen.

Login timeout

The MAX disconnects users 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. The timer begins when the login prompt appears on the terminal-server screen, and it continues (is not reset) when the user makes unsuccessful login attempts.

Telnet and Rlogin session defaults

You can enable or disable the use of the Rlogin, and Telnet commands at the terminal-server command line. When they are enabled, you can set parameters to affect session defaults. (Users can modify some of these default values on the command line.)

Term Type specifies a default terminal type, such as the VT100.

Def Telnet instructs the terminal server to interpret unknown command strings as the name of a host for a Telnet session.

Clear Call specifies whether the connection terminates when the user terminates a Telnet or Rlogin session.

Telnet Mode specifies whether binary, ASCII, or transparent mode is the default for Telnet sessions.

Local Echo sets a global default for echoing characters locally. The default can be changed for an individual session within Telnet.

Buffer Chars determines whether the terminal server buffers input characters for 100 milliseconds before forwarding them to the host, or sends the characters as they are received.

3rd Prompt and 3rd Prompt Seq

The 3rd Prompt parameter specifies another login prompt, and 3rd Prompt Seq specifies whether the third prompt appears before or after the regular terminal server login prompts.

For RADIUS-authenticated logins, some servers require a third prompt and require that it appear last in the login sequence.

Some ISPs use a terminal server that follows a login sequence that includes a menu selection before to login. Administrators at those sites can configure the third prompt to appear first, to mimic their terminal server and retain compatibility with client software in use by subscribers.

IP Addr Msg

When informing users of their address, the terminal server displays *Your IP address is...* followed by the assigned address. You can change this default message.

Example of terminal-mode configuration

This example shows how to configure the password and make the Rlogin option available to dial-in users.

1 Open Ethernet > Mod Config > TServ Options.

2 Set Telnet to Yes.

3 Specify the terminal-server password. For example:

```
Passwd=tspasswd
Rlogin=Yes
```

4 Configure a multiline login prompt. For example:

```
Ethernet
   Mod Config
      TServ options...
         Login Prompt=Welcome to Ascend Remote Server\Enter your
         name:
         Prompt Format=Yes
```

5 Enable the use of the Rlogin command in terminal mode:

```
Passwd=tspasswd
Rlogin=Yes
```

6 Close the Ethernet profile.

Configuring immediate mode

When dial-in calls are directed immediately to a host, the MAX establishes a session between the remote user's PC and that host via Rlogin, Telnet, or TCP. The following parameters (shown with sample values) affect:

```
Mod Config
   TServ options...
      Immed Service=None
      Immed Host=N/A
      Immed Port=N/A
      Telnet Host Auth=No
```

Understanding the immediate-mode parameters

This section provides background information about the immediate-mode configuration parameters. For complete information, see the *MAX Configuration Guide*.

Immediate Service and Telnet Host Auth

The Immed Service parameter enables a particular type of service for establishing an immediate host connection for dial-in users. You can specify Telnet, Raw-TCP, Rlogin, or X25-PAD. For details about X.25, see Chapter 6, "Configuring X.25."

For Telnet service, you can set the Telnet Host Auth parameter to bypass the terminal-server authentication and go right to a Telnet login prompt.

Immed Host and Immed Port

Specify the hostname or address to which users will connect in terminal-server immediate mode. You can also specify a TCP port number to use for the connections.

Example of immediate-mode configuration

To configure immediate Telnet service relying on the Telnet host for authentication:

1. Open Ethernet > Mod Config > TServ Options.
2. Set the Immed Service parameter to Telnet.
3. Specify the name or IP address of the Telnet host.
4. If appropriate, specify the TCP port to use on the Telnet host.
5. Set the Telnet Host Auth parameter to Yes.
6. Close the Ethernet profile.

Following is an example of this configuration:

```
Ethernet
   Mod Config
      TServ options...
         Immed Service=Telnet
         Immed Host=host1.abc.com
         Immed Port=23
         Telnet Host Auth=Yes
```

Configuring menu mode

You can set up the terminal server to display a menu of up to four Telnet hosts that dial-in users can select for logging in. You can set up menu mode with the following parameters (shown with sample settings):

```
Ethernet
   Mod Config
      TServ options...
         Initial Scrn=Cmd
         Toggle Scrn=No
         Remote Conf=No
         Host #1 Addr=0.0.0.0
         Host #1 Text=
         Host #2 Addr=0.0.0.0
         Host #2 Text=
         Host #3 Addr=0.0.0.0
         Host #3 Text=
         Host #4 Addr=0.0.0.0
         Host #4 Text=
```

Understanding the menu-mode parameters

This section provides background information about the menu-mode configuration parameters. For complete information, see the *MAX Configuration Guide*.

Initial Scrn and Toggle Scrn

The Initial Scrn parameter determines whether the terminal server brings up a menu interface first for interactive users initiating connections. Depending on the Toggle Scrn setting, users can switch to the command-line interface from menu mode by pressing the 0 (zero) key. The Security setting (Ethernet > Mod Config > Tserv Options) determines whether a login and password is required when entering the menu interface.

Remote Conf

The Remote Conf parameter specifies that the terminal-server menu and list of hosts will be obtained from a RADIUS server.

Host addresses and names

The Host #*N* Addr and Host #*N* Text parameters expect an IP address and hostname, respectively, for up to four Telnet hosts which will appear in the menu interface.

Example of menu-mode configuration

Configuration of this example enables the menu to appear at login, and specifies four hosts. The user does not have access to the command line. To implement the configuration:

1 Open Ethernet > Mod Config > TServ Options.

2 Specify that the dial-in users are in menu mode initially:

```
Ethernet
   Mod Config
      TServ options...
         Initial Scrn=Menu
```

3 Specify the IP addresses and hostnames of up to four hosts to appear in the menu. For example:

```
Ethernet
   Mod Config
      TServ options...
         Host #1 Addr=10.2.3.4
         Host #1 Text=host1.abc.com
         Host #2 Addr=10.2.3.57
         Host #2 Text=host2.abc.com
         Host #3 Addr=10.2.3.121
         Host #3 Text=host3.abc.com
         Host #4 Addr=10.2.3.224
         Host #4 Text=host4.abc.com
```

Dial-in users are able to Telnet to these hosts by selecting the hostname or IP address. For an example menu, see “Enabling terminal-server calls and setting security” on page 3-56.

4 Close the Ethernet profile.

Configuring PPP mode

Users who are logged into the terminal server in terminal mode can invoke an async PPP session by using the PPP command, to initiate PPP mode. Or, even if users do not have access to the command line, they can begin an async PPP session from an application such as Netscape Navigator or Microsoft Explorer. For example, if a user initiates a session from Windows 95, which has a resident TCP/IP stack, the async PPP session can begin immediately, without the user entering the terminal-server interface. The following parameters (shown with their sample settings) configure PPP mode:

```
Ethernet
   Mod Config
      TServ options...
         PPP=No
         ...
         PPP Delay=5
         PPP Direct=No
         PPP Info=mode
```

Understanding the PPP mode parameters

This section provides some background information about the PPP mode configuration parameters. For complete information, see the *MAX Configuration Guide*.

PPP

Users cannot initiate PPP sessions unless you enable PPP mode by setting PPP to No.

PPP Delay

The PPP Delay parameter specifies the number of seconds the terminal server waits before transitioning to packet-mode processing.

PPP Direct

The PPP Direct parameter specifies whether to start PPP negotiation immediately after a user enters the PPP command in the terminal-server interface, or to wait to receive a PPP packet from an application. (Some applications expect to receive a packet first.)

PPPInfo

You can set the PPP Info parameter to specify one of the three messages to inform users that they are in PPP mode. The selections are None (no message), PPP Mode, and PPP Session.

Example of PPP configuration

The configuration in this example enables PPP direct mode. To implement the configuration:

1 Open Ethernet > Mod Config > TServ Options.

2 Enable the use of the PPP command in terminal mode.

3 Enable PPP direct negotiation:

```
Ethernet
   Mod Config
      TServ options...
         PPP=Yes
         PPP Direct=Yes
```

4 Close the Ethernet profile.

Configuring Serial Line IP (SLIP) mode

If you enable SLIP mode in the terminal server, users can initiate a SLIP session and then run an application such as FTP in that session. SLIP mode configuration uses the following parameters (shown with their default settings):

```
Ethernet
   Mod Config
      TServ options...
        SLIP=No
        SLIP BOOTP=N/A
        IP Netmask Msg
        IP Gateway Adrs Msg
       Slip Info
```

Understanding the SLIP mode parameters

This section provides some background information about the SLIP mode configuration parameters. For complete information, see the *MAX Configuration Guide*.

SLIP

To enable SLIP sessions, set the SLIP parameter to Yes.

SLIP BOOTP

Setting the SLIP BOOTP parameter to Yes enables the terminal server to respond to BOOTP within SLIP sessions. A user who initiates a SLIP session can then get an IP address from the designated IP address pool via BOOTP. If the parameter is set to No, the terminal server does not run BOOTP. Instead, the user is prompted to accept an IP address at the start of the SLIP session

IP Netmask Msg

The IP Netmask Msg parameter enables you to specify a text message the MAX displays before the netmask field in the SLIP session startup message. You can enter up to 64 characters. The default is `Netmask:` (IP Netmask Msg does not apply unless you set SLIP Info to Advanced.)

IP Gateway Adrs Msg

The IP Gateway Adrs Msg parameter specifies the text the MAX displays before the MAX IP address field in the SLIP session startup message. You can enter up to 64 characters. The default is `Netmask:` (IP Netmask Msg does not apply unless you set SLIP Info to Advanced.)

SLIP Info

The SLIP Info parameter has the following two settings:

- Basic—Enables the MAX to report the SLIP user's IP address and the Maximum Transmission Unit (MTU).
- Advanced—Enables the MAX to report the SLIP user's IP address, the MTU, the Netmask, and the Gateway to SLIP users.

  Note: The gateway is the MAX unit's IP address.

Example of SLIP configuration

The configuration in this example enables SLIP sessions and ensures the terminal server's response to BOOTP in SLIP sessions. To implement the configuration:

1 Open Ethernet > Mod Config > TServ Options.

2 Enable the use of the SLIP command:

```
SLIP=Yes
```

3 Enable the use of BOOTP in SLIP sessions:

4 Close the Ethernet profile.

Configuring dial-out options

The terminal server has access to the MAX digital modems, and can be configured to enable users on the local network to dial through the digital modems. To enable local dial-out, you set the following parameters (shown with sample settings):

```
Ethernet
   Mod Config
      TServ options...
         Modem dialout=No
         Immediate Modem=N/A
         Imm. Modem port=N/A
         Imm. Modem Pwd=N/A
```

Understanding the Dialout parameters

This section provides some background information about the dialout configuration parameters. For complete information, see the *MAX Configuration Guide*.

Modem Dialout

If you set the Modem Dialout parameter to Yes, local users can connect to the terminal server via Telnet and then issue AT commands to the modem as if connected locally to the modem's asynchronous port.

Immediate-modem parameters

If you set the Immediate Modem parameter to Yes, users Telnet to a particular port on the MAX and the MAX provides immediate modem dial-out service. The port number configured for immediate-modem dial-out tells the MAX that all telnet sessions initiated with the port number want modem access. Immediate-modem service has its own password (up to 64 characters). If the Imm. Modem Pwd setting is non-null, users will be prompted for a password before being allowed access to a modem.

How to use non-immediate-modem dial-out

If you enable dial-out (not immediate modem), users can access a modem after Telneting to the MAX from a workstation. For example:

`Telnet max01`

Once the Telnet session is established, the user proceeds as follows:

1 Invoke the terminal-server command-line interface (System > Sys Diag > Term Serv).

Users see the terminal-server prompt, for example:

`ascend%`

2 Enter the terminal-server Open command.

`ascend%` **`open`**

Without an argument, the Open command sets up a virtual connection to the first available digital modem. Alternatively, the user can specify a particular modem by including its slot and item number as an argument to the command. For example:

`ascend%` **`open 7:1`**

3 Use the standard Rockwell AT commands to dial out on the modem, just as if using a modem connected directly to a workstation. For example:

`ATDT 1V1 ^M`

4 To suspend a virtual connection to a digital modem and return to the terminal-server prompt, press Ctrl-C three times.

5 To resume the suspended virtual connection, enter the Resume command:

`ascend%` **`resume`**

6 To terminate a virtual connection, enter the Close command:

`ascend%` **`close`**

How to use immediate-modem dial-out

Immediate Modem enables users to access a modem directly by Telneting to the specified port. For example, users can access a modem as follows:

1 Telnet to the MAX from a workstation, specifying the immediate-modem port number on the command line. For example:

`Telnet max01 5000`

Where **`max01`** is the system name of the MAX and **`5000`** is the immediate-modem port.

2 Use the standard Rockwell AT commands to dial out on the modem, just as if using a modem connected directly to a workstation. For example:

`ATDT 1V1 ^M`

3 Press Ctrl-C to terminate the connection.

Example of dial-out configuration

The configuration in this example enables direct access (immediate modem) on port 5000. To implement the configuration:

1 Open Ethernet > Mod Config > TServ Options.

2 Enable the use of the modem-dial-out and direct-access (immediate-modem) features:

```
Ethernet
   Mod Config
      TServ options...
         Modem dialout=Yes
         Immediate Modem=Yes
```

3 Specify the port on which port the immediate-modem feature functions and specify a password for modem access:

```
Ethernet
   Mod Config
      TServ options...
         Imm. Modem port=5000
         Imm. Modem Pwd=dialoutpwd
```

4 Close the Ethernet profile.

Configuring DHCP services

A MAX performs a number of Dynamic Host Configuration Protocol (DHCP) services, including responding to DHCP requests to borrow IP addresses, managing Plug and Play requests, and DHCP spoofing.

A MAX can respond to DHCP requests for up to 43 clients at any given time. DHCP server responses provide an IP address and subnet mask. You can define two address pools of up to 20 IP addresses each. Additionally, up to three hosts, identified by their MAC (Ethernet) addresses, can each have an IP address reserved for its exclusive use.

The Plug and Play management feature responds to requests for TCP/IP configuration settings from computers using Microsoft Windows 95 or Windows NT.

A DHCP spoofing response supplies a temporary IP address for a single host. The IP address supplied is always one greater than that of the MAX. The IP address is good for only 60 seconds—just long enough to enable a security-card user to acquire the current password from an ACE or SAFEWORD server and bring up an authenticated dial-up session. Once the MAX establishes the dial-up session, an official IP address can be retrieved from a remote DHCP or BOOTP server. The ability to retrieve an IP address, together with network address translation (NAT), enables a single computer to connect to a remote network that assigns IP addresses dynamically.

How the MAX assigns IP addresses

When you configure a MAX to be a DHCP server and it receives a DHCP client request, it assigns an IP address by means of Plug and Play, reserved address, lease renewal, or assignment from a pool.

Plug and Play

When you enable the Plug and Play option (DHCP PNP Enabled=Yes), the MAX takes its own IP address, increments it by one, and returns it in the BOOTP reply message along with IP addresses for the Default Gateway and Domain Name Server. Plug and Play works with Microsoft Windows 95 (and possibly with other IP stacks) to assign an IP address and other wide-area networking settings to a requesting device automatically. With Plug and Play you can use the MAX to respond to distant networks without having to configure an IP address first.

Reserved address

If there is an IP address that is reserved for the host, the MAX assigns the reserved address.

Lease renewal

If the host is renewing the address it currently has, the MAX assigns the host the same address. When a host gets a dynamically assigned IP address from one of the address pools, it periodically renews the lease on the address until it has finished using it, as defined by the DHCP protocol. If the host renews the address before its lease expires, the MAX always provides the same address.

Assignment from a pool

If the host is making a new request and there is no IP address reserved for the host, the MAX assigns the next available address from its address pools. It can draw from up to two 20-address pools of contiguous IP addresses. Addresses are assigned by using the first available address from the first pool or, if there are no available addresses in that pool and there is a second pool, the first available address in the second pool.

Configuring DHCP services

To configure a DHCP service, open Ethernet > Mod Config > DHCP Spoofing. Although the name of this menu is DHCP Spoofing, it contains parameters for all DHCP services, including DHCP Spoofing, DHCP Server, and Plug and Play:

```
20-A00 Mod Config
 DHCP Spoofing...
  DHCP Spoofing=Yes
  DHCP PNP Enabled=Yes
  Renewal Time=10
  Become Def. Router=No
  Dial If link down=No
  Always Spoof=Yes
  Validate IP=Yes
  Maximum no reply wait=5
```

```
IP group 1=181.100.100.100/16
Group 1 count=1
IP group 2=0.0.0.0/0
Group 2 count=0
Host 1 IP=181.100.100.120
Host 1 Enet=0080c75Be95e
Host 2 IP=0.0.0.0/0
Host 2 Enet=000000000000
Host 3 IP=0.0.0.0/0
Host 3 Enet=000000000000
```

If you need more information about a particular parameter, see the *MAX Reference Guide*. Set each parameter according to the function it provides, as follows.

1 Set the DHCP Spoofing parameter to Yes to enable any DHCP service. If you set it to No, other settings in this menu are ignored.

2 Set the DHCP PNP Enabled parameter to Yes to enable Plug and Play. Setting this parameter to Yes and DHCP Spoofing set to Yes is all that is required to enable Plug and Play support.

3 Renewal Time specifies how long a DHCP IP address lives before it needs to be renewed. It applies to both DHCP spoofed addresses and DHCP server replies. If the host renews the address before it expires, the MAX provides the same address. Plug and Play addresses always expire in 60 seconds.

4 Become Default Router is an option you can set to advertise the address of your MAX as the default router for all DHCP request packets.

5 Dial If Link Down is used with DHCP spoofing in conjunction with BOOTP Relay. This parameter applies when both DHCP spoofing and BOOTP relay are enabled. If no wide area network links are active, the MAX performs DHCP spoofing. If the parameter is set to Yes, as soon as the dialed link is established, the MAX stops DHCP spoofing and acts as a BOOTP relay agent.

6 Set Always Spoof to Yes or No, to enable either the DHCP server or DHCP spoofing:

- Yes enables the DHCP server. A DHCP server always supplies an IP address for every request, until all IP addresses are exhausted.
- No enables DHCP spoofing. DHCP spoofing only supplies an IP address for a single host on the network. It does not respond to all requests.

7 Set Validate IP to Yes to check on whether a spoofed address that is about to be assigned is already in use, and if it is, automatically assign another address.

8 Set Maximum No-Reply Wait only if you are validating IP addresses. To validate the IP address, DHCP sends an ICMP echo (Ping) to determine whether the address is in use. The maximum time it waits for a reply depends on this setting. The default is 10 seconds.

9 To assign IP addresses dynamically, set the IP Group 1 parameter to the first address for the IP address pool.

10 Set the Group 1 Count parameter to the number of addresses in the pool. The pool can contain up to 20 addresses.

11 To define an additional address pool for dynamic address assignment, set the IP Group 2 parameter to the first address for the second IP-address pool.

12 Set the Group 2 Count parameter to the number of addresses in the pool. The second pool, which can also contain up to 20 addresses, is used only if there are no addresses available in the first pool.

13 To reserve an IP address for a particular host, set the Host 1 IP parameter to the IP address for the host.

14 Set the Host 1 Enet parameter to the MAC (Ethernet) address of the host. The MAC address is normally the Ethernet address of the network interface card that the host uses to connect to the local-area network. When the DHCP server receives an IP-address request from the host with this MAC address, it assigns that host the IP address you specified for the Host 1 IP parameter.

15 To reserve an IP address for another host, set the Host 2 IP parameter to the IP address for the host and set the Host 2 Enet parameter to the MAC (Ethernet) address of the host.

16 To reserve an IP address for another host, set the Host 3 IP parameter to the IP address for the host and set the Host 3 Enet parameter to the MAC (Ethernet) address of the host.

Setting up a DHCP server

To set up a DHCP server, set these required parameters:

```
DHCP Spoofing...
  DHCP Spoofing=Yes
  Always Spoof=Yes
  IP group 1=nnn.nnn.nnn.nnn/nn
  Group 1 count=n
```

For detailed information about each parameter, see the *MAX Reference Guide*.

Additionally, you can set these parameters:

```
  Renewal Time=nn
  IP group 2=0.0.0.0/0
  Group 2 count=0
  Host 1 IP=nnn.nnn.nnn.nnn/nn
  Host 1 Enet=0080c75Be95e
  Host 2 IP=0.0.0.0/0
  Host 2 Enet=000000000000
  Host 3 IP=0.0.0.0/0
  Host 3 Enet=000000000000
```

For detailed information about each parameter, see the *MAX Reference Guide*.

Setting up Plug and Play support

To set up Plug and Play, you must set the following parameters:

```
DHCP Spoofing...
  DHCP Spoofing=Yes
  DHCP PNP Enabled=Yes
```

For detailed information about each parameter, see the *MAX Reference Guide*.

Setting up DHCP spoofing

To set up DHCP spoofing, you must set the following parameters:

```
DHCP Spoofing...
  DHCP Spoofing=Yes
  Always Spoof=No
```

Additionally, you can set the following parameters:

```
  Renewal Time=nn
  Become Def. Router=Yes|No
  Dial If Link Down=Yes|No
  Validate IP=Yes
  Maximum no reply wait=n
```

For detailed information about each parameter, see the *MAX Reference Guide*.

Configuring Frame Relay

4

Introduction

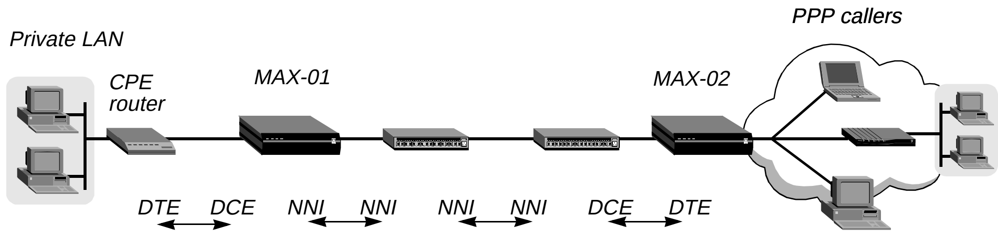
In the Frame Relay network, every access point connects directly to a switch. Frame Relay virtual circuits (VCs) are bidirectional data paths between two endpoints. An established permanent virtual circuit (PVC) is a connection between two endpoints, which can include a number of hops in between.

Depending on how a device such as the MAX is integrated into a Frame Relay network, it can operate as a Frame Relay terminating unit (Customer Premise Equipment or CPE) or as a Frame Relay switch.

A CPE is the source or destination of data traversing the Frame Relay service. For example, the MAX labeled MAX-02 in Figure 4-1 terminates the data stream to its PPP callers. When it is configured with a User-to-Network (UNI) interface to Frame Relay, the MAX acts as the user side (UNI-DTE) communicating with the network side (UNI-DCE) of a switch.

The network-side device connects the CPE device to a Frame Relay network. For example, the MAX labeled MAX-01 in Figure 4-1 receives Frame Relay encapsulated frames from a CPE and forwards them on to another Frame Relay switch. When it is configured with a UNI-DCE interface to Frame Relay, the MAX acts as the network side (UNI-DCE) communicating with the user side (UNI-DTE) of a Frame Relay device.

Figure 4-1. Frame Relay network



A Frame Relay switch is another kind of network-side device, which switches frames from one interface to another and exchanges status information with its peer switch. For example, the MAX labeled MAX-01 in Figure 4-1 receives frames from its peer switch and switches them to its other Frame Relay interface. When it is configured with a Network-to-Network (NNI) interface to Frame Relay, the MAX acts as a Frame Relay switch. Switch-to-switch communication includes both user side (NNI-DTE) and network side (NNI-DCE) functions.

Frame Relay link management

Frame Relay link management enables administrators to retrieve information about the status of the Frame Relay interface via special management frames with a unique Data Link Connection Identifier (DLCI) address. (DLCI 0 is the default for link management frames.) Link management frames are used to monitor the interface and provide information about DLCI status.

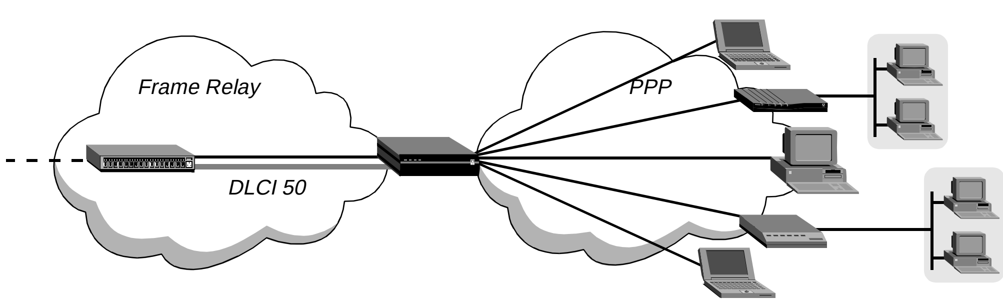
On a UNI interface to Frame Relay, link management procedures occur in one direction. The UNI-DTE device requests information and the UNI-DCE device provides it.

On an NNI interface, link management procedures are bidirectional. Switches perform both the NNI-DTE and NNI-DCE link management functions, since both sides of the connection request information from their peer switches.

Using the MAX as a Frame Relay concentrator

As a Frame Relay concentrator, the MAX forwards many lower-speed PPP connections onto one or more high-speed Frame Relay interfaces, as shown in Figure 4-2:

Figure 4-2. Frame Relay concentrator



In this kind of configuration, the decision to forward frames onto the Frame Relay interface can be made through OSI layer 3 (routing), or by Frame Relay Direct.

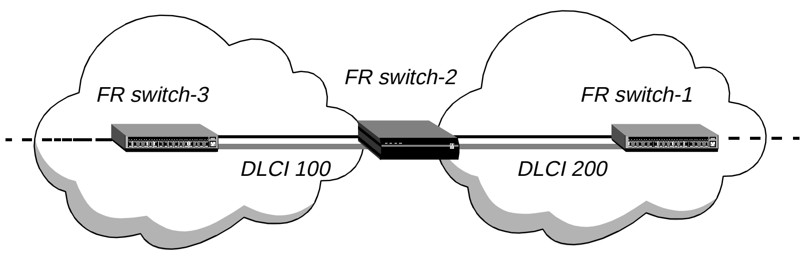
Using the MAX as a Frame Relay switch

As a Frame Relay switch, the MAX receives frames on one interface and transmits them on another interface. The decision to forward frames onto the Frame Relay interface is made through the assignment of circuit names. The MAX router software is not involved.

To use the MAX as a switch, you must configure a circuit that pairs two Frame Relay DLCI interfaces. Instead of going to the layer 3 router for a decision on which interface to forward the frames, it relies on the circuit configuration to relay the frames received on one interface to its paired interface. A circuit is defined in two Connection or RADIUS user profiles.

Figure 4-3 shows the MAX operating as a Frame Relay switch:

Figure 4-3. Frame Relay switch



Components of a Frame Relay configuration

The physical link to another Frame Relay device must be nailed (similar to a dedicated leased line). The administrator allocates nailed bandwidth in a line profile (the profile of a T1, E1, SWAN, or other network line).

The link interface to the Frame Relay device, which is also called a datalink, references specific nailed bandwidth in the MAX and defines the operations and link management functions the MAX performs on the interface. The administrator specifies these settings in a Frame-Relay profile or RADIUS frdlink pseudo-user profile.

The logical interface is a PVC endpoint, which requires a DLCI. DLCIs uniquely identify the logical endpoints of a virtual circuit (a specific end device). Administrators obtain DLCIs from Frame Relay providers and assign them in Connection profiles or RADIUS user profiles.

Configuring nailed bandwidth for Frame Relay

Each Frame Relay interface in the MAX requires its own nailed bandwidth, which is similar to a dedicated leased line.

Note: If you configure the bandwidth on nailed T1, make sure that the number of channels the MAX uses for the link matches the number of channels used by the device at the other end of the link, and that only one line profile specifies the Nailed-Group number to be used by the Frame Relay datalink.

Following are some examples of relevant parameters, shown with sample settings:

```
Net/T1 > Line Config > Line 1 > Ch 2=Nailed
Net/T1 > Line Config > Line 1 > Ch 2 Prt/Grp=1
Net/E1 > Line Config > Line 1 > Ch 2=Nailed
Net/E1 > Line Config > Line 1 > Ch 2 Prt/Grp=1
Serial WAN > Mod Config > Nailed Grp=1
```

Parameter	Specifies
Ch *N*	Switched or Nailed channel usage. To configure nailed bandwidth on a channelized T1 or E1 card, set to Nailed-64-Channel (a clear-channel 64K circuit). On unchannelized cards, this parameter does not apply.
Ch *N* Prt/Grp Nailed Grp	A number from 1 to 1024, used to identify nailed bandwidth. Frame-Relay profiles or RADIUS frdlink pseudo-user profiles specify this number to use the associated bandwidth.

For more details about configuring T1, see the *Hardware Installation Guide* for your MAX.

Defining Frame Relay link operations

A Frame-Relay profile defines datalink operations, including link management functions. The same settings can be specified in a RADIUS frdlink pseudo-user profile.

Note: Link management settings are optional. It is possible to set up a Frame Relay interface and pass data across it without setting these parameters. However, link management parameters provide a mechanism for retrieving information about the status of the interface and its DLCIs.

Settings in a Frame-Relay profile

Following are the Frame-Relay profile parameters, shown with sample settings:

```
Ethernet
   Frame Relay
      Name*=""
      Active=Yes
      Call Type=Nailed
      FR Type=NNI
      Nailed Grp=1
      Data Svc=56KR
      PRI # Type=N/A
      Dial #=N/A
      Bill #=N/A
      Call-by-Call=N/A
      Transit #=N/A
      Link Status Dlci=0
```

```
Link Mgmt=T1.617D
N391=6
DTE N392=3
DTE N393=4
DCE N392=3
DCE N393=4
T391=10
T392=15
MRU=1532
```

Understanding the Frame Relay parameters

This section provides some background information about the Frame Relay parameters. For detailed information about each parameters, see the *MAX Reference Guide*.

Name and Active

User connections link up with the Frame Relay connection specified in a Frame Relay profile by specifying the profile's name, which is defined by the name profile. The name must be unique and cannot exceed 15 characters.

Set the Active parameter to Yes to make the profile available for use.

LinkUp

The LinkUp parameter specifies whether the data link comes up automatically and stays up even when the last DLCI has been removed. If you set this parameter to No, the data link does not come up unless a Connection profile (DLCI) brings it up, and it shuts down after the last DLCI has been removed.

Note: You can start and drop Frame Relay data-link connections with the DO Dial and DO Hangup commands. DO Dial brings up a datalink connection. DO Hangup closes the link and any DLCIs on it. If LinkUp=Yes, DO HANGUP brings the link down, but it automatically restarts. A restart also occurs if a DLCI Connection (DLCI) profile invokes the data link.

FR Type

You can set the FR Type parameter to NNI (for an NNI interface to the switch), DCE (for a UNI-DCE interface), or DTE (for a UNI-DTE interface).

Call Type, telco options, and Data Svc

Nailed is the default call type for Frame Relay connections. When you set Call Type to Nailed, dial numbers and other telco options are N/A. You can specify Switched if the Frame Relay switch allows dial-in. However, Frame Relay networks currently have no dial-out connection capability. The two types of data service available are 64K and 56K.

Link management protocol

The Link Mgmt setting can be None (no link management), T1.617D (for T1.617 Annex D), or Q.933A (for Q.933 Annex A).

Frame Relay timers and event counts

Frame Relay timers and event counts function as follows:

- N391—Specifies the interval at which the MAX requests a Full Status Report (from 1 to 255 seconds). Is N/A if FR Type is DCE.
- DCE N392—Specifies the number of errors, during DCE N393 monitored events, that causes the network side to declare the user-side procedures inactive. The value should be less than that of DCE N393 (from 1 to 10). DCE N392 is N/A when FR Type is DTE.
- DCE N393—Specifies the DCE monitored event count (from 1 to 10). It is N/A when FR Type is DTE.
- DTE N392—Specifies the number of errors, during DTE N393 monitored events, that cause the user side to declare the network-side procedures inactive. The value should be less than that of DTE N393 (from 1 to 10). DTE N.392 is N/A when FR Type is DCE.
- DTE N393—Specifies the number of DTE monitored events per testing cycle (from 1 to 10). It is N/A when FR Type is DCE.
- T391—Specifies the Link Integrity Verification polling timer (from 5 to 30 seconds). The value should be less than that of T392. T391 is N/A when FR Type is DCE.
- T392—Specifies the interval for Status Enquiry messages (from 5 to 30 seconds). The MAX records an error message if it does not receive an Status Enquiry message within T392 seconds. This parameter is N/A when FR Type is DTE.

MRU (Maximum Receive Units)

The MRU parameter specifies the maximum number of bytes the MAX can receive in a single packet across this link. Usually the default of 1532 is the right setting, unless the far end device requires a lower number.

Settings in a RADIUS frdlink profile

An frdlink profile is a pseudo-user profile in which the first line has this format:

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

The *name* argument is the MAX system name (specified by the Name parameter in the System profile), and *N* is a number in a sequential series, starting with 1. Make sure there are no missing numbers in the series specified by *N*. If there is a gap in the sequence of numbers, the MAX stops retrieving the profiles when it encounters the gap in sequence.

The following attributes can be used to define a frdlink pseudo-user profile:

Attribute	Value
Ascend-FR-Profile-Name (180)	A Frame-Relay profile name (up to 15 characters), to be referenced in user profiles that make use of this datalink.

Attribute	Value
Ascend-FR-Nailed-Grp (158)	Group number assigned to nailed bandwidth in a line profile, such as a T1 or E1 profile. The default is 1. Make sure the Frame-Relay profile specifies the correct group number. If the channels are on nailed T1, make sure that the number of channels the MAX uses for the link matches the number of channels used by the device at the other end of the link, and that only one T1 profile specifies the Nailed-Group number to be used by the Frame Relay datalink.
Ascend-Call-Type (177)	Type of nailed connection: Nailed (1), Nailed/Mpp (2), or Perm/Switched (3). Nailed is the default.
Ascend-Data-Svc (247)	Type of data service on the nailed link.Typically set to Nailed-64K for a Frame Relay datalink.
Ascend-FR-Link-Mgt (160)	The link management protocol. Settings are Ascend-FR-No-Link-Mgt (0) (link management protocol is disabled), Ascend-FR-T1-617D (1) (Annex D), and Ascend-FR-Q-933A (2)(CCITT Q.933 Annex A). Ascend-FR-No-Link-Mgt is the default. To ensure interoperability with equipment from different vendors, the same version of management protocol must be used at each end of the Frame Relay link.
Ascend-FR-Type (159)	Type of operations performed by the MAX on this interface. Settings are Ascend-FR-DTE (0), Ascend-FR-DCE (1), or Ascend-FR-NNI (2). Ascend-FR-DTE is the default. (For more information, see “Examples of a UNI-DTE link interface” on page 4-8, “Examples of a UNI-DCE link interface” on page 4-9, and “Examples of an NNI link interface” on page 4-10.)
Ascend-FR-N391 (161)	Number of T391 polling cycles between full Status Enquiry messages. The default is 6, which indicates that after 6 status requests spaced Ascend-FR-T391 seconds apart, the UNI-DTE device requests a Full status report. Does not apply when Ascend-FR-Type is Ascend-FR-DCE.
Ascend-FR-DTE-N392 (163)	Number of errors which, if occurring in the number of DTE monitored events specified by Ascend-FR-DTE-N393, causes the user-side to declare the network-side procedures inactive. The value should be less than that of Ascend-FR-DTE-N393l (which can be from 1 to 10). The default value is 3. Does not apply when Ascend-FR-Type is Ascend-FR-DCE.
Ascend-FR-DTE-N393 (165)	DTE monitored event count (from 1 to 10). The default is 4. Does not apply when Ascend-FR-Type is Ascend-FR-DCE.
Ascend-FR-T391 (166)	Link Integrity Verification polling timer. The value should be less than that of Ascend-FR-T392. The default is 10, which indicates that after Ascend-FR-N391 status requests spaced 10 seconds apart, the UNI-DTE device requests a Full status report. Does not apply when Ascend-FR-Type is Ascend-FR-DCE.

Attribute	**Value**
Ascend-FR-T392 (167)	Interval in which Status Enquiry messages should be received (from 5 to 30 seconds). The default T392 value is 15. An error is recorded if no Status Enquiry is received within the specified number seconds. Does not apply when Ascend-FR-Type is Ascend-FR-DTE.
Framed-MTU (12)	Maximum number of bytes the MAX can transmit in a single packet across the link interface. Usually the default of 1532 is the right setting. However, the far-end device might require a lower number.
Ascend-FR-DCE-N392 (162)	Number of errors which, if occurring in the number of DCE monitored events specified by Ascend-FR-DCE-N393, causes the network-side to declare the user-side procedures inactive. The value should be less than that of Ascend-FR-DCE-N393 (which can be from 1 to 10). Does not apply when Ascend-FR-Type is Ascend-FR-DTE.
Ascend-FR-DCE-N393 (164)	DCE monitored event count (from 1 to 10). The default is 4. Does not apply when Ascend-FR-Type is Ascend-FR-DTE.
Ascend-FR-Link-Status-Dlci (106)	DLCI to use for LMI link management on the Frame Relay datalink. Valid values are DLCI0 (the default) and DLCI1023.

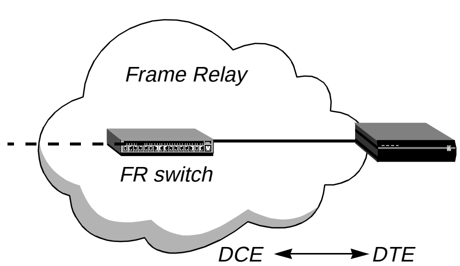
Examples of a UNI-DTE link interface

On a UNI-DTE interface, the MAX acts as the user side communicating with the network side DCE switch. It initiates link management functions by sending a Status Enquiry to the UNI-DCE device. Status Enquiries may include queries about the status of PVC segments the DTE knows about, as well as the integrity of the datalink between the UNI-DTE and UNI-DCE interfaces.

The UNI-DTE uses the values of the N391, N392, N393, and T391 parameters in the Frame-Relay profile to define the timing of its Status Enquiries to the DCE and its link integrity parameters. (These correspond to the Ascend-FR-N391, Ascend-FR-DTE-N392, Ascend-FR-DTE-N393, and Ascend-FR-T391 attributes in a RADIUS profile.)

Figure 4-4 shows an example of the MAX with a UNI-DTE interface.

Figure 4-4. Frame Relay DTE interface



The following parameters specify nailed group 11 as the bandwidth for the sample DTE interface. *Make sure that the Frame-Relay profile specifies the correct nailed group.*

```
Ethernet
   Frame Relay
      Active=Yes
      FR Type=DTE
      Nailed Grp=11
      Link Mgmt=Q.933A
```

With these link management settings, the MAX uses the CCITT Q.933 Annex A link management protocol to communicate with the Frame Relay DCE. It initiates link management functions by sending a Status Enquiry to the DCE every 10 seconds.

On a UNI-DTE interface, the state of a DLCI is determined by the Full status report from the DCE or by an async PVC update. The Full status report from the DCE specifies active and inactive and new DLCIs. If the DCE does not specify a DLCI as active or inactive, the DTE considers it inactive.

Following is a comparable RADIUS profile:

```
frdlink-max-1 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "fr-dte",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-DTE,
    Ascend-FR-Nailed-Grp = 11,
    Ascend-FR-Link-Mgt = Ascend-FR-Q-933A,
    Ascend-Data-Svc = Nailed-64K
```

Examples of a UNI-DCE link interface

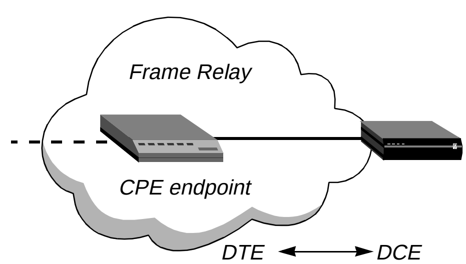
On a UNI-DCE interface, the MAX acts as the network side communicating with the user side (UN-DTE) of a Frame Relay terminating unit.

The UNI-DCE uses the values of the T392, DCE N392, and DCE N393 parameters in the Frame Relay profile to define the parameters of the Status Enquiries expected from the DTE. (These correspond to the Ascend-FR-T392, Ascend-FR-DCE-N392, and Ascend-FR-DCE-N393 attributes in a RADIUS profile.)

For example, if the MAX expects a Status Enquiry from the DTE every ten seconds, it records an error if it does not receive a Status Enquiry in ten seconds.

Figure 4-5 shows an example of the MAX with a UNI-DCE interface.

Figure 4-5. Frame Relay DCE interface



The following parameters specify nailed group 36 as the bandwidth for the sample DCE interface. *Make sure that the Frame-Relay profile specifies the correct nailed group.*

```
Ethernet
   Frame Relay
      Active=Yes
      FR Type=DCE
      Nailed Grp=36
      Link Mgmt=Q.933A
      T392=15
```

With these link management settings, the MAX uses the CCITT Q.933 Annex A link management protocol to communicate with the CPE endpoint. It expects a Status Enquiry at intervals less than seven seconds.

On a UNI-DCE interface, if the datalink is up, the DLCI is considered to be up as well. In the DCE Full status response to the DTE, if a PVC segment terminates within the DCE, it is reported as active. If the PVC segment is not terminated, the DCE has to request further information on the Frame Relay network. In that case, it requests information about the DLCI from the next hop switch, and reports back to the DTE when the segment is confirmed to be active or inactive.

Following is a comparable RADIUS profile:

```
frdlink-max-2 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "fr-dce",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-DCE,
    Ascend-FR-Nailed-Grp = 36,
    Ascend-FR-Link-Mgt = Ascend-FR-Q-933A,
    Ascend-Data-Svc = Nailed-64K,
    Ascend-FR-T392 = 15
```

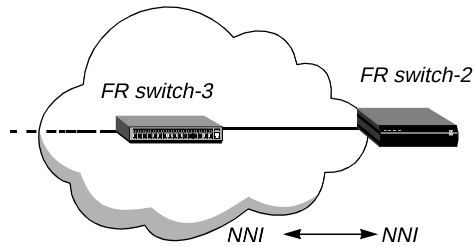
Examples of an NNI link interface

An NNI interface implements procedures used by Frame Relay switches to communicate status between them. The MAX uses these procedures to inform its peer switch about the status of PVC segments from its side of the Frame Relay network, as well as the integrity of the datalink between them. The procedure is bidirectional. The switches act as both the user side (DTE) and network side(DCE) in that they both send Status Enquiries and respond to them.

Because NNI is bidirectional, all of the link management values defined in the Frame-Relay profile are used. The values of the N391, N392, N393, and T391 parameters define the user side of the NNI. These values define the timing of the status enquiries the MAX MAX sends to its peer switch and the boundary conditions that define link integrity. The values of the T392l, DCE N392, and DCE N393 parameters are used by the network side of the NNI to define the parameters of the Status Enquiries it expects from the its peer switch.

Figure 4-6 shows a MAX with an NNI interface:

Figure 4-6. Frame Relay NNI interface



To operate as a switch, the MAX requires a hard-coded circuit configuration in two Connection profiles. It relies on the circuit configuration to relay the frames received on one of the circuit endpoints to the other circuit endpoint. For details about circuit configuration, see "Configuring the MAX as a Frame Relay switch" on page 4-23.

Note: The two Frame Relay endpoints that make up the circuit do not require NNI interfaces.

The following parameters specify the nailed group 52 as the bandwidth for the NNI interface to Switch-3 (Figure 4-6). *Make sure that the Frame-Relay profile specifies the correct nailed group.*

```
Ethernet
   Frame Relay
      Active=Yes
      FR Type=NNI
      Nailed Grp=52
      Link Mgmt=T1.617D
      N391=6
      T391=10
      T392=15
```

With these link management settings, the MAX uses the ANSI Annex D link management protocol to communicate with Switch-3. It sends a Status Enquiry for Link Integrity Verification to Switch-3 every 10 seconds, and requests a Full status report every sixth enquiry (every 60 seconds). It also sends a Full Status report in response to requests from the other switch. If it does not receive a Status Enquiry within a 15-second interval (T392), it records an error.

Following is a comparable RADIUS profile:

```
frdlink-max-3 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "switch-3",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-NNI,
    Ascend-FR-Nailed-Grp = 52,
    Ascend-FR-Link-Mgt = Ascend-FR-T1-617D,
    Ascend-Data-Svc = Nailed-64K,
    Ascend-FR-N391 = 6,
    Ascend-FR-T391 = 10,
    Ascend-FR-T392 = 15
```

Configuring a DLCI logical interface

A Connection profile defines a DLCI interface. The same settings can be specified in a RADIUS permconn pseudo-user profile.

Overview of DLCI interface settings

Administrators configure a Connection or RADIUS permconn profile that specifies a connection to a far end device across Frame Relay. The first hop of the connection is known by the DLCI assigned in the profile.

A DLCI is an integer between 16 and 991 that uniquely identifies a specific endpoint in the Frame Relay network. The Frame Relay administrator must provide a valid DLCI for each logical interface to a Frame Relay network.

Settings in a Connection profile

All connections that use Frame Relay must specify the name of a configured Frame Relay profile that defines the data link between the MAX and the Frame Relay network. Forwarded or routed connections over the Frame Relay link use the following sets of parameters (shown with sample settings):

```
Ethernet
   Answer
      Encaps...
         PPP=Yes
         FR=Yes

      PPP Options...
         Route IP=Yes
```

For gateway connections:

```
Ethernet
   Connections
      any Connection profile
         Encaps=FR
         Encaps options...
            FR Prof=pacbell
            DLCI=16
            Circuit=N/A

         Route IP=Yes

         Ip options...
         LAN Adrs=10.2.3.4/24
```

For Frame Relay circuits:

```
Ethernet
   Connections
      any Connection profile
         Encaps=FR_CIR
         Encaps options...
            FR Prof=pacbell
            DLCI=16
            Circuit=circuit-1
```

For FR Direct connections:

```
Ethernet
   Connections
      any Connection profile
         Encaps=PPP
         Route IP=Yes
         Ip options...
            LAN Adrs=10.2.3.4/24

         Session options...
            FR Direct=Yes
            FR Prof=pacbell
            DLCI=16
```

Understanding the Frame Relay connection parameters

This section provides some background information about the Frame Relay connection parameters. For detailed information about each parameter, see the *MAX Reference Guide*.

Gateway connections (Encaps=FR)

Gateway connections require FR encapsulation, a Frame Relay profile name, and a DLCI. Your Frame Relay provider tells you the DLCI to assign to each connection.

A Connection profile that specifies Frame Relay encapsulation must include a DLCI to identify the first hop of a permanent virtual circuit (PVC). The MAX does not allow you to enter duplicate DLCIs, except when they are carried by separate physical links specified in different Frame Relay profiles.

Frame Relay circuits (Encaps=FR_CIR)

A circuit is a PVC segment configured in two Connection profiles. Data coming in on the DLCI configured in one Connection profile is switched to the DLCI configured in the other. Data gets dropped if the circuit has only one DLCI. If more than two Connection profiles specify the same circuit name, the MAX uses only two DLCIs.

In a circuit, both Connection profiles must specify FR_CIR encapsulation and the same circuit name. Each profile must specify a unique DLCI. The MAX does not allow you to enter duplicate DLCIs, except when separate physical links specified in different Frame Relay profiles carry duplicate DLCIs.

FR Direct connections (FR Direct=Yes)

In an FR Direct connection, the MAX simply *attaches* a Frame Relay PVC to multiple Connection profiles. It does so in the Session Options subprofile, by enabling FR Direct, specifying a Frame Relay profile, and setting a DLCI for the PVC endpoint in the FR DLCI parameter. Any packet coming into the MAX on these connections gets switched out on the DLCI. In this mode, the MAX allows multiple Connection profiles to specify the same PVC (the same DLCI).

FR Direct is an unusual mode, in that the MAX ignores the destination of the packets. It assumes that some device at the far end of the PVC makes the routing decisions. The

Connection profile, however, must use IP routing to enable the MAX to route data back to the client.

Settings in a RADIUS profile

A permconn profile is a pseudo-user profile in which the first line has this format:

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

The *name* argument is the MAX system name (specified by the Name parameter in the System profile), and *N* is a number in a sequential series, starting with 1. Make sure there are no missing numbers in the series specified by *N*. If there is a gap in the sequence of numbers, the MAX stops retrieving the profiles when it encounters the gap in sequence.

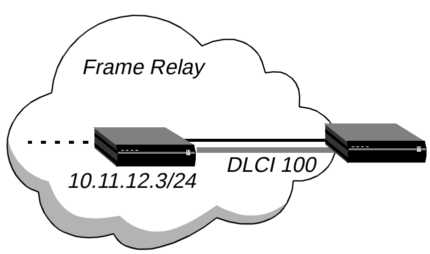
The following attributes can be used to define a permconn pseudo-user profile that uses Frame Relay:

Attribute	**Value**
User-Name (1)	Name of the far end Frame Relay device.
Framed-Protocol (7)	The encapsulation protocol. Must be set to FR (261).
Ascend-FR-Profile-Name (180)	Name of the Frame-Relay profile that defines the data link.
Ascend-FR-DLCI (179)	A DLCI for this PVC endpoint.The DLCI must be obtained from a Frame Relay provider. The MAX does not allow you to enter duplicate DLCIs, except when they are carried by separate physical links specified in different Frame-Relay profiles.
Ascend-Backup (176)	Name of a backup Connection profile to the next hop (optional). See “Examples of backup interfaces for nailed Frame Relay links” on page 4-15.

Examples of a DLCI interface configuration

In the following example, the MAX has a connection to a Frame Relay switch that also supports IP routing, as shown in Figure 4-7:

Figure 4-7. Frame Relay PVC



The following set of parameters configures the Connection profile, assigning DLCI 100:

```
Ethernet
   Connections
      any Connection profile
```

```
Active=Yes
Encaps=FR
IP options
   LAN Adrs=10.11.12.3/24
Encaps options
   FR Prof=fr-dce
   DLCI=100
Telco options
   Call Type=Nailed
```

Following is a comparable RADIUS profile:

```
permconn-max-1 Password = "ascend", User-Service = Dialout-Framed-User
    User-Name = "max-switch",
    Framed-Protocol = FR,
    Framed-Address = 10.11.12.3,
    Framed-Netmask = 255.255.255.0,
    Ascend-Route-IP = Route-IP-Yes,
    Ascend-FR-DLCI = 100,
    Ascend-FR-Profile-Name = "fr-dce"
```

Note: When IP routing is enabled, the MAX creates a route for this destination. Administrators can choose to add static routes to other subnets or to enable RIP updates to or from the router across Frame Relay. The usual considerations for IP routing connections apply (see Chapter 10, “Configuring IP Routing”).

Examples of backup interfaces for nailed Frame Relay links

On UNI-DTE and NNI interfaces, the MAX issues Status Enquiries that check the state of the other end of PVC segments on the interface. If a DLCI becomes inactive, and the profile configuring its nailed interface specifies a backup connection, the MAX uses the backup connection to provide an alternate route to the other end. For an introduction to backup interfaces, see “Examples of backup interfaces for nailed Frame Relay links” on page 4-15.

In the sample profiles that follow, the primary interface is a Frame Relay DLCI interface defined in a profile named `fp7`, and the backup interface is another DLCI interface defined in a profile named `pvc`. In this example, the remote IP address of the primary and the backup connection are different.

The following set of parameters defines the primary and backup interfaces in local Connection profiles:

```
Ethernet
   Connections
      fp7
         Name=fp7
         Active=Yes
         Encaps=FR
         IP options
            LAN Adrs=10.168.7.9/24
         Encaps options
            FR Prof=frt2-7
            DLCI=18
```

```
          Telco options
             Call Type=Nailed
          Session options
             BackUp=pvc

Ethernet
   Connections
      pvc
         Name=pvc
         Active=Yes
         Encaps=FR
         IP options
            LAN Adrs=10.168.7.11/24
         Encaps options
            FR Prof=frt1-7
            DLCI=16
         Telco options
            Call Type=Nailed
```

Following are comparable RADIUS profiles:

```
permconn-max1-1 Password = "ascend", User-Service = Dialout-Framed-
User
   User-Name = "fp7",
   Framed-Protocol = FR,
   Framed-Address = 10.168.7.9,
   Framed-Netmask = 255.255.255.0,
   Ascend-Route-IP = Route-IP-Yes,
   Ascend-Backup = "pvc",
   Ascend-Metric = 7,
   Ascend-FR-DLCI = 18,
   Ascend-FR-Profile-Name = "radius-frt2-7",
   Framed-MTU = 1524,
   Ascend-Call-Type = Nailed

permconn-max1-2 Password = "ascend", User-Service = Dialout-Framed-
User
   User-Name = "pvc",
   Framed-Protocol = FR,
   Framed-Address = 10.168.7.11,
   Framed-Netmask = 255.255.255.0,
   Ascend-Route-IP = Route-IP-Yes,
   Ascend-Metric = 7,
   Ascend-FR-DLCI = 16,
   Ascend-FR-Profile-Name = "radius-frt1-7",
   Framed-MTU = 1524,
   Ascend-Call-Type = Nailed
```

When the MAX brings up the two Frame Relay PVC, the routing table includes entries such as this:

```
...
```

```
10.168.7.0/24    10.168.7.9     wan33     rGT     60    1     0    89
10.168.7.0/24    10.168.7.9     wan33     *SG    120    7     0   198
10.168.7.9/32    10.168.7.9     wan33     rT      60    1     0    89
10.168.7.9/32    10.168.7.9     wan33     *      120    7         198
10.168.7.11/32   10.168.7.11    wan32     rT      60    1     0    51
10.168.7.11/32   10.168.7.11    wan33     *S     120    1          89
...
```

At this point, both nailed connections are up, and the output of the Ifmgr command contains entries such as the following:

```
bif slot sif u m p ifname   host-name remote-addr      local-addr
--------------------------------------------------------------------
032 1:03 001 *   p wan32    pvc       10.168.7.11/32   11.168.6.234/32
033 1:03 002 *   p wan33    fp7       10.168.7.9/32    11.168.6.234/32
```

If the primary PVC becomes unavailable, the routing table does not change, but the entries in the output of the Ifmgr command look like the following output:

```
bif slot sif u m p ifname  host-name  remote-addr      local-addr
--------------------------------------------------------------------
032 1:03 001 *   p wan32    pvc       10.168.7.11/32   11.168.6.234/32
033 1:17 000 +   p wan33    fp7       10.168.7.9/32    11.168.6.234/32
```

Notice that `fp7` is shown with a plus-sign (+) to show that it is in the Backup Active state (that it is backed up by another connection). When the primary PVC comes up again, the data flow is directed to that interface again. At that point, the Ifmgr command output again shows both interfaces as up.

Concentrating incoming calls onto Frame Relay

A common way to concentrate incoming connections onto a Frame Relay link is by making use of OSI layer 3 (IP routing). For this purpose, the MAX requires ordinary profiles for the callers, and a DLCI logical interface that specifies a destination IP router. When clients dial in to reach the destination router, the MAX consults its routing table to forward the packets onto Frame Relay. In this type of configuration, the MAX acts as a Frame Relay gateway.

For incoming PPP connections, Frame Relay Direct is another way to concentrate the calls onto a Frame Relay link. Frame Relay Direct aggregates multiple PPP connections and forwards them as a combined data stream solely on the basis of the FR-Direct specifications. The assumption is that an upstream device will examine the packets and route them appropriately.

Note: A Frame Relay Direct connection is not a full-duplex tunnel between a PPP dial-in and a far-end device. Although the MAX does not use the router to forward packets onto the Frame Relay link, it must use the router to send packets received across Frame Relay back to the appropriate PPP caller. For this reason, Frame Relay Direct connections must enable IP routing.

Setting up a Frame Relay gateway

To act as a Frame Relay gateway, the Frame Relay DLCI profile must specify a destination router. Incoming connections are routed in the usual way, and all of the usual options apply.

Administrators can choose to create static routes, enable or disable RIP, and so forth. For details, see Chapter 10, "Configuring IP Routing."

For background information about specifying a DLCI interface, see "Configuring a DLCI logical interface" on page 4-12.

Routing parameters in the DLCI profile

In addition to the Frame Relay settings described in "Overview of DLCI interface settings" on page 4-12, the following Connection parameters are relevant to a gateway DLCI profile:

```
Ethernet
   Connections
      any Connection profile
         Route IP=Yes
      IP options
         LAN Adrs=0.0.0.0/0
```

Parameter	Specifies
Route IP	Enables/disables IP routing for this connection. It is enabled by default, and must be enabled for a Frame Relay gateway.
LAN Adrs	Destination IP address, which lies at the end of a PVC whose first hop is known by the specified DLCI.

Routing parameters in RADIUS

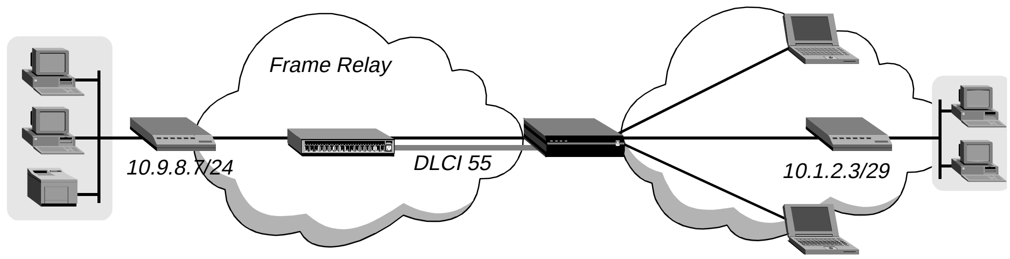
In addition to the attributes described in "Overview of DLCI interface settings" on page 4-12, the following attribute-value pairs must be specified in the permconn profile of a Frame Relay gateway:

Attribute	Value
Ascend-Route-IP (228)	Enables/disables IP routing for this connection. (IP is enabled by default. If this attribute is present, it must be set to Route-IP-Yes for Frame Relay gateway connections.)
Framed-Address (8)	Destination IP address, which lies at the end of a PVC whose first hop is known by the specified DLCI.
Framed-Netmask (9)	A subnet mask for Framed-Address.

Examples of a gateway configuration

In the following example, the MAX acts as a gateway between a client that dials in with the address 10.1.2.3/29, and a remote router that is reachable across Frame Relay, as shown in Figure 4-8:

Figure 4-8. Frame Relay gateway



The following set of parameters configures an MP+ Connection profile for the dial-in client in Figure 4-8:

```
Ethernet
   Connections
      mpp-client
         Name=mpp-client
         Active=Yes
         Encaps=MPP
         Encaps options
            Recv PW=clientpw
         IP options
            LAN Adrs=10.1.2.3/29
```

Following is a comparable RADIUS profile:

```
mpp-client Password = "clientpw", User-Service = Dialout-Framed-User
    Framed-Protocol = MPP,
    Framed-Address = 10.10.1.3,
    Framed-Netmask = 255.255.255.248
```

The next set of parameters configures a DLCI Connection profile to the CPE router:

```
Ethernet
   Connections
      cpe-router
         Name=cpe-router
         Active=Yes
         Encaps=FR
         IP options
            LAN Adrs=10.9.8.7/24
         Encaps options
            FR Prof=fr-dte
            DLCI=55
```

Following is a comparable RADIUS profile:

```
permconn-max-2 Password = "ascend", User-Service = Dialout-Framed-User
    User-Name = "cpe-router",
    Framed-Protocol = FR,
    Framed-Address = 10.9.8.7,
    Framed-Netmask = 255.255.255.0,
```

```
Ascend-Route-IP = Route-IP-Yes,
Ascend-FR-DLCI = 55,
Ascend-FR-Profile-Name = "fr-dte"
```

Note: The MAX creates a route for this destination and uses it to forward packets from PPP clients. Administrators can choose to add static routes to other subnets or to enable dynamic routing updates to or from the router across Frame Relay. The usual considerations for IP routing connections apply (see "Configuring IP Routing" on page 10-1).

Configuring Frame Relay Direct

When a PPP Connection profile specifies FR-Direct, the MAX simply forwards the data stream out on a specified DLCI interface. It leaves the task of routing the packets to an upstream device.

For background information about specifying a DLCI interface, see "Configuring a DLCI logical interface" on page 4-12.

Settings in a Connection profile

Following are the relevant FR-Direct parameters, shown with sample settings:

```
Ethernet
   Connections
      any Connection profile
         Active=Yes
         Encaps=PPP
         Route IP=Yes
         Encaps options
            Recv PW=clientpw
         IP options
            LAN Adrs=10.111.112.113/24
         Session options
            FR Direct=Yes
            FR Prof=
            FR Dlci=16
```

Parameter	Specifies
Encaps	Specifies the supported encapsulation protocol. Must be set to PPP, MP, or MPP for Frame Relay Direct connections.
FR Direct	Enables/disables FR-Direct mode for this connection.
FR Prof	Specifies the name of the Frame Relay profile that defines the datalink.
FR Dlci	DLCI assigned in a Connection profile to a next hop on the specified interface. Multiple FR-Direct Connection profiles can refer to the same DLCI in this setting.

Parameter	Specifies
Route IP	Enables/disables IP routing for this connection. Must be enabled for the MAX to send data back to the appropriate PPP caller.
LAN Adrs	Specifies the PPP caller's IP address. As the MAX receives return packets for many Frame Relay Direct connections on the same DLCI, it uses this address to determine which PPP caller should receive the return packets.

Settings in a RADIUS profile

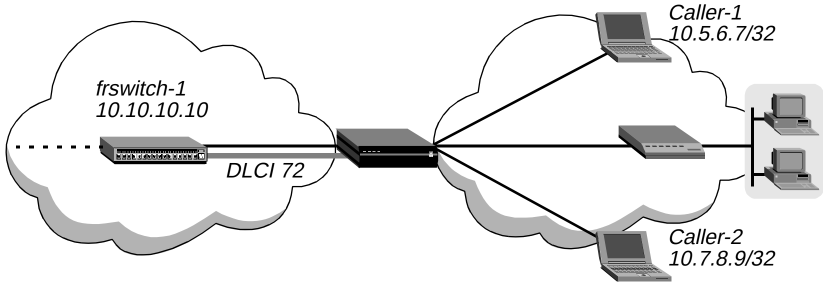
Following are the relevant RADIUS attributes for FR-Direct connections:

Attribute	Value
Framed-Protocol (7)	The encapsulation protocol. Must be set to PPP (1), MP (262), or MPP (256) for FR-Direct connections.
Ascend-FR-Direct (219)	Enables/disables FR-Direct mode for this connection. FR-Direct-No (0) is the default. Set to FR-Direct-Yes (1) for FR-Direct connections.
Ascend-FR-Direct-Profile (220)	Name of the Frame-Relay profile that defines the datalink.
Ascend-FR-Direct-DLCI (221)	DLCI assigned in a Connection profile to a next hop on the specified interface. Multiple FR-Direct Connection profiles can refer to the same DLCI in this setting.
Ascend-Route-IP (228)	Enables/disables IP routing for this connection. (IP is enabled by default. If this attribute is present, it must be set to Route-IP-Yes to enable the MAX to send data back to the appropriate PPP caller.
Framed-Address (8)	PPP caller's IP address. As the MAX receives return packets for many Frame Relay Direct connections on the same DLCI, it uses this address to determine which PPP caller should receive the return packets.
Framed-Netmask (9)	A subnet mask for Framed-Address.

Examples of FR-Direct connections

In the following example, the MAX forwards the data stream from two PPP dial-in hosts across Frame Relay on the same DLCI interface, as shown in Figure 4-9:

Figure 4-9. Frame Relay Direct



The following parameters specify the DLCI interface to frswitch-1 in Figure 4-9:

```
Ethernet
   Connections
      frswitch-1
         Name=frswitch-1
         Active=Yes
         Encaps=FR
         IP options
            LAN Adrs=10.10.10.10/24
         Encaps options
            FR Prof=fr-dte
            DLCI=72
```

Following is a comparable RADIUS profile:

```
permconn-max-3 Password = "ascend", User-Service = Dialout-Framed-User
    User-Name = "frswitch-1",
    Framed-Protocol = FR,
    Framed-Address = 10.10.10.10,
    Framed-Netmask = 255.255.255.0,
    Ascend-Route-IP = Route-IP-Yes,
    Ascend-FR-DLCI = 72,
    Ascend-FR-Profile-Name = "fr-dte"
```

The following set of parameters configures FR Direct Connection profiles for the incoming calls:

```
Ethernet
   Connections
      caller-1
         Name=caller-1
         Active=Yes
         Encaps=PPP
         Encaps options
            Recv PW=caller1*3
         IP options
            LAN Adrs=10.5.6.7/32
         Session options
            FR Direct=Yes
            FR Prof=fr-dte
```

```
            FR Dlci=72

Ethernet
   Connections
      caller-2
         Name=caller-2
         Active=Yes
         Encaps=PPP
         Route IP=Yes
         Encaps options
            Recv PW=caller2!!8
         IP options
            LAN Adrs=10.5.6.7/32
         Session options
            FR Direct=Yes
            FR Prof=fr-dte
            FR Dlci=72
```

Following are comparable RADIUS profiles:

```
caller-1 Password = "caller1*3", User-Service = Framed-User
    Framed-Protocol = PPP,
    Framed-Address = 10.5.6.7,
    Framed-Netmask = 255.255.255.255
    Ascend-FR-Direct = FR-Direct-Yes,
    Ascend-FR-Direct-Profile = "fr-dte",
    Ascend-FR-Direct-DLCI = 72
caller-2 Password = "caller2!!8", User-Service = Framed-User
    Framed-Protocol = PPP,
    Framed-Address = 10.7.8.9,
    Framed-Netmask = 255.255.255.255
    Ascend-FR-Direct = FR-Direct-Yes,
    Ascend-FR-Direct-Profile = "fr-dte",
    Ascend-FR-Direct-DLCI = 72
```

Configuring the MAX as a Frame Relay switch

As a Frame Relay switch, the MAX receives frames on one DLCI interface and transmits them on another one. The decision to forward frames is made on the basis of circuit name assignments.

To use the MAX as a switch, you must configure a circuit that pairs two DLCI interfaces. Instead of going to the layer 3 router for a decision on which interface to forward the frames, it relies on the circuit name to relay the frames to the paired interface. A circuit is defined in two Connection profiles, one for each endpoint of the circuit.

Note: When it is operating as a switch, the MAX relays all frames received on one endpoint of the circuit to the other endpoint of the circuit. It does not examine the packets at OSI layer 3.

Overview of circuit-switching options

With a Frame Relay circuit configuration, the MAX can operate as a switch on UNI-DCE interfaces, NNI interfaces, or a combination of the two. NNI is not required.

Routing parameters or attributes should be disabled for switched connections.

Note: Make sure that the Enabled parameter is set to Yes in the Answer-Defaults FR-Answer subprofile.

Settings in a Connection profile

Following are the relevant circuit parameters, shown with sample settings:

```
Ethernet
   Connections
      caller-1
         Name=caller-1
         Active=Yes
         Encaps=FR-Cir
         Encaps options
            FR Prof=max
            DLCI=100
            FR Circuit=frcir1
```

Parameter	Specifies
Encaps	Encapsulation protocol. Both endpoints of the circuit must specify Frame-Relay-Circuit encapsulation.
FR Prof	Name of the Frame-Relay profile that defines the datalink.
DLCI	A DLCI for this PVC endpoint.The DLCI must be obtained from a Frame Relay provider. The MAX does not allow you to enter duplicate DLCIs, except when they are carried by separate physical links specified in different Frame-Relay profiles.
FR Circuit	Circuit name (up to 16 characters). The other endpoint must specify the same circuit name. If only one profile specifies a circuit name, data received on the specified DLCI is dropped. If more than two profiles specify the same circuit name, only two of the profiles will be used to form a circuit.

Settings in a RADIUS profile

Following are the RADIUS attributes for configuring a Frame Relay circuit:

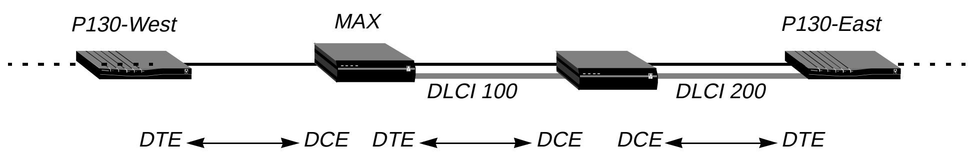
Attribute	Value
Framed-Protocol (7)	Encapsulation protocol. Both endpoints of a circuit must specify FR-CIR (263) encapsulation.
Ascend-FR-Profile-Name (180)	Name of the Frame-Relay profile that defines the datalink.

Attribute	**Value**
Ascend-FR-DLCI (179)	A DLCI for this PVC endpoint. The MAX does not allow you to enter duplicate DLCIs, except when they are carried by separate physical links specified in different Frame-Relay profiles.
Ascend-FR-Circuit-Name (156)	Circuit name (up to 16 characters). The other endpoint must specify the same circuit name. If only one profile specifies a circuit name, data received on the specified DLCI is dropped. If more than two profiles specify the same circuit name, only two of the profiles will be used to form a circuit.

Examples of a circuit between UNI interfaces

Figure 4-10 shows a circuit configuration using UNI-DCE interfaces in the MAX:

Figure 4-10. Frame Relay circuit with UNI interfaces



Using local profiles

The following parameters on the MAX define the datalinks to the MAX and to the Pipeline 130 (P130-East):

```
Ethernet
   Frame Relay
      max
         Name=max
         Active=Yes
         FR Type=DCE
         Nailed Grp=111

Ethernet
   Frame Relay
      p130east
         Name=p130east
         Active=Yes
         FR Type=DCE
         Nailed Grp=222
```

The next set of parameters specifies the circuit between the two Frame Relay interfaces:

```
Ethernet
   Connections
      max6
         Name=max6
         Active=Yes
```

```
            Encaps=FR-Cir
            Route IP=No
            Encaps options
               FR Prof=max
               DLCI=100
               FR Circuit=frcir1

Ethernet
   Connections
      p130
         Name=p130
         Active=Yes
         Encaps=FR-Cir
         Encaps options
            FR Prof=p130east
            DLCI=200
            FR Circuit=frcir1
```

Using RADIUS profiles

The following RADIUS frdlink pseudo-user profiles define the datalinks to the MAX and to the Pipeline 130 (P130-East):

```
frdlink-max-21 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "max",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-DCE,
    Ascend-FR-Nailed-Grp = 111

frdlink-max-22 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "p130east",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-DCE,
    Ascend-FR-Nailed-Grp = 222
```

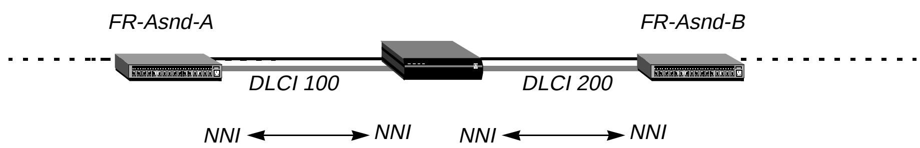
The next set of profiles specifies the circuit between the two Frame Relay interfaces:

```
permconn-max-10 Password = "ascend" , User-Service = Dialout-Framed-
User
    User-Name = "max6",
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 100,
    Ascend-FR-Profile-Name = "max",
    Ascend-FR-Circuit-Name = "fr-cir1"

permconn-max-11 Password = "ascend", User-Service = Dialout-Framed-
User
    User-Name = "p130",
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 200,
    Ascend-FR-Profile-Name = "p130east",
    Ascend-FR-Circuit-Name = "fr-cir1"
```

Examples of a circuit between NNI interfaces

Figure 4-11 shows a circuit configuration that uses NNI interfaces:

Figure 4-11. Frame Relay circuit with NNI interfaces



Using local profiles

The following parameters on the MAX define the datalinks to the two switches labeled FR-Asnd-A and FR-Asnd-B:

```
Ethernet
   Frame Relay
      fr-asnd-a
         Name=fr-asnd-a
         Active=Yes
         FR Type=NNI
         Nailed Grp=333

Ethernet
   Frame Relay
      fr-asnd-b
         Name=fr-asnd-b
         Active=Yes
         FR Type=NNI
         Nailed Grp=444
```

The next set of parameters specifies the circuit between the two Frame Relay interfaces:

```
Ethernet
   Connections
      asnd-a
         Name=asnd-a
         Active=Yes
         Encaps=FR-Cir
         Route IP=No
         Encaps options
            FR Prof=fr-asnd-a
            DLCI=100
            FR Circuit=pvc-pipe

Ethernet
   Connections
      asnd-b
         Name=asnd-b
         Active=Yes
```

```
Encaps=FR-Cir
Route IP=No
Encaps options
   FR Prof=fr-asnd-b
   DLCI=200
   FR Circuit=pvc-pipe
```

Using RADIUS profiles

The following frdlink pseudo-user profiles define the datalinks to the two switches labeled FR-Asnd-A and FR-Asnd-B:

```
frdlink-max-23 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "fr-asnd-a",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-NNI,
    Ascend-FR-Nailed-Grp = 333

frdlink-max-24 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "fr-asnd-b",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-NNI,
    Ascend-FR-Nailed-Grp = 444
```

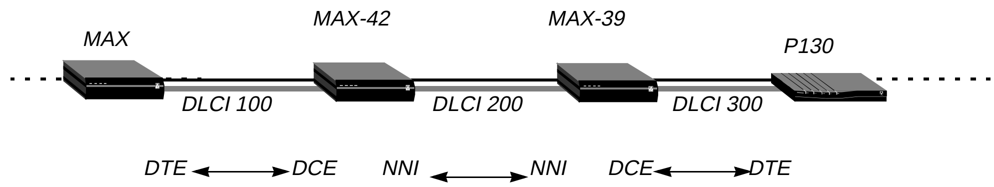
The next set of profiles specifies the circuit between the two Frame Relay interfaces:

```
permconn-max-12 Password = "ascend", User-Service = Dialout-Framed-
User
    User-Name = "asnd-a",
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 100,
    Ascend-FR-Profile-Name = "fr-asnd-a",
    Ascend-FR-Circuit-Name = "pvc-pipe"

permconn-max-13 Password = "ascend", User-Service = Dialout-Framed-
User
    User-Name = "asnd-b",
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 200,
    Ascend-FR-Profile-Name = "fr-asnd-b",
    Ascend-FR-Circuit-Name = "pvc-pipe"
```

Examples of circuits that use UNI and NNI interfaces

Figure 4-12 shows circuit configurations that use one UNI-DCE and one NNI interface:

Figure 4-12. Frame Relay circuit with UNI and NNI interface



Using local profiles

The following parameters on MAX-42 define the datalinks to the MAX and MAX-39:

```
Ethernet
   Frame Relay
      dce-max
         Name=dce-max
         Active=Yes
         FR Type=DCE
         Nailed Grp=555

Ethernet
   Frame Relay
      nni-39
         Name=nni-39
         Active=Yes
         FR Type=NNI
         Nailed Grp=999
```

The next set of parameters on MAX-42 specifies the circuit between its two Frame Relay interfaces:

```
Ethernet
   Connections
      max
         Name=max
         Active=Yes
         Encaps=FR-Cir
         Route IP=No
         Encaps options
            FR Prof=dce-max
            DLCI=100
            FR Circuit=cir-42

Ethernet
   Connections
      max39
         Name=max39
```

```
        Active=Yes
        Encaps=FR-Cir
        Route IP=No
        Encaps options
           FR Prof=nni-39
           DLCI=200
           FR Circuit=cir-42
```

The following parameters on MAX-39 define the datalinks to MAX-42 and to the Pipeline 130:

```
Ethernet
   Frame Relay
      nni-42
         Name=nni-42
         Active=Yes
         FR Type=NNI
         Nailed Grp=777

Ethernet
   Frame Relay
      dce-p130
         Name=dce-p130
         Active=Yes
         FR Type=dce
         Nailed Grp=888
```

The next set of parameters on MAX-39 specifies the circuit between its two Frame Relay interfaces:

```
Ethernet
   Connections
      max42
         Name=max42
         Active=Yes
         Encaps=FR-Cir
         Route IP=No
         Encaps options
            FR Prof=nni-42
            DLCI=200
            FR Circuit=cir-39

Ethernet
   Connections
      max39
         Name=max39
         Active=Yes
         Encaps=FR-Cir
         Route IP=No
         Encaps options
            FR Prof=dce-p130
```

```
DLCI=300
FR Circuit=cir-39
```

Using RADIUS profiles

The following profiles define the datalinks from MAX-42 to the MAX and MAX-39:

```
frdlink-max-25 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "dce-max",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-DCE,
    Ascend-FR-Nailed-Grp = 555

frdlink-max-26 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "nni-39",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-NNI,
    Ascend-FR-Nailed-Grp = 999
```

The next set of profiles specifies the circuit on MAX-42:

```
permconn-max-14 Password = "ascend", User-Service = Dialout-Framed-
User
    User-Name = "max"
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 100,
    Ascend-FR-Profile-Name = "dce-max",
    Ascend-FR-Circuit-Name = "cir-42"

permconn-max-15 Password = "ascend", User-Service = Dialout-Framed-
User
    User-Name = "max39",
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 200,
    Ascend-FR-Profile-Name = "nni-39",
    Ascend-FR-Circuit-Name = "cir-42"
```

The following profiles define the datalinks from MAX-39 to MAX-42 and the Pipeline 130:

```
frdlink-max-27 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "nni-42",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-NNI,
    Ascend-FR-Nailed-Grp = 777

frdlink-max-28 Password = "ascend", User-Service = Dialout-Framed-User
    Ascend-FR-Profile-Name = "dce-p130",
    Ascend-Call-Type = Nailed,
    Ascend-FR-Type = Ascend-FR-DCE,
    Ascend-FR-Nailed-Grp = 888
```

The next set of profiles specifies the circuit on MAX-39:

```
permconn-max-16 Password = "ascend", User-Service = Dialout-Framed-
User
    User-Name = "max42"
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 200,
    Ascend-FR-Profile-Name = "nni-42",
    Ascend-FR-Circuit-Name = "cir-39"
permconn-max-17 Password = "ascend", User-Service = Dialout-Framed-
User
    User-Name = "p130",
    Framed-Protocol = FR-CIR,
    Ascend-Route-IP = Route-IP-No,
    Ascend-FR-DLCI = 300,
    Ascend-FR-Profile-Name = "dce-p130",
    Ascend-FR-Circuit-Name = "cir-39"
```

Configuring switched Frame Relay connections

You can enable the MAX to support Frame Relay switched connections over ISDN BRI or PRI connections. A switched Frame Relay connection provides either a 56K or 64K connection, depending on the ISDN network configuration.

Overview

When a Frame Relay profile and an associated Connection profile are configured for a switched Frame Relay connection, the Connection profile can establish a Frame Relay session either by placing an outgoing call or by matching the CLID or DNIS of an incoming call. Once the session is established, it behaves just like a nailed Frame Relay connection with an access rate of 64K or 56K, depending on the ISDN network configuration. Authentication can be by DNIS and CLID.

Switched Frame Relay connections support the same logical interfaces as do nailed connections: NNI, DTE, and DCE.

Keep the following information in mind:

- Your Frame Relay service provider must allow switched Frame Relay connections.
- A switched Frame Relay connection is a point-to-point connection and supports only one DLCI.
- Verify that the Committed Information Rate of the DLCI(s) using switched connections allow 56K or 64K connections.

Configuring a switched Frame Relay connection

To set up a switched Frame Relay connection, you must perform the following general steps:

1. Set up a Frame Relay profile as follows:
   – Call Type set to Switched
   – FR Type set to NNI, DTE, or DCE, depending on the network configuration
   – FR Prof set to the name of the Frame Relay encapsulated Connection profile
   – Data link information specified as given to you by your service provider
2. Set up a Frame Relay encapsulated Connection profile as follows:
   – Encaps set to FR
   – Call Type set to Switched
   – Dial#, Calling# and Called# specified if you are authenticated with CLID or DNIS
   –
3. Set up the Answer profile as follows:
   – FR set to Yes
   – Profile Reqd set to Yes
   – Id Auth set to Require (for CLID) or set to Called Require (for DNIS), depending on the authentication

Configuring a Frame Relay profile

The following example shows how to configure a switched Frame Relay NNI connection, but you configure a switched DCE or DTE connection similarly.

To configure a Frame relay profile for a Frame Relay switched connection, proceed as in the following example:

1. Open Ethernet > Frame Relay> *any profile*
2. Specify a Name. For example:
   `Station=fr-sw-fr`
3. Set Active to Yes.
4. Set Call Type to Switched.
5. Set FR Type=NNI.
6. Specify the data link information as given to you by your Frame Relay Service provider.
7. Exit and save the Frame Relay profile.

Configuring a Connection profile

Next, to configure a Connection profile for a Frame Relay switched connection, proceed as in the following example:

1. Open Ethernet > Connection > *any profile*
2. Specify a Station Name. For example:
   `Station=fr-sw-conn`

3. Set Active to Yes.
4. Set Encaps to FR.
5. Open the Encaps Options submenu.
6. Specify the name of the Frame Relay profile that uses this Connection profile. For example:

   `FR Prof=fr-sw-fr`
7. Specify the DLCI for this Frame Relay connection. For example:

   `DLCI=165`
8. Open the Telco Options submenu.
9. Set Call Type to Switched.

   You can only set Call Type to Switched if the Frame Relay Profile associated with it also has Call Type set to Switched.
10. If necessary, set AnsOrig to control whether the MAX establishes the Frame Relay connection for incoming or outgoing connections.
11. Exit the Telco Options submenu.
12. If you are authenticating with CLID or DNIS, specify a Dial#, Calling# and Called#.
13. If necessary, open the Session options submenu and set the Idle parameter to the number of seconds inactive sessions remain connected. For example:

    `Idle=120`
14. Exit and save the Connection profile.

Configuring the Answer profile

To allow incoming calls to bring up the Frame Relay connection, configure the Answer profile as in the following example:

1. Open Ethernet > Answer.
2. Set Profile Reqd=Yes.
3. If necessary, set the Id Auth parameter as follows:
   – Require (for CLID)
   – Called Require (for DNIS)
4. Open the Encaps Options submenu.
5. Set FR to Yes.
6. Exit and save the Answer profile.

Establishing the connection

To bring up the Frame Relay manually, open the Connection profile and press Ctrl-D, then select `1=Dial`.

If you configure an Answer profile, an incoming call with the correct CLID or DNIS brings up the session.

AppleTalk Routing

5

Introduction to AppleTalk routing

The MAX functions as an AppleTalk internet router, providing routing functions for AppleTalk nodes (Macintosh workstations or Apple printers) that are connected to the MAX over Ethernet or a WAN. MAX routing supports the following AppleTalk protocols:

- Datagram Delivery Protocol (DDP)
- Routing Table Maintenance Protocol (RTMP)
- AppleTalk Echo Protocol (AEP)
- Zone Information Protocol (ZIP)
- Name Binding Protocol (NBP)
- AppleTalk Control Protocol (ATCP— for router-to-router applications)

When to use AppleTalk routing

Use AppleTalk routing to connect two or more networks that have AppleTalk nodes such as Mac OS computers or Apple printers. The primary benefits of routing AppleTalk traffic (as opposed to bridging this traffic) are:

- Gives you more control over calls
- Reduces broadcast and multicast traffic over the WAN
- Provides startup information to local AppleTalk devices

Reducing broadcast and multicast traffic

Because AppleTalk uses multicast and broadcast addresses extensively, routing AppleTalk can greatly improve the efficiency of a LAN or WAN. By using AppleTalk zones to segment traffic, you can significantly reduce the amount of broadcast and multicast traffic on a LAN or WAN. When you set up a router for the first time, you identify the cable range (network-number range) for the subnetwork segment and one or more zones.

For example, when a user on a network without a router selects a device in the Chooser, the MAC OS computer sends out a Name Binding Protocol (NBP) Lookup as a broadcast packet. Because a bridge forwards all broadcast traffic, all devices on the network receive the Lookup packet. A router can significantly reduce AppleTalk traffic over the WAN because it does not forward broadcast traffic from one subnetwork to another, but stops it at the subnetwork port of the router.

Zone multicasting is intended to prevent any node not in the destination zone for the lookup from receiving the lookup packet. Any AppleTalk node responds only to NBP lookups for that node's zone name. In the example in the preceding paragraph, a router would convert the Broadcast Request packet generated by the Lookup request to a Forward Request packet for each network that contains nodes in the target zone specified by the Lookup request.

A bridge can filter directed traffic between two specific nodes but cannot filter broadcast or multicast traffic, since there is not a specific port that can be assigned to a multicast or broadcast address. This means that although filters used with bridging can reduce the number of AppleTalk packets sent to remote network segments, bridging does not reduce the number of broadcast and multicast packets over these networks.

Providing dynamic startup information to local devices

In addition to routing services, the Ascend AppleTalk router provides startup information to AppleTalk stations. As with other routed protocols, AppleTalk station, or *node,* addresses consist of a unique network number/node combination. AppleTalk addresses are dynamically assigned when a node starts up. In addition, the router provides an AppleTalk node with the network cable range to which it is attached, and supplies zone name information.

Understanding AppleTalk zones and network ranges

AppleTalk zones and network ranges are configured in AppleTalk routers. Network numbers are assigned to network segments, and must be unique within the internetwork. A network range is a range of network numbers specified the port descriptor of the router port and then transmitted through RTMP to the other nodes of the network. Each of the numbers within a network range can represent up to 253 devices.

AppleTalk zones

A zone is a multicast address containing an arbitrary subset of the AppleTalk nodes in an internet. Each node belongs to only one zone, but a particular extended network can contain nodes belonging to any number of zones. Zones provide departmental or other groupings of network entities that a user can easily understand.

In the Ascend AppleTalk router, zone names are case-insensitive. However, because some routers regard zone names as case-sensitive, you should be consistent in spelling zone names when you configure multiple connections or routers.

Extended and nonextended AppleTalk networks

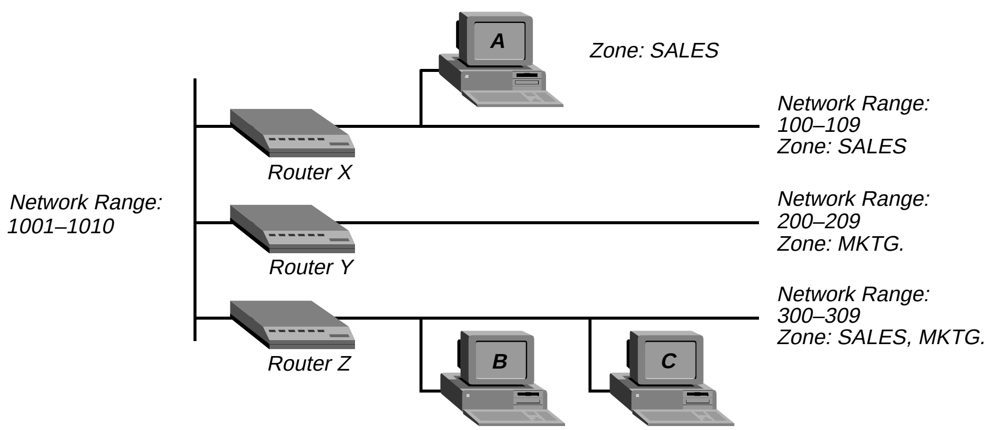
AppleTalk subnetworks are either nonextended or extended. Nonextended networks theoretically allow up to 254 nodes. A nonextended network has one network number (not a range) and one zone.   Examples of nonextended networks are LocalTalk and ARA dial-up networks.

An extended network is a group of nonextended networks on the same physical data link, and contains a range of network numbers. Each network in the range supports up to 253 devices. EtherTalk and TokenTalk are examples of extended networks.

At least one router on a network, called the seed router, must have the network number range specified in its port description. Other routers on the network can have a network range of 0 (zero), which specifies that they acquire the network-number range from RTMP packets sent by the seed router. AppleTalk routers on a network must not have conflicting network-number ranges for that network. A zero value does not cause a conflict, but otherwise, all seed routers on the same network must have the same value for the start and end of the network-number range.

Figure 5-1 shows a network with three routers and three zones configured. Each zone has a range of network numbers.

Figure 5-1. AppleTalk LAN



Router X, Router Y, and Router Z connect to the backbone network (Range 1001-1010). Each router has an additional connection to a local network segment. For example, Router X has a connection to the network range 100-109. User A’s computer also connects to the 100-109 range.

Because Router X is configured with only one zone, any AppleTalk device joining the segment belongs to the SALES zone. But User B’s computer can belong to either the SALES zone or the MKTG. zone. Some AppleTalk devices allow you to select the zone to which they belong. If there is no way to manually assign the zone, the AppleTalk device is put into the *default* zone, which is defined on the AppleTalk router.

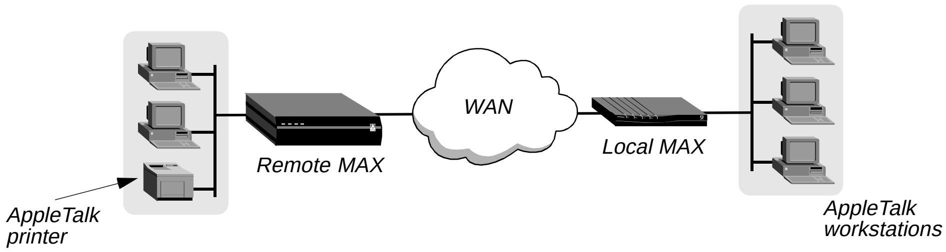
Figure 5-1 shows two important concepts about network numbers and zones. When a network range is defined, all values within that range are unusable for any other segment. The segment to which user C’s computer connects uses network range 300-309. No other network segment in this AppleTalk network can use network numbers 300, 301, 302, etc., in their ranges. As an example, network number 310 *is* available to a new network segment

Zones can be shared among network segments. In Figure 5-1, network 100-109 supports zone SALES. So does network 300-309.

Understanding how AppleTalk works

Figure 5-2 illustrates a connection between a workstation on a MAX that is connected to another MAX over a synchronous PPP WAN connection.

Figure 5-2. Routed connection



Following is a brief description of how a workstation user sees a typical AppleTalk connection. The steps describe in a general way what is happening as the user makes the choices that lead to a connection:

1 An AppleTalk workstation user opens the Macintosh Chooser for the first time since it has been attached to the router and configured.

2 The workstation sends a ZIP Query to obtain an updated zone list from the local MAX, and the MAX returns the updated zone list. This list might contain different zones than did the initial list.

3 The user selects a zone and a specific device in the Chooser.

4 The workstation sends a Name Binding Protocol (NBP) Broadcast Request to the MAX, which checks its Zone Information Table (ZIT) to determine which subnetwork that printer is located in, and sends the request to the remote MAX via the port configured in the Connection profile.

5 The remote MAX determines the port to which the subnetwork is attached and performs the lookup in the appropriate multicast address (multicast addresses are assigned to zones).

6 All devices in the appropriate zone on the subnetwork detect and process the NBP Lookup packet.

7 The selected printer obtains the sender’s address from the Lookup packet (in this case the routers are *forwarders* and the workstation is the *sender*) and sends the reply through the routers to the workstation.

8 The user sends the print job to the printer.

9 When the print job is complete and no data packets are passing through the connection, the MAX units continue to pass routing information.

Configuring AppleTalk routing

To configure AppleTalk routing, you must set system-level parameters in the Ethernet Mod COnfig profile and, if required for caller authentication, in the Answer profile. In addition, you can configure AppleTalk for specific connections, You can also configure AppleTalk connections in RADIUS.

System-level AppleTalk routing parameters

To set the required parameters in the Ethernet Mod Config profile:

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

2 Set AppleTalk to Yes.

Otherwise you cannot configure the remaining parameters.

3 In the Ethernet > Mod Config > AppleTalk Options menu, set the Zone Name parameter to the name of any of the zones assigned to the network segment to which the Ascend unit is connected. Enter up to 33 alphanumeric characters. For example, for router X in Figure 5-1:

```
50-C00 Mod Config
    AppleTalk Options...
      Peer=Router
     >Zone Name=SALES
      AppleTalk Router=Seed
      Net Start=300
      Net End=309
      Default Zone=SALES
      Zone Name #1=MKTG
      Zone Name #2=ENGINEERING
      Zone Name #3=
      Zone Name #4=
```

4 Set the AppleTalk Router parameter to Seed or Non-Seed to specify whether the Ascend unit is a seed or nonseed router. For example:

```
50-C00 Mod Config
    AppleTalk Options...
      Peer=Router
     >Zone Name=SALES
      AppleTalk Router=Seed
      Net Start=300
      Net End=309
      Default Zone=SALES
      Zone Name #1=MKTG
      Zone Name #2=ENGINEERING
      Zone Name #3=
      Zone Name #4=
```

A seed router has a manually defined network configuration. When a nonseed router boots, it has no local network configuration. It examines local network traffic and learns its local network configuration.

Note: You should configure the MAX as a nonseed router provided there is *at least one* seed router on the local network. Having only one seed router on a local network simplifies potential network configuration changes. Should you need to change the network numbering, only the seed router needs to be reconfigured. The remaining nonseed routers simply need to be rebooted to learn the changes.

5 If the MAX is to be a seed router, set the Net Start and Net End parameters to specify the range for the network to which the unit is attached. (For example, the menu shown in step 4 specifies a range of 300–309.)

If there are other seed routers sharing the MAX unit's network segment, this information must be identical on *all* routers that *share the network segment*. If there are no other seed routers, every network number from Net Start to Net End must be unique for the entire internet. Valid network numbers are of from 1–65,534.

6 If the MAX is to be a seed router, specify the default-zone name assigned to the local AppleTalk network segment. Enter up to 33 alphanumeric characters in the Default Zone field. (For example, the menu shown in step 4 specifies SALES as the default zone.)

AppleTalk routers assign the default zone to any AppleTalk device that is connected to the local Ethernet segment but has not explicitly been assigned to another zone.

Note: Zones can be shared across network segments. However, the Default Zone and list of additional zones need to be identical for any AppleTalk router sharing the local network segment.

7 If the MAX is to be a seed router, specify the names of any other zones assigned to the network segment to which the MAX is connected. Enter up to 33 alphanumeric characters in each of one or more of the Zone Name fields. (For example, the menu shown in step 4 specifies MKTG in the Zone Name #1 field and SALES, MKTG in Zone Name #2.)

Answer profile parameter

If you configure the MAX to authenticate with names and passwords, enable AppleTalk routing in the Ethernet > Answer profile by setting Route AppleTalk=Yes. For example:

```
90-800 Answer
  PPP Options...
  >Route IP=No
   Route IPX=No
   Route AppleTalk=Yes
   Bridge=Yes
   Recv Auth=None
   MRU=1524
```

(You cannot set the Route AppleTalk parameter if AppleTalk is set to No in the Ethernet Configuration profile or if AppleTalk Router is set to Off in that profile's AppleTalk Options submenu.)

Per-connection AppleTalk routing parameters

To enable AppleTalk routing for a specific connection:

1 Open Ethernet > Connections > *any Connection profile*.

2 Set Route AppleTalk to Yes.

You cannot set the Route AppleTalk parameter unless you set Ethernet > Mod Config > AppleTalk Options > AppleTalk to No or Ethernet > Answer profile > Route AppleTalk to No in the Answer profile.

3 Set the Encaps parameter to PPP, MPP, or MP.

4 Set Dial # to the number the MAX dials when it receives AppleTalk data that it should forward to the remote network specified by this profile.

5 Open the AppleTalk Options menu.

6 Set Zone Name to specify the zone name for the AppleTalk router at the remote end of the connection. For example:

```
90-101 Macintosh 1
  >AppleTalk options...
    Peer=Router
    Zone Name=ENGINEERING
    Net Start=2001
    Net End=2010
```

This zone name appears in the AppleTalk Zones window of the Chooser. If the WAN segment for the zone is not already connected when packets for the zone are received (for example, when a user selects this zone in the Chooser, and then selects AppleShare), the MAX places a call to the number in the Dial # field of the Connection profile.

7 Enter the network range in the Net Start and Net End fields.

This range defines the networks available for packets that are to be routed to this static route. Valid entries for these fields are in the range from 1–65,534. All routes that share a network segment must specify the same network range.

Configuring an AppleTalk connection with RADIUS

You can configure an AppleTalk-routed connection in a RADIUS user profile and configure static AppleTalk routes in a RADIUS pseudo-user file. For more information, see the *MAX RADIUS Configuration Guide.*

Reading more about AppleTalk

This chapter provides only a very brief description of AppleTalk networking. For more complete information, see the following books:

Apple Computer. *Inside Macintosh: Networking.*

Chappell, Laura A., and Roger L. Spicer. *Novell's Guide to Multiprotocol Internetworking*.

Sidhu, Andrews, and Alan B. Oppenheimer. *Inside AppleTalk, Second Edition.*

Cougias, Dell, and Heiberger. *Designing AppleTalk Network Architectures.*

Configuring X.25

6

Introduction to Ascend X.25 implementation

This chapter describes how the MAX supports X.25. The CCITT Blue Book Recommendation X series 1988 has full technical specifications for X.25, X.3, X.28, X.29, and Link Access Protocol–Balanced (LAPB). IETF RFC 1356 has the technical specification for IP over X.25 (X25/IP).

X.25 is a connection oriented (virtual circuits) protocol, providing services such as multiplexing, in-sequence delivery, transfer of addressing information, segmenting and reassembly, flow control, error control, reset, and restart. Allocation of logical channels can be either static (PVC) or dynamic (SVC).

Configuring the MAX to communicate with an X.25 network involves the following elements:

- A physical interface to the X.25 network. This can be a nailed serial-WAN, one of the D-channels in T1 or E1 PRI, or a BRI D-channel connection. The MAX supports only one physical X.25 connection. (To configure the interface, see Chapter 2, “Configuring the MAX for WAN Access.”)
- A logical datalink to the X.25 network. Defined in an X.25 profile, the link should normally be set in DTE. See “Configuring the logical link to an X.25 network” on page 6-2.
- Dial-in connections (defined in Connection profiles) may use X.25. The application layer of an X.25 connection can be a TCP/IP network connection or terminal emulation using X.25 Packet Assembler/Disassembler (PAD).

The MAX supports PPP encapsulation over X.25 as defined in RFC 1598. There are advantages to using PPP/X.25 instead of IP/X.25. PPP/X.25 supports:

- STAC compression
- PAP authentication
- multiprotocol encapsulation including: IP routing, IPX routing, Appletalk routing, and bridging

Configuring the logical link to an X.25 network

An X.25 profile defines the logical data link between the MAX and a remote X.25 network. The Ethernet menu contains X.25 profiles, which include the following parameters (shown with sample settings):

```
Ethernet
   X.25
    any X.25 profile
      Name=
      Active= No
      Call Type=Nailed
      Nailed Grp=1
      Data Svc=56K
      Tei #=N/A
      PRI #=N/A
      Dial #=N/A
      Bill #=N/A
      Call-by-Call=N/A
      Transit #=N/A
      LAPB T1=3
      LAPB T2=0
      LABP N2=20
      LAPB k=7
      X.25 Seq Number Mode=NORMAL
      X.25 Link Setup Mode=ACTIVE
      X.25 Node Type=DTE
      X.25 window size=2
      X.25 pkt size=128
      X.25 Min pkt size=64
      X.25 Max pkt size=1024
      X.25 lowest PVC=0
      X.25 highest PVC=0
      X.25 lowest SVC=1
      X.25 highest SVC=8
      X.25 Clear/Diag=Yes
      X.25 Reset/Diag=Yes
      X.25 Restart/Diag=Yes
      X.25 options=NPWS
      X.25 Rev Charge Accept=No
      X.25 Network Type=CCITT
      X.25 T20=18
      X.25 R20=1
      X.25 T21=20
      X.25 T22=18
      X.25 T22=1
      X.25 R23=18
```

```
X.25 R23=1
X.121 src addr=
VCE Timer Val=300
```

Understanding the X.25 parameters

This section provides some background information about the X.25 parameters. For detailed information about each of these parameters, see the *MAX Reference Guide*.

Profile name and activation

User connections link up with the connection specified in an X.25 profile by specifying the profile’s name. The name must be unique and cannot exceed 15 characters.

To make the profile available for use, set the Active parameter to Yes.

Type of connection

The Call-Type parameter specifies the type of physical connection, which can be nailed or switched (X.25 PAD requires nailed). For a nailed connection, specify the Nailed Grp number. For a switched connection, specify the Dial # and telco options.

LAPB and reliable data transfer

The X.25 frame layer implements Link Access Protocol–Balanced (LAPB), an HDLC-like protocol that facilitates the exchange of information packets. To configure LAPB, set the following parameters:

- LAPB T1—Maximum number of seconds the transmitter waits for acknowledgment before initiating a recovery procedure (Response timeout). The default is 3 seconds.
- LAPB T2—Maximum number of milliseconds LAPB waits for outgoing data before sending a Restart-Request packet to the network. The default of 0 (zero) specifies immediate acknowledgment.
- LAPB N2—How many times the MAX can resend a frame when the LAPB T1 timer expires. The default is 20. This relatively high value increases the probability of a correct transfer of data.
- LAPB K—Maximum number of sequentially numbered frames that can be unacknowledged at a given time. This value is also called the Level 2 Window Size or the Frame Window Size. The default is 7. Higher values enable faster throughput.

X.25 packet handling

The X.25 packet layer defines the packet format as well as the procedures for the exchange of packets containing control information and user data. The following parameters control X.25 packet handling:

- X.25 Seq Number Mode selects between modulo 8 (Normal) and modulo 128 (Extended) sequence-number mode.
- X.25 Link Setup Mode specifies whether the X.25 link comes up in active- or passive-disconnect mode. In active-disconnect mode (the default), the link layer sends a DISC, and the packet layer sends a Restart-Request packet, upon initialization. In

passive-disconnect mode, the link layer sends SABM(E), upon initialization and issues a restart to the network only upon receipt of a Restart-Request packet. It does not issue a Restart-Request packet upon initialization, but responds to Restart packets it receives.

- X.25 Node Type specifies whether the MAX interacts with the remote end of the connection as a DTE (the default) or a DCE (when emulating the X.25 network).
- X.25 Window Size is the default for maximum number of outstanding data packets that can accumulate before the MAX requires an acknowledgment. The default is 2.
- X.25 packet-size parameters as specify the default, maximum, and minimum number of bytes in the data field of a data packet.

X.25 PVC and SVC numbers

The X.25 Lowest PVC and X.25 Highest PVC parameters define a range of PVCs from 1 to 4096. If the lowest PVC number is zero, no PVCs are supported.

The X.25 Lowest SVC and X.25 Highest SVC parameters define a range of SVCs from 1 to 4096. If the lowest SVC number is zero, no SVCs are supported.

X.25 diagnostic fields in packet types

X.25 Clear/Diag specifies whether Clear-Request packets include the diagnostic field. The default is No.

X.25 Reset/Diag specifies whether Reset-Request packets include the diagnostic field. The default is No.

X.25 Restart/Diag specifies whether Restart-Request packets include the diagnostic field. The default is No.

X.25 options

The X.25 options parameter can be set to None (no options) or NPWS (specifying that the MAX negotiates packet and window size). The default is None.

X.25 reverse charge accept

The X.25 RevChargeAccept parameter specifies whether the MAX accepts packets that request charge reversal. The default is No.

X.25 network type

Currently, the MAX supports only the CCITT network type.

Timer and limit for Restart-Requests

The X.25 T20 parameter sets the duration of the Restart timer (the number of ten-second ticks the MAX waits before retransmitting a Restart-Request packet). The corresponding X.25 R20 parameter specifies the number of Restart-Request retransmits the MAX sends before waiting indefinitely for a response.

Timer for Call-Requests

The X.25 T21 parameter sets the duration of the Call-Request timer (the number of ten-second ticks the MAX waits before clearing an unacceptable outgoing call).

Timer and limit for Reset-Requests

The X.25 T22 parameter sets the duration of the Reset-Request timer (the number of ten-second ticks the MAX waits before retransmitting a Reset-Request packet). The corresponding R22 parameter specifies the number of times the MAX retransmits a Reset-Request packet before clearing a call.

Timer and limit for Clear-Requests

The X.25 T23 parameter sets the duration of the Clear-Request timer (the number of ten-second ticks the MAX waits before retransmitting a Clear-Request packet). The corresponding R23 parameter specifies the number of Clear-Request retransmits the MAX sends before waiting indefinitely for a response.

X.121 source address

The X.121 Src Addr parameter specifies the MAX source address for logical links defined in the X.25 profile. An X.121 address contains from 1 to 15 decimal digits (for example, 031344159782738.)

Virtual Call Establishment (VCE) timer value

The VCE Timer Val parameter specifies the number of seconds to maintain a connection to a character-oriented device, such as a terminal server, that has not established a virtual call. This timer value is link-wide. Each X.25 PAD connection has a parameter to enable or disable this timer on a per-connection basis. A value of 0 (zero) disables the timer systemwide, regardless of the value of each connection’s VC-timer-enable flag. The default is 300 seconds.

Example of an X.25 profile configuration

This example focuses on an X.25 profile that establishes the logical link to an X.25 switch. It does not show how to configure the nailed channels used for the physical connection to the switch. For details about how to configure physical nailed connections, see Chapter 2, “Configuring the MAX for WAN Access.”

You must obtain a copy of the telco’s subscription form containing the values provisioned in the switch and then configure the MAX X.25 profile to comply with those values.

Table 6-1 shows a sample telco subscription form and the corresponding settings to enter in an X.25 profile:

Table 6-1. Sample telco subscription form

Subscription-item	Value	X.25 profile setting
Maximum seconds the transmitter waits for acknowledgment before starting recovery procedure (T1)	5	LAPB T1=5
Maximum times to resend a frame after the T1 timer expires (N2)	10	LAPB N2=10
Maximum sequentially numbered frames that a given DTE/DCE link can have unacknowledged at any given time (K)	7	LAPB K=7
Is the X.25 node a DTE or DCE?	DTE	X.25 Node Type=DTE
Is the link SVC or PVC?	SVC	X.25 Link Setup Mode=Active X.25 Lowest PVC=1 X.25 Highest PVC=8
Maximum packet size	1024	X.25 Max Pkt Size=1024
Maximum number of data packets that can be outstanding between a DTE and a DCE before acknowledgment is required (W)	2	X.25 Window Size=2
Number of PVCs	0	X.25 Lowest PVC=0
Highest PVC channel number	0	X.25 Highest PVC=0
Default packet size	256	X.25 Pkt Size=256
Minimum packet size	64	X.25 Min Pkt Size=64
Maximum packet size	1024	X.25 Max Pkt Size=1024

To configure the X.25 profile to comply with the subscription form in this example:

1 Open the X.25 profile, assign the profile a name, and activate it:

```
Ethernet
   X.25...
     any X.25 profile
        Name=ATT
       Active=Yes
```

2 Set Call Type to Nailed and specify the nailed group number:

```
Call Type=Nailed
Nailed Grp=7
```

3 Set the LAPB parameters to comply with the settings in the subscription form:

```
 LAPB T1=5
 LAPB T2=0
 LAPB N2=10
LAPB k=7
```

4 Set the X.25 Node Type to DTE, as specified in the subscription form:

```
X.25 Node Type=DTE
```

5 Configure the profile to support up to 8 switched virtual circuits:

```
 X.25 Link Setup Mode=ACTIVE
 X.25 lowest PVC=0
 X.25 highest PVC=0
 X.25 lowest SVC=1
 X.25 highest SVC=8
```

6 Configure packet sizes and flow control:

```
X.25 window size=2
X.25 pkt size=128
X.25 Min pkt size=64
X.25 Max pkt size=1024
```

7 Specify the X.121 source address to use on this link:

```
X.121 src addr=031344159782738
```

8 Close the X.25 profile.

Configuring X.25 IP connections

This section describes how to configure the MAX to exchange IP datagrams over the X.25 network connection specified in an X.25 profile. X.25 IP connections must be routed. They cannot be bridged. Following are the related parameters (shown with sample settings):

```
Ethernet
  Answer
      Encaps...
      X25/IP=Yes

Ethernet
  Connections
    any Connection profile
      Encaps=X25/IP

      Encaps options...
         X.25 Prof=ATT
         LCN=0
         Encaps Type=RFC877
         Reverse Charge=No
         RPOA=1234
         CUG Index=
         NUI=
         Max Unsucc. calls=0
         Inactivity Timer=0
         MRU=1500
         Call Mode=Both
         Answer X.121 Addr=
         Remote X.121 addr=

      Route IP=Yes
```

```
Ip options...
   LAN Adrs=10.65.212.226/24
```

For detailed information about each parameter, see the *MAX Reference Guide*.

Understanding the X.25 IP connection parameters

This section provides some background information about the X.25 IP connection parameters and the required IP configuration for this type of connection. For detailed information about each parameter, see the *MAX Reference Guide*.

X.25 Prof

The X.25 Prof parameter specifies a 15-character text field containing the name of an X.25 profile that the MAX uses for the logical connection. If the specified X.25 profile cannot be found, the MAX does not start a session for this Connection profile. As a safeguard against such misconfiguration, an active Connection profile specifying X.25 encapsulation cannot be saved unless you define the named X.25 profile and make it active.

LCN

The LCN parameter specifies the logical channel number to use in the case of a PVC. The default of 0 (zero) specifies that the MAX does not provide a (logical channel number) number, so the connection is not a PVC.

Encap Type

The encapsulation type can be RFC877 (for backward compatibility), SNAP, or NULL (multiplexing). The Encaps Type parameter specifies which encapsulation to use when calling the remote site. When receiving a call, the MAX accepts any of the three types of encapsulation. The default is RFC877.

Reverse Charge

The Reverse Charge parameter specifies whether the X.25 facility field indicates *reverse charge request* when the X.25 user calls a host. The default is No.

RPOA

The RPOA parameter specifies the set of Recognized Private Operating Agency (RPOA) user facilities to use in the next call request. The RPOA facilities provide the data network identification code for the requested initial RPOA transit network. You can specify up to 4 digits. The default is null.

CUG Index

The CUG Index parameter specifies the Closed User Group (CUG) index facility to use in the next call request. The CUG index facility specifies for the called switch, the closed user group selected for a virtual call. You can specify up to two digits. The default is null.

NUI

The NUI parameter specifies the set of Network User Identification (NUI) related facilities to use in the next call request. NUI provides information to the network for billing, security, network management purposes, and activation of subscribed facilities. You can specify the NUI, consisting of up to six digits, to use in the next call request. The default is null.

Max Unsucc. calls

You can specify the maximum number of unsuccessful X.25 calls that the MAX can attempt before it drops the modem connection. The default of 0 (zero) allows an unlimited number.

Inactivity Timer

The Inactivity Timer parameter specifies the number of seconds the MAX allows a connection to remain inactive before it drops the virtual circuit.

MRU

The MRU parameter specifies the maximum number of bytes the MAX can receive in a single IP packet on the X.25 link. If the MRU is larger than the X.25 packet size, the IP packet is further fragmented to fit the maximum X.25 packet size. The default is 1500 bytes.

Call Mode

The Call Mode parameter specifies whether the MAX can initiate a call request on the connection. The parameter has three possible settings:

- Incoming—The MAX does not issue a call request when data shows up for forwarding. If there is no virtual circuit is established, the MAX drops the IP packet. If a host receives an incoming call from a host whose address matches the Answer X.121 address (below), the MAX accepts the call.
- Outgoing—The MAX issues a call request to the Remote X.121 address setting when data shows up for forwarding. If the MAX does not establish a virtual circuit and the MAX receives an incoming call request, the MAX rejects the call.
- Both—The MAX accepts incoming call requests and issues a call request to the Remote X.121 address setting when data shows up for forwarding. The called address must match the Answer X.121 address. If the MAX does not establish a virtual circuit and IP packets arrive, the MAX issues a call request to the Remote X.121 address.

Answer X.121 Address

The Answer X.121 Addr parameter specifies the X.121 address of the remote X.25 host to which the profile defines a connection. The remote host must also support RFC1356 encapsulation of IP packets. This setting must not be left blank if you set Call Mode to Both or Incoming.

Remote X.121 address

The Remote X.121 Addr parameter specifies the X.121 address of the remote X.25 host to which the profile defines a connection. The remote host must also support RFC1356 encapsulation of IP packets. This setting must not be left blank if you set Call Mode to Both or Outgoing.

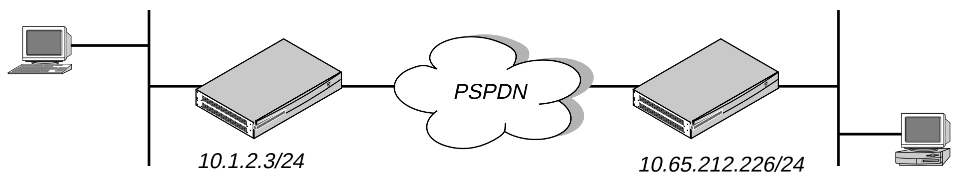
IP configuration parameters

The IP configuration for an X.25 IP connection is identical to an IP routing connection that uses PPP encapsulation. You must set the LAN Adrs parameter to the address of the remote Ascend unit. If you are using numbered interfaces, you can also specify a local IF Adrs and a remote WAN Alias value. For details about IP routing configurations, see Chapter 10, “Configuring IP Routing.”

Example of an X.25 IP configuration

This section shows a sample configuration that enables two IP networks to connect through a Public or Private Packet Switched Network, as shown in Figure 6-1.

Figure 6-1. Example of an X.25 IP connection



To configure this sample connection:

1 Open the Answer profile and enable X.25 IP encapsulation:

```
Ethernet
   Answer
      Encaps...
         X25/IP=Yes
```

2 Open a Connection profile, name it, and activate the profile:

```
Ethernet
   Connections
     any Connection profile
      Name=newyork
      Active=Yes
```

3 Enable IP routing and specify the IP address of the answering unit:

```
Route IP=Yes
Ip options...
   LAN Adrs=10.65.212.226/24
```

4 Enable X.25/IP encapsulation and then open the Encaps Options subprofile.

5 Specify the name of the X.25 profile that carries this connection:

```
Encaps=X25/IP
Encaps options...
   X.25 Prof=ATT
```

6 Set the inactivity timer. (to 30 seconds, for example):

```
   Inactivity Timer=30
```

7 Set the call mode and the local and remote X.121 addresses:

```
Call Mode=Both
Answer X.121 Addr=031344159782111
Remote X.121 addr=031344159782111
```

8 Close the Connection profile.

Configuring X.25 PAD connections

An X.25 Packet Assembler/Disassembler (PAD) is an asynchronous terminal concentrator that enables several terminals to share a single network line. It has its own command interface and uses an X.3 profile to fine-tune its parameters.

When a user calls an X.25 PAD through a modem, a digital modem processes and forwards the call to the terminal server. The terminal server authenticates the call, using the password specified in the caller's Connection profile, and establishes the session. If the MAX does not authenticate the session, either because an unauthenticated user enters the PAD command at the terminal-server prompt or because you use the terminal server's immediate X25/PAD services, the MAX uses X.25 parameters specified in the Answer Profile.

When the MAX establishes the session, the caller can see the terminal-server command line or is directed immediately to an X.121 host. If the connection auto-calls an X.121 host, the initial session display is similar to the following:

```
ATDT 555-1212
CONNECT 9600
ASCEND TERMINAL PAD v0.99:  ASYNC PORT # 1, 9600 BAUD
*
```

If the MAX directs the user to the terminal-server command line, the user sees the terminal-server login banner. The user can then establish a PAD session by using the PAD command. For example:

```
ascend% pad
*
```

(The asterisk is the PAD prompt for input.) The user can then place a call. For example:

```
*call 031344159782738
```

For more details, see "X.25 PAD commands" on page 6-20. This section describes how to configure X.25 PAD connections. Following are the related parameters (shown with sample settings):

```
Ethernet
   Answer
      PAD options...
         X25 Prof=
         X.3 Param Prof=CRT
         VC Timer enable=DISABLE
         Auto-Call X.121 addr=
         Reverse Charge=No
         RPOA=
         CUG Index=
        NUI=
```

```
Ethernet
   Connections
    any Connection profile
      Encaps=X25/PAD
      Encaps options...
         X.25 Prof=
         Recv PW=localpw
         X.3 Param Prof=CRT
         VC Timer enable=DISABLE
         Auto-Call X.121 addr=
         Reverse Charge=No
         RPOA=1234
         CUG Index=
         NUI=
         PAD banner msg=
         PAD prompt=
         NUI prompt=
         NUI PW prompt=
         PAD Alias #1=
         PAD Alias #2=
         PAD Alias #3
```

Understanding the X.25 PAD connection parameters

This section provides some background information about the X.25 PAD connection parameters. For detailed information about each parameter, see the *MAX Reference Guide*.

Auto-Call X.121 Addr

The Auto-Call X.121 Addr parameter specifies an X.25 host to call immediately when the MAX uses the x or x profile in which you set the parameter to establish an X.25/PAD session. If you set this parameter to specify an address, the PAD session can begin automatically. Otherwise, the MAX displays the terminal-server prompt, where the user can enter the PAD command to begin a session.

CUG Index

The CUG Index parameter specifies the Closed User Group (CUG) index facility to use in the next call request. The CUG index facility specifies for the called switch, the closed user group selected for a virtual call. You can specify up to two digits. The default is null.

NUI

The NUI parameter specifies the set of Network User Identification (NUI) related facilities to use in the next call request. NUI provides information to the network for billing, security, network management purposes, and activation of subscribed facilities. You can specify the NUI, consisting of up to six digits, to use in the next call request. The default is null.

NUI prompt

The NUI prompt parameter specifies the NUI prompt for a PAD application. You can specify up to 15 characters. The default is null. A value in NUI prompt overrides any value entered in the NUI setting.

NUI PW prompt

The NUI PW prompt specifies the NUI password prompt for a PAD application. You can specify up to 12 characters. The default is null. This parameter is used as Call User Data in the outbound Call Request Packet.

PAD Alias #1
PAD Alias #2
PAD Alias #3

These parameters specify a string for single-command substitution. You can specify up to 40 characters. The default is null. For one command string (including a space) to be treated as equivalent to another, you must enter a slash (/) between the two strings.

PAD banner msg

The PAD banner msg parameter specifies the banner message that the user or a calling device sees when starting an X.25 PAD (Triple-X) session on the MAX. The PAD user can either be a user or a calling device running a script. You can specify up to 32 characters. The default is null.

PAD prompt

The PAD prompt specifies the PAD prompt. You can specify up to 12 characters. The default is null.

Recv PW

The Recv PW parameter specifies a case-sensitive password to use for authenticating the caller.

Reverse Charge

The Reverse Charge parameter specifies whether the X.25 facility field indicates *reverse charge request* when the X.25 user calls a host. The default is No.

RPOA

The RPOA parameter specifies the set of Recognized Private Operating Agency (RPOA) user facilities to use in the next call request. The RPOA facilities provide the data network identification code for the requested initial RPOA transit network. You can specify up to 4 digits. The default is null.

VC Timer Enable

You can enable or disable use of the Virtual Call Establishment (VCE) timer on a per-user basis. The VC Timer Enable parameter specifies the number of seconds to maintain a connection to a character-oriented device (such as the terminal server) that has not established a virtual call. If the X.25 profile disables this parameter, it has no effect in a Connection profile.

X.25 Prof

The X.25 Prof parameter specifies a 15-character text field containing the name of an X.25 profile that the MAX uses for the logical connection. If the specified X.25 profile cannot be found, the MAX does not start a session for this Connection profile. As a safeguard against such misconfiguration, an active Connection profile specifying X.25 encapsulation cannot be saved unless you name the X.25 profile and make it active.

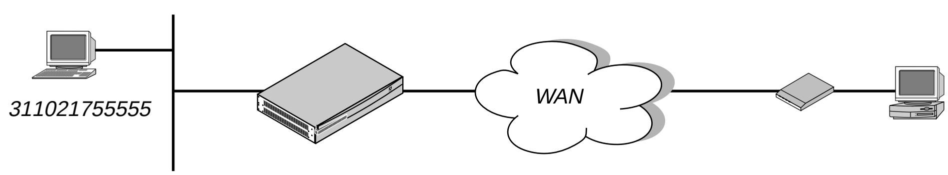
X.3 Param Prof

Table 6-3 on page 6-18 lists supported X.3 profiles. You can set the X.3 Param Prof parameter to specify a default X.3 profile for the connection. You can also use a PAD command to specify a profile. A profile specified on the command line overrides the default profile for the length of the current session.

Example of X.25 PAD

This section shows a sample configuration in which the MAX immediately directs the X.25 modem caller to a PAD interface on the host whose X.121 address appears in Figure 6-2.

Figure 6-2. Example of an X.25 PAD connection



To configure this sample X.25 PAD connection:

1 Open the Answer profile and enable X.25/PAD encapsulation:

```
Ethernet
   Answer
      Encaps...
         X25/PAD=Yes
```

2 Open a Connection profile, name it, and activate the profile:

```
Ethernet
  Connections
    any Connection profile
      Name=rchan
      Active=Yes
```

3 Enable X.25/PAD encapsulation:

```
Encaps=X25/PAD
```

4 Open the Encaps Options subprofile and specify the name of the X.25 profile that carries this connection:

```
Encaps options...
   X.25 Prof=ATT
```

5 Specify the password that authenticates the user connection:

```
   Recv PW=localpw
```

6 Specify a default X.3 parameter profile for this connection:

```
   X.3 Param Prof=CRT
```

7 Specify the X.121 address and password for automatic calling:

```
   Auto-Call X.121 Addr=031344159782111 *Dpassword
```

8 Close the Connection profile.

Setting up X.25 PAD sessions

This section describes some of the PAD commands and X.3 parameter profiles that can affect how users' terminal sessions operate.

X.3 parameters and profiles

By setting one or more X.3 parameters or by applying an X.3 profile, the user's terminal or host DTE can modify PAD operations. This section lists the X.3 parameters and profiles and then describes how to set them from the PAD. Table 6-2 lists the X.3 parameters, numbered 1–22.

Table 6-2. X.3 parameters

Parameter	Description	Possible values
1	PAD recall	0—Escape not allowed 1—Escape allowed (the default)
2	Echo	0—No echo 1—Echo (the default)
3	Data forwarding characters	0—None (full packet) 1—Alphanumeric 2—Carriage return (the default) 4—ESC, BEL, ENQ, ACK 8—DEL, CAN, DC2 16—ETX, EOT 32—HT, LT, VT, FF 64—All other characters in columns 0 and 1 of International Alphabet #5

Table 6-2. X.3 parameters (continued)

Parameter	Description	Possible values
4	Idle timer delay	0—No timer 1–255—Delay value in twentieths of a second
5	Ancillary device control	0—Not operational 1—Use X-ON (DC1 of International Alphabet #5) and X-OFF (DC3 of International Alphabet #5)
6	PAD service and command signals	0—Do not transmit service signals 1—Transmit service signals
7	PAD operation on receipt of break signal from the start-stop mode DTE	0—No action 1—Transmit Interrupt packet 2—Reset 4—Indication of break (PAD message) 8—Escape from data transfer 16—Discard output to DTE-C 21—Combine actions 1, 4, and 16
8	Discard output	0—Normal data delivery (the default) 1—Discard output to DTE-C
9	Padding after carriage return	0—No padding 1–7—Number of padding characters inserted after the carriage return
10	Line folding	0—No line folding (the default) 1–255—Number of characters per line
11	Terminal-server-access speed	10—50 bps 5—75 bps 9—100 bps 0—110 bps 1—134.5 bps 6—150 bps 8—200 bps 2—300 bps ...

Table 6-2. X.3 parameters (continued)

Parameter	Description	Possible values
11 (continued)	Terminal server access speed	The following values are dependent on the PAD type: 4—600 bps 3—1200 bps 7—1800 bps 11—75 bps from, 1200 bps to DTE-C. 12—2400 bps 13—4800 bps 14—9600 bps 15—19200 bps 16—48000 bps 17—56000 bps 18—64000 bps
12	Flow control of the PAD by the start-stop mode DTE	0—Not operational 1—Use X-ON and X-OFF (DC1 and DC3 of International Alphabet #5)
13	Linefeed insertion after carriage return	0—Option not selected 1—Linefeed insertion after a carriage return in data the PAD sends to DTE-C 2—Linefeed insertion after a carriage return in data the PAD receives from DTE-C 4—Linefeed insertion after echo of each carriage return to DTE-C
14	Linefeed padding	0—No padding 1-7—Number of padding characters inserted after the linefeed
15	Editing	0—No editing in data transfer 1—Editing in data transfer
16	Character delete	0–127 (a character from International Alphabet #5)
17	Line delete	0–127 (a character from International Alphabet #5)
18	Line display	0–127 (a character from International Alphabet #5)
19	Editing PAD service signals	0—No editing PAD service signals 1—Editing PAD service signals

Table 6-2. X.3 parameters (continued)

Parameter	Description	Possible values
20	Echo mask	0—None (full packet) 1—Alphanumeric 2—Carriage return (the default) 4—ESC, BEL, ENQ, ACK 8—DEL, CAN, DC2 16—ETX, EOT 32—HT, LT, VT, FF 64—All other characters in columns 0 and 1 of International Alphabet #5
21	Parity treatment	0—No parity checking or generation 1—Parity checking 2—Parity generation
22	Page wait	0—No page wait 1–255—The number of linefeed characters sent by the PAD before page wait condition

Table 6-3 lists the permanent (noncustom) X.3 profiles, and the settings of their parameters.

Table 6-3. X.3 profiles

X.3 profile	Contents
CRT	1:64, 2:1, 3:2, 4:0, 5:0, 6:5, 7:2, 8:0, 9:0, 10:0, 11:0, 12:1, 13:4, 14:0, 15:1, 16:8, 17:24, 18:18, 19:2, 20:0, 21:3, 22:0
INFONET	1:1, 2:0, 3:2, 4:0, 5:0, 6:0, 7:21, 8:0, 9:2, 10:0, 12:1, 13:0, 14:2, 15:1, 16:8, 17:24, 18:18, 19:0, 20:0, 21:0, 22:0
SCEN	1:64, 2:1, 3:2, 4:0, 5:1, 6:5, 7:21, 8:0, 9:0, 10:0, 12:1, 13:4, 14:0, 15:1, 16:127, 17:24, 18:18, 19:1, 20:0, 21:0, 22:0
CC_SSP	1:1, 2:1, 3:126, 4:0, 5:1, 6:1, 7:2, 8:0, 9:0, 10:0, 12:1, 13:0, 14:0, 15:0, 16:127, 17:24, 18:18, 19:1, 20:0, 21:0, 22:0
CC_TSP	1:0, 2:0, 3:0, 4:20, 5:0, 6:0, 7:2, 8:0, 9:0, 10:0, 12:0, 13:0, 14:0, 15:0, 16:127, 17:24, 18:18, 19:1, 20:0, 21:0, 22:0
HARDCOPY	1:64, 2:1, 3:2, 4:0, 5:2, 6:5, 7:21, 8:0, 9:5, 10:80, 12:1, 13:4, 14:5, 15:1, 16:8, 17:24, 18:18, 19:1, 20:0, 21:3, 22:0
HDX	1:1, 2:1, 3:2, 4:0, 5:2, 6:5, 7:2, 8:0, 9:0, 10:0, 12:1, 13:4, 14:0, 15:1, 16:8, 17:24, 18:18, 19:2, 20:0, 21:3, 22:0
SHARK	1:0, 2:0, 3:2, 4:0, 5:0, 6:0, 7:2, 8:0, 9:0, 10:0, 12:0, 13:0, 14:0, 15:0, 16:0, 17:0, 18:0, 19:0, 20:0, 21:0, 22:0

Table 6-3. X.3 profiles (continued)

X.3 profile	Contents
DEFAULT (MINIMAL)	1:64, 2:1, 3:2, 4:0, 5:2, 6:5, 7:2, 8:0, 9:25, 10:72, 12:1, 13:5, 14:25, 15:1, 16:8, 17:24, 18:18, 19:1, 20:0, 21:0, 22:0
NULL	1:0, 2:0, 3:0, 4:0, 5:0, 6:0, 7:0, 8:0, 9:0, 10:0, 12:0, 13:0, 14:0,15:0, 16:0, 17:0, 18:0, 19:0, 20:0, 21:0, 22:0

X.25 PAD commands

This section describes the X.25 PAD user commands in two categories: those that manage calls from the PAD and those that affect X.3 profile and parameter settings for the local or remote PAD. Underlined letters in a command indicate the minimum string you have to type to execute the command. To display a list of all X.25 PAD commands and syntaxes, enter the Help command.

```
help
```

Commands for working with X.3 parameters and profiles

Following are the commands you can enter at the PAD prompt (*) to change an X.3 parameter setting or profile:

- par? [*param1*[,*param2*,...]]

  The Par? command displays the current values of the specified X.3 parameters. Or, if you specify no parameters, the command displays all current X.3 settings. For example:

  ```
  par 2
  ```

- prof [*profile* | ?]

  The Prof command activates the X.3 profile (specified by the name shown in Table 6-3 on page 6-18), or if you use this command with the question mark (?) keyword, it displays the currently active profile followed by a list of available profiles. If you do not specify any arguments, the Prof command displays the currently active profile. For example:

  ```
  prof infonet
  ```

- set [*param1*:*value1* [,*param2*:*value2*,...]]

  The Set command sets one or more X.3 parameter values. For example:

  ```
  set 1:0, 2:1
  ```

- set? [*param1*:*value1* [,*param2*:*value2*,...]]

  The Set command is identical to the Set command, except that it displays all X.3 parameter values after setting those specified on the command line.

- tabs [LCL *num1*][REM *num2*][EXP *num3*]

  The Tabs command sets and reads three nonstandard X.3 parameters that control tab expansion. You cannot access these parameters by the remote host using Q-bit packet PAD commands on the remote host. You must keep the PAD's view of the current screen position accurate by setting EXP to 0 and LCL to the number of columns to which your terminal expands tabs. The settings enable the PAD to perform correct line folding, line deletion, and character deletion. The keywords function as follows:

  – LCL sets the number of columns to which tabs are expanded locally (*num1*). If the EXP keyword disables local tab expansion, LCL *num1* specifies the number of columns to which the asynchronous device expands tabs sent to it. You can specify a number from 0 to 16. Zero specifies that no expansion takes place.

  – REM sets the number of columns to which tabs are expanded remotely (*num2*), that is, on input from the terminal to the network. You can specify a number from 0 to 16. Zero specifies that no expansion takes place.

  – EXP enables (1) or disables (0) tab expansion locally. If you specify 1 after this keyword, the MAX expands tabs according to the LCL specification.

Following are similar commands for changing X.3 settings on the remote PAD:

- rpar? [*param1*[,*param2*,...]]

  The Rpar? command displays the current values of the specified X.3 parameters on the remote PAD. Or, if you specify no parameters, the command displays all current X.3 settings. For example:

  ```
  rpar 2
  ```

- rprof [*profile* | ?]

  The Rprof command activates the X.3 profile for the remote PAD. Or, if you use this command with the question mark (?) keyword, it displays the currently active profile followed by a list of available profiles. If you do not specify any arguments, the Rprof command displays the currently active profile. For example:

  ```
  rprof infonet
  ```

- rset [*param1*:*value1* [,*param2*:*value2*,...]]

  The Rset command sets one or more X.3 parameter values for the remote PAD. For example:

  ```
  set 1:0, 2:1
  ```

- rset? [*param1*:*value1* [,*param2*:*value2*,...]]

  The Reset? command is identical to the Reset command, except that it displays all X.3 parameter values after setting those specified on the command line.

X.25 PAD commands for managing calls

You can enter the following commands at the X.25 PAD prompt to generate calls, specify a matching pattern for incoming calls, and perform related functions:

- call [?] | [[*address*][*P|*D|*F *data*]]

  The Call command generates a call by sending a Call-Request packet. If you enter the Call command with only a question mark (?), the MAX displays the address the PAD would use if you entered the Call command with no address.

  The *address* argument specifies the X.121 address to which the MAX makes the call. The address can contain up to 15 characters. If you do not specify a value for *address*, the MAX makes the call request for the last address specified.

  The MAX inserts the *data* following the *P and *D keywords into the last 12 bytes of the user data field. If you specify *P, the screen does not echo the data as you enter it, even if you set X.3 parameter number 2 to Echo. This specification is useful for entering passwords. If you specify *D, the screen echoes the data as you enter it.

  If you specify *F, the MAX inserts all the <data> into the user data portion of the call packet (with a maximum length of 124 bytes), and the MAX flags the packet as a *fast select* call. For example:

  ```
  call 3331055567
  ```

- clr

  The Clr command clears a virtual circuit by sending a Clear-Request packet (from a DTE) or a Clear-Indication packet (from a DCE).

- facilities [* | *facilities*]

  The Facilities command specifies which facilities to use in subsequent Call commands. If you enter the Facilities command with no arguments, the MAX displays the current facilities.

- If you specify an asterisk (*), the command clears the current facilities and resets them to their default values. The default facilities are window size 2 and packet size 128 (420202430707).
- The *facilities* argument can consist of up to 63 hexadecimal digits. The MAX converts the specified value you specify from hexadecimal format, and it becomes the byte sequence inserted in the Facilities field of outgoing Call-Request packets.

For example,

```
facil *
```

- full

  The Full command selects full-duplex mode.

- half [*] | [[-] <ch1>, <ch2>,...]

  The Half command selects half-duplex mode and specifies the characters echoed. In half-duplex mode, the MAX does not echo most characters. In half-duplex mode with echo enabled, the PAD does most of the work of echoing and then discards the data instead of sending it to the asynchronous device. The PAD can therefore provide line folding, tab expansion, linefeed insertion, carriage return and linefeed padding, and character and line deletion. For more information about these features, see “X.3 parameters and profiles” on page 6-15.

  If you disable echo, the amount of processing the PAD must perform on every character decreases substantially, and the PAD cannot perform line folding, tab expansion, or other actions described in the previous paragraph. This mode is most efficient for file transfers. The command’s arguments function as follows:

  - If you specify an asterisk (*), the MAX does not echo any characters.
  - If you specify only a list of characters (<ch1>, <ch2>, and so on), the MAX echoes only these characters.
  - You must specify each character in decimal format.
  - If you insert a hyphen (-) before the list of characters, only the characters you specify are not echoed.
  - If you enter the Half command with no arguments, the command sets half-duplex mode without altering the characters selected for echo by any previously entered Half command.

- interrupt

  The Interrupt command generates an Interrupt packet. An Interrupt packet can transmit from 1 to 32 bytes of data to the remote DTE without being subject to flow control. The exchange of Interrupt packets does not affect the exchange of data packets or flow-control packets.

- listen [addr=<address> | data=*data*]

  The Listen command specifies the match pattern for accepting an incoming call. It uses the following syntax:

  - The MAX matches the <address> argument against the subaddress specified by the incoming call. If the subaddresses match, the MAX accepts the incoming call.
  - The MAX matches the <data> against the last 12 bytes of the user data field of incoming calls. If the data matches, the MAX accepts the incoming call.

- reset

  The Reset command resets a virtual circuit by generating a Reset-Request packet with 0 cause (DTE originated) and 0 diagnostic.
- status

  The Status command requests the status of a virtual call placed to a remote DTE.

PAD service signals

The PAD acknowledges commands and informs the user about the internal state of the PAD by transmitting PAD service signals to the terminal server. The terminal-server user can suppress the reception of PAD service signals by setting PAD parameter #6 to 0. Table 6-4 on page 6-23 lists the PAD service signals.

Table 6-4. PAD service signals

Service signal	Description
RESET DTE	The remote DTE has reset the virtual circuit.
RESET ERR	A reset has occurred because of a local procedure error.
RESET NC	A reset has occurred because of network congestion.
COM	A call has been connected.
PAD ID	Precedes a string that identifies the PAD.
ERROR	The terminal-server user used faulty syntax when entering an X.25/PAD command.
CLR	A virtual circuit has been cleared.
ENGAGED	In response to the Status command, this signal indicates that a virtual call is up.
FREE	In response to the Status command, this signal indicates that a virtual call has been cleared.
PAR with X.3 parameter reference numbers and their current values	This string is a response to the Set? command.

X.25 clear cause codes

Table 6-5 shows hexadecimal X.25 clear cause codes.

Table 6-5. Clear cause codes

Hex value	Cause code
01	Number busy
03	Invalid facility request
05	Network congestion
09	Out of order
0B	Access barred
0D	Not obtainable
11	Remote procedure error
13	Local procedure error
15	RPOA out of order
19	Reverse charging acceptance not subscribed
21	Incompatible destination
29	Fast select acceptance not subscribed
39	Ship absent
C1	Gateway-detected procedure error
C3	Gateway congestion

X.25 diagnostic field values

Table 6-6 shows X.25 diagnostics.

Table 6-6. X.25 diagnostic field values

Hex value	Dec value	Diagnostic
0	0	No additional information
1	1	Invalid P(S)
2	2	Invalid P(R)
10	16	Packet type invalid
11	17	For state r1
12	18	For state r2
13	19	For state r3
14	20	For state p1
15	21	For state p2
16	22	For state p3
17	23	For state p4
18	24	For state p5
19	25	For state p6
1A	26	For state p7
1B	27	For state d1
1C	28	For state d2
1D	29	For state d3
20	32	Packet not allowed
21	33	Unidentifiable packet
22	34	Call on one-way LC
23	35	Invalid packet type on a PVC
25	37	Reject not subscribed to
26	38	Packet too short
27	39	Packet too long

Table 6-6. X.25 diagnostic field values (continued)

Hex value	Dec value	Diagnostic
29	41	Restart packet with nonzero LC
2B	43	Unauthorized interrupt confirmation
2C	44	Unauthorized interrupt
2D	45	Unauthorized reject
30	48	Timer expired
31	49	For incoming call (or for DTE timer expired for Call request)
32	50	For clear indication (or for DTE timer expired or retransmission count surpassed for clear request)
33	51	For reset indication (or for DTE timer expired or retransmission count surpassed for reset request)
34	52	For restart indication (or for DTE timer expired or retransmission count surpassed for restart request)
40	64	Call setup, call clearing, or registration problem
41	65	Facility/registration code not allowed
42	66	Facility parameter not allowed
43	67	Invalid called address
44	68	Invalid calling address
45	69	Invalid facility/registration length
46	70	Incoming call barred
47	71	No logical channel available
48	72	Call collision
49	73	Duplicate facility requested
4A	74	Nonzero address length
4B	75	Nonzero facility length
4C	76	Facility not provided when expected

Customizing script support for X.25 PAD

The MAX X.25 PAD provides additional flexibility to work with a variety of devices that have their own expectations of banner messages, PAD prompt, PAD commands, and PAD signals. The MAX provides a way for you to configure the banner messages, PAD prompt, and PAD commands to meet these expectations.

Note: The MAX X.25 PAD supports the X.3, X.28 and X.29 protocols and can be referred to as a Triple-X PAD.

Parameters and commands

The following parameters and commands allow you to configure the MAX X.25 PAD to meet the expectations of devices to which it might connect.

- Five parameters appear in the Ethernet > Connections >Encaps Options submenu for an X.25/PAD connection.
  - Banner
  - PAD prompt
  - NUI prompt
  - NUI PW prompt
  - PAD Alias #*n* (where *n*=1–3)
- One terminal server command
  - X28
- Two X.25 PAD commands
  - storeprofile
  - call

Banner

The Banner parameter specifies the Banner message that the user or the calling device sees when starting an X.25 PAD (Triple-X) session on the MAX. The PAD user can either be a human user or a calling device running a script. You can specify up to 32 characters. The default is null.

NUI prompt

The NUI prompt parameter specifies the message that prompts the user or the calling device to enter his/its NUI when starting an X.25 PAD (Triple-X) session on the MAX. The PAD user can either be a human user or a calling device running a script. You can specify up to 20 characters. The default is null.

NUI PW prompt

The NUI PW prompt specifies the message that prompts the user or the calling device to enter his/its NUI password when starting an X.25 PAD (Triple-X) session on the MAX. The PAD user can either be a human user or a calling device running a script. You can specify up to 20 characters. The default is null.

PAD Alias #n (n=1-3)

Each of these three parameters each can declare an alias for an X.25 command. When the calling device uses a script to communicate with the X.25 PAD (Triple-X) of the MAX, the script might send X.25 commands using terminology that the MAX must interpret. If the MAX receives an X.25 command which contains an alias established by a PAD Alias #n it interprets the command as set in the parameter. See the section on Accessing the PAD through X.25 Commands for further information. You can specify up to 40 characters. The default is null. For one command string (including a space) to be treated as equivalent to another, a slash (/) must be placed between the two strings.

PAD prompt

The PAD prompt parameter specifies the prompt the user or the calling device sees when running an X.25 PAD (Triple-X) session on the MAX. The PAD user can either be a human user or a calling device running a script. You can specify up to 12 characters. The default is null.

Terminal server command

X28

X28 appears in the list of terminal-server commands. X28 accesses the PAD. It is not case sensitive and x28 also accesses the PAD.

Note: The current manuals have an error. They are missing PAD, a terminal server command. Both PAD and X28 have identical functionality; that is, both access the X.25 PAD.

To access the PAD, enter the X28 command at the terminal-server prompt:

```
% X28
```

X.25 PAD command

Storeprofile

Storeprof (storeprofile) is a new X.25 PAD command. Use it to store the current settings of the PAD parameters to a specified X.3 profile.

Note: At the moment, you can store the current settings only the X.3 profile named custom.

To store the current settings of the PAD parameters to the X.3 profile name custom, enter the Storeprof command at the PAD prompt using the following syntax:

```
storeprof custom
```

See "X.25 PAD commands" on page 6-20 for instructions on how to set the X.3 parameters.

The table listing the 10 named X.3 profile should include the X.3 profile named custom noting that the settings of the X.3 parameters is not preset, but accomplished through X.25 commands.

Call

In the Call command, the called address can be followed by a comma, and the command can accept all the characters after the comma as Call User Data, up to a maximum of 12 characters. For example, you can enter the following command at the PAD prompt:

`call 123456789,CallUserData`

Accessing the PAD using the PAD script support feature

When the calling device accesses the PAD as a result of matching an X25/PAD profile via CLID, DNIS, or password authentication, the PAD must prompt the calling device for the optional NUI and NUI password. If the input is valid, the PAD must include the NUI input as an NUI facility, and the NUI password input as Call User Data, for all subsequent outgoing calls for the calling device.

Assume that the following aliases have been established by the following parameter settings:

PAD Alias #1=call/n
PAD Alias #2=prof CUSTOM/profile 6
PAD Alias #3=storeprof CUSTOM/storeprofile 6

Assume that a calling device, such as a PC with a modem attached, dials into the MAX, successfully matching a Connection profile that uses X25/PAD encapsulation. The user at the calling device can enter a series of commands as illustrated below. (Note that the user at the calling end may be a result of an application running a PAD script.)

The **`bold face type`** gives the user or the calling devices input. The normal face type gives the prompts and messages sent to the user from the PAD at the MAX. In this example, the user starts by command his modem to dial to the MAX *atd12234567*. The MAX connects and starts the X.25 session by returning the message *CONNECTED*.

```
% atd1234567

CONNECTED
THIS IS A BANNER MESSAGE
ENTER NUI:

% 123456

123456
ENTER NUI PASSWORD:

% 654321

******

PROMPT>

PROMPT> profile 6 */User loads the CUSTOM profile. */

PROMPT> set 1:1 /* User sets the Escape char to ctrl-P */

PROMPT> n 031454159782738 /* User places X.25 call. */
```

```
PROMPT>

COM /* X.25 call connected. */

PROMPT> <ctrl-P> /* After exchanging some data with the called host,
the user escapes to command mode. */

PROMPT>

PROMPT> clr /* User clears the X.25 call. */

CLR CONF
PROMPT>

PROMPT> storeprofile 6 /* User saves the changed parameters to the CUS-
TOM profile */

PROMPT>

PROMPT>+++ /* User quitting modem call */

OK

% ath

OK
```

Setting up ISDN D-channel X.25 support

This section discusses support of X.25 over the D-channel but T3POS, X25/PAD, X25/IP, X25/PPP, X25/MP protocols are also supported over any channel that supports X.25. For example: B-channel, and serial WAN.

Configuring ISDN D-channel X.25 support

To configure the MAX to support X.25 over the signaling D channel:

1 Open Ethernet > X25 > *any X25 profile*.

2 Set TEI to the value specified by your X.25 carrier.

You can set TEI to any value from 0 to 63. The default is 23. If you set TEI to 0 (zero), the MAX requests a TEI assignment from the network.

3 Set Call Type to D Channel.

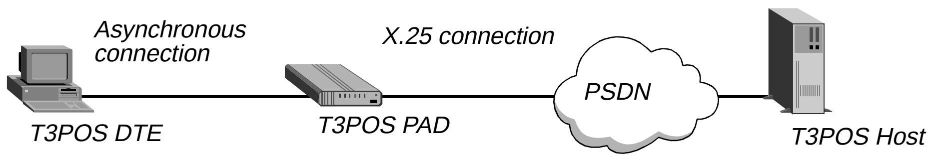
4 Exit and save the settings.

Customized X.25 T3POS support

MAX units with X.25 support X25 Transaction Processing Protocol for Point-of-Service (T3POS), which can be used to send point of sale (POS) data over the ISDN D channel.

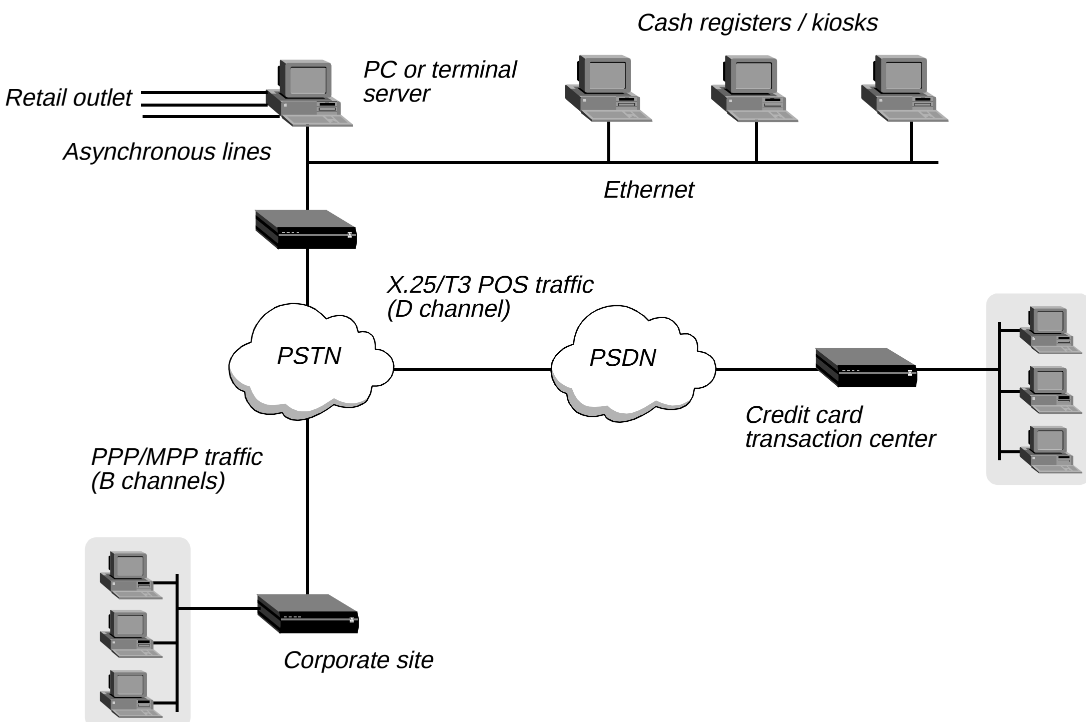
T3POS is a character-oriented, frame-formatted protocol designed for point-of-service (POS) transactions through an X.25-based packet switched network. T3POS enables you to send data over the ISDN D channel while continuing to send traffic over both B channels. The T3POS protocol involves three parties: the T3POS DTE (DTE), the T3POS PAD (PAD) and the T3POS Host (host), as shown in Figure 6-3.

Figure 6-3. T3POS set up



A typical use of T3POS is performing credit card authorization over the D channel while using the B channels to transmit inventory control data and other traffic. Figure 6-4 shows an example of a T3POS setup.

Figure 6-4. Example of a T3POS configuration



The Ascend T3POS implementation supports the following T3POS features:

- Local, Transparent, Blind, and Binary-Local mode
- T1-T6 timers
- All the control characters, described in Bellcore GR-2803
- Error recovery procedures, described in Bellcore GR-2803 and EIS 1075-V2.1
- DTE-initiated calls
- Host-initiated calls

Protocol summary

This section provides a brief summary of the T3POS protocol. For complete details about the protocol and the MAX X.25 PAD, refer to the documents listed in “References” on page 6-34.

The T3POS protocol provides reliable and efficient data interchange (transactions) between a host (usually a transaction server) and a DTE (usually a client). The T3POS DTE is usually a client device communicating through an asynchronous port, while the T3POS host is a mainframe or server communicating through an X.25 packet network. The T3POS PAD (the MAX) converts data arriving from a T3POS DTE to a format that can be transmitted over a packet network. It also ensures reliability and efficiency as described in the protocol specifications.

Note that the T3POS PAD does not alter, check, or convert the parity of characters it receives from or sends to the X.25 network or the T3POS DTE. T3POS essentially uses a data format of 8 bits no parity. The format is actually 7 bits, 1 parity, but the MAX ignores the parity bit.

Depending on the current state of a transaction or call, and the mode of operation selected, T3POS uses different data formats and frame structures. The MAX supports four modes of operation: Local, Binary-Local, Transparent, and Blind.

General frames

A general frame (or data frame) is any sequence of octets received from or sent to the DTE within the period specified by the T1 timer (this timer is known as the Char-to-Char timer). In Local and Binary-local modes and in opening frames, general frames are encapsulated in the following format:

STX [*data*] *ETX XRC*

where:

- *STX* is the ascii character \002.
- *Data* is the user data being sent in this frame.
- *ETX* the ascii character \003.
- *XRC* is the checksum. For all modes except Binary-Local, the checksum is a one character Longitudinal Redundancy Check (LRC) checksum. For Binary Local mode, the checksum is a two character Cyclic Redundancy Check (CRC) checksum.

Control frames

The MAX uses a control frame only when establishing a call and not during data transfer. You can configure the T3POS modes and most of the T3POS parameters for the T3POS PAD using the VT-100 interface in the MAX. However, use of a control frame can override the operating mode, called number, call user data, and some user facilities. A control frame is a supervisory frame with the following format:

SOH MSS CUD STX [*data*] *ETX XRC*

where:

- *SOH* is the ascii character \001.
- *MSS* is the Mode Selection Signal which can be (optionally) used to indicate the mode for the call.
- *CUD* is the Called User Data. It can contain an X.121 address, and user facilities or call user data in an X.28 format.
- Data is optional in the control frame. In Transparent and Blind modes, the T3POS PAD is essentially restricted to passing data frames between the T3POS DTE and the T3POS host.
- *ETX* is the ascii character \003.
- *XRC* is the checksum. For all modes except Binary-Local the checksum is a one character Longitudinal Redundancy Check (LRC) checksum. For Binary-Local mode, the checksum is a two character Cyclic Redundancy Check (CRC) checksum.

T3POS Timers

The T3POS protocol defines six timers:

- T1: Char-to-Char timer
- T2: SYN-to-SYN timer
- T3: ENQ Handling timer
- T4: Response timer
- T5: DLE, EOT timer
- T6: Frame Arrival timer

DTE-initiated calls

If the first T3POS frame (which can be either a general frame or a control frame) the MAX receives is from the DTE, the session is qualified as DTE-initiated. When the MAX receives a general frame from the DTE, it uses the settings in the Answer profile (or the Connection profile) to trigger a call to the host when it receives a control frame from the DTE. The MAX also triggers a call to the host. In this case, however, the MAX uses the mode and called address if any specified in the control frame for the call, overriding any setting configured in the MAX.

Host-initiated calls

The current implementation does not directly support incoming calls to the DTE. Instead, the DTE answers any host-initiated calls by connecting to the T3POS PAD and *listening* for such calls. The host must send a called address matching the pattern the DTE is listening for. The pattern need not be a complete X.121 address, but can be a subpattern (including wildcard characters). You configure the listening pattern by setting the Listen X.121 Addr parameter (which is described in the *MAX Reference Guide*).

Flow control

Flow control should not be an issue for the X25 T3POS implementation, because the T3POS protocol has an effective window size of one (that is, every frame must be acknowledged before another frame is sent) and because the MAX buffers all the frames before forwarding them to the DTE or the host. However, you should chose the T2, T3, and T4 timers carefully, because the MAX buffers the data before forwarding it. Note that the current Ascend modem code performs continuous RTS/CTS flow control, which cannot be disabled.

References

The T3POS protocols are derived from several documents that have become de facto standards:

- GR-2803—“Generic requirements for a Packet Assembler/Disassembler supporting T3POS,” Bellcore GR-2803-CORE Issue 2, Dec. 1995. This is the basic defining document.
- EIS 1075-V2.1—“External Interface Specification for Data-Terminal-Equipment Support of T3POS,” Applied Digital Design, version 2.1, March 1994. Specifies error recovery mechanisms between a T3POS DTE and a T3POS PAD on one side and a T3POS PAD and the T3POS host in the other side.

Configuring a T3POS connection

Configuring a T3POS connection requires two general procedures:

- Create a Connection profile for each authenticated user connecting to the T3POS, or configure the Answer profile for unauthenticated users.
- Create an X.25 profile that defines the X.25 connection the T3POS PAD uses.

Note: For detailed information about the T3POS parameters, see the *MAX Reference Guide*.

Note: The settings in the Connection or Answer profile can be overridden by the settings sent in control frames.

To configure a T3POS Connection profile:

1. From the Main Edit Menu select Ethernet > Connections > *any Connection profile*.
2. Set Active to Yes.
3. Set Encaps to X25/T3POS.
4. Open the Encaps Options submenu.
5. Set X.25 Prof to the name of the X.25 profile that is to be used for this T3POS connection.
   The X.25 profile must exist and be active before you can save this Connection profile.

6. Specify the Recv PW value used to authenticate the caller.
7. Set specify the parameters used for the T3POS connection.
8. Exit and save the Connection profile.

To configure a T3POS Answer profile:

1. From the Main Edit Menu select Ethernet > Answer > Encaps.
2. Set X25/PAD to Yes and X25/T3POS to Yes.
3. Exit the Encaps submenu.
4. Select T3POS Options.
5. Set X.25 Prof to the name of the X.25 profile that is to be used for this T3POS connection.

   The X.25 profile must exist and be active before you can save the Answer profile.
6. Set the parameters used for the T3POS connection.
7. Exit and save the Answer profile.

Accessing the T3POS

Users can access the T3POS in any of the following ways:

- Through a modem (for MAX units only).
- Via a TCP/IP client to the default TCP modem port 6150 (or to the TCP modem port configured on the Ascend unit).
- Via a TCP/IP client to port 23 (for Telnet access) or to 513 (for Rlogin access).

Accessing the T3POS from a dial-in connection

The following example describes how a user accesses the X.25/T3POS from a modem. The X.25 data link is already up because it is a nailed physical connection. This scenario also applies to Telnet users connecting to port 150 of the MAX.

Note: Telnet client programs should use 8 bit mode to connect to the MAX.

In this example:

1. A user dial in through a modem or through Telnet.
2. The user is authenticated against a Connection profile. If no Connection profile exists for the user, the Answer profile is used (if configured).

   Both the Connection and the Answer profile specify that the user is an X.25 user (that is, Encaps is set to X25/T3POS). An X.25 profile specifies the physical interface where the X.25 call is to be established. The X.25 profile determines the settings for the LAPB (or LAPD) and packet level, (for example, timers and window size). For LAPB, the X.25 profile also specifies the nailed group to use for the logical call.
3. The connection is then established on the basis of the settings in both the Connection profile (or Answer profile) and the X.25 profile, and the call is directed to the T3POS.
4. The user then must use the normal X.25/PAD commands.

Accessing the T3POS from the MAX terminal-server interface

The following example describes how a user accesses the X.25/T3POS from the MAX terminal-server interface or through Telnet.

1. At the terminal-server prompt, the user enters the T3POS command. For example:
   `ascend%` **`t3pos`**
2. The user is directed to the T3POS PAD, and T3POS traffic can be transmitted.

Accessing the T3POS through immediate mode

To allow access to the T3POS PAD immediately upon connecting, set Immediate Service to X25/T3POS in the Ethernet > Mod Config > TServ Options submenu. Users typically use this mode to connect to the T3POS PAD.

Ascend recommends that, when using immediate service, you set the Banner parameter to suppress the terminal-server banner, and reduce the PPP Delay parameter to its minimum value. Both parameters are in the Ethernet > Mod Config > TServ Options submenu.

Always On/Dynamic ISDN (AO/DI)

The MAX supports Always On/Dynamic ISDN (AO/DI) which is described in the Internet Engineering Task Force (IETF) draft titled *Always On/Dynamic ISDN*, dated October, 1997. AO/DI enables you to send and receive data through a nailed X.25 connection (supported over an ISDN D-channel, ISDN B-Channel, or leased-56k line), using switched ISDN B-channels only when required on the basis of increased bandwidth utilization.

Introduction

AO/DI is a networking service that enables you to send and receive data by means of an X.25 connection over and ISDN line (or leased-56k line) as well as by means of switched B-channels. Through its use of X.25 and Bandwidth Allocation Control Protocol (BACP), the MAX avoids dialup charges and usage of switched B-channels whenever it sends or receives data over the X.25 connection.

In a traditional ISDN environment, data moves across B-channels, and signalling information moves across the D-channel. Because signalling information uses a small percentage of available D-channel bandwidth, AO/DI was developed to maximize bandwidth usage while reducing the necessity that all data travel over B-channels. Ascend’s implementation of AO/DI enables you to configure a nailed X.25 connection over a BRI D-channel, BRI B-channel, or over a leased-56k line.

Among the functions that can take advantage of AO/DI are the following:

- Transfer of email
- Reception of news broadcasts and other pushed information
- Automated collection of data

For all Ascend units, AO/DI enables you to use X.25 bandwidth up to 9600 bps. If data transfers require more bandwidth, B-channels are dialed and combined using BACP. Although MAX units support an X.25 connection over the serial WAN connection rather than an ISDN line, Pipeline units support X.25 only through a B-channel or the D-channel. Contact your carrier for more details.

How it works

When you configure AO/DI for a connection, data flows over the X25 connection as long as bandwidth usage is less than the value specified in the Ethernet > Connections > *any Connection profile* > Encaps options > Target Util parameter. The MAX dials a B-channel if the Average Line Utilization (ALU) for the connection stays above the value in Target Util for the amount of seconds specified in the Ethernet > Connections > *Any* Connection profile > Encaps Options > Add Pers parameter.

When the MAX adds bandwidth on the basis of DBA, it brings up a B-channel to transport data and stops sending data over the X.25 connection. Because the 9600 bps bandwidth available over the X.25 connection is so small when compared to that available through the B-channel, it is not efficient to continue to transfer data over the X.25 connection simultaneously.

When ALU for the connection drops below the value specified in the Target Util parameter for the amount of seconds specified in the Sub Pers parameter, the MAX disconnects the switched channel and data traffic flows over the X.25 connection.

The MAX can add bandwidth to a connection using multiple B-channels to transfer data for a specific call, but discontinues using the X.25 connection for data transfer if at least one B-channel is active.

Configuring an AO/DI connection

Configuring an AO/DI connection consists of the following steps:

- Create an X.25 profile that defines the X.25 connection.
- Configure the Answer profile to enable BACP and MP support.
- Create a Connection profile for each AO/DI connection.

Note: For more complete information about each of the X.25 and BACP parameters, see the *MAX Reference Guide*.

Configuring the X.25 profile

To configure the MAX to support the X.25 connection:

1 Open Ethernet > X25 > `any` *X25 profile*.

2 Set Name to a descriptive name for the X.25 link.

3 Set Active to Yes.

4 Set TEI to the value specified by your X.25 carrier.

You can set TEI to any value from 0 to 63. The default value is 23. If you set TEI to 0, the Ascend unit requests a TEI assignment from the network.

5 Set Call Type as follows:

– Call Type = D-Channel if X.25 services are over the D-channel.

– Call Type = Nailed if X.25 services are over either a B-channel or the leased-56k line.

6. Set Nailed Grp that AO/DI-related Connection profiles reference when using the X.25 connection.

   The value specified for Nailed Grp must match the value specified in the Ethernet > Connections > *any Connection profile* > Telco options > Group parameter of any AO/DI-related profile that uses the X.25 connection.
7. Set X.25 highest SVC as directed by your carrier.
8. Set X.25 lowest SVC as directed by your carrier.
9. Set X.121 src addr to the called number that the remote side sends when establishing the X.25 connection with the MAX. Contact your carrier for the correct value.
10. Set any remaining X.25 parameters as your carrier specifies.
11. Exit and save the settings.

Configuring the Answer profile

To configure the Answer profile to allow support of AO/DI:

1. From the main Edit menu, select Ethernet > Answer profile.
2. Open the Encaps submenu.
3. Set MP to Yes.
4. Set PPP to Yes.
5. Close the Encaps submenu.
6. Open the PPP options submenu.
7. Set BACP = Yes.
8. Exit and save the Answer profile.

Configuring a Connection profile to support AO/DI

Before you configure a Connection profile to support AO/DI, you must understand each of the X.25 parameters related to the Connection profile.

Understanding the X.25 connection parameters

The following table displays background information about the X.25 connection parameters.

Parameter	Description
X.25 profile name	This 15-character text field contains the name of an X.25 profile that the MAX uses for this logical connection. If the matching X.25 profile cannot be found, the MAX does not start a session for this Connection profile. To guard against this misconfiguration, an active Connection profile specifying X.25 encapsulation can not be saved unless you define the named X.25 profile and make it active.
X.25 reverse charge	Specifies whether the X.25 facility field indicates *reverse charge request* when the X.25 user calls a host. The default is No.

Parameter	Description
RPOA	Specifies the set of RPOA (Recognized Private Operating Agency) user facilities to use in the next call request. The RPOA facilities provide the data network identification code for the requested initial RPOA transit network. You can specify up to 4 digits. The default is null.
CUG Index	Specifies the Closed User Group (CUG) index/selection facility to use in the next call request. The closed user group selection/index facility specifies to the called switch the closed user group selected for a virtual call. You can specify up to two digits. The default is null.
NUI	Specifies the set of Network User Identification (NUI) related facilities to use in next call request. NUI provides information to the network for billing, security, network management purposes, and for activating subscribed facilities. You can specify the NUI to use in the next call request. You can specify up to six digits. The default is null.
Call mode	Specifies whether the MAX can initiate, receive a call request on the connection. Incoming—Specifies that the MAX does not issue a call request when data shows up for forwarding. If there is no virtual circuit established, the MAX drops the IP packet. If a host receives an incoming call from a host whose called address matches the value specified in Answer X.121 addr or if Answer X.121 addr is blank, the MAX accepts the called number. Outgoing—Specifies that the MAX issues a call request to the number specified in the Remote X.121 addr parameter when you enable the Connection profile. If the MAX does not establish a virtual circuit and the MAX receives an incoming call request, the MAX rejects the call. Both—Specifies that the MAX accepts incoming call requests and makes outgoing call requests on the basis of packets that need to be forwarded across the WAN. For incoming calls, the MAX accepts the called address if: The remote host's called address matches the value specified in Answer X.121 addr or if Answer X.121 addr is blank. The remote host's calling address matches the value specified in Remote X.121 addr or if Remote X.121 addr is blank.
Answer X.121 Addr	Typically matches the value specified in the X.121 src addr parameter of the X.25 profile on the MAX, although the value might be different because the MAX unit's X.25 connection can have more than one X.121 address. You should not leave Answer X.121 address blank if Call Mode specifies either Both or Incoming. You can substitute the beginning portion of the address with the wildcard `*` which indicates that the MAX should accept any value, requiring a match only on the trailing digits that you specify after the wildcard character.

Parameter	Description
Remote X.121 Addr	Specifies the value specified in the X.121 source address of the remote X.25 host to which the profile connects. You should not leave Remote X.121 addr blank if you set Call Mode to Both or Outgoing. If you configure a value for Remote X.121 address, the MAX attempts to match the incoming call to Remote X.121 address as well as Answer X.121 address. You can substitute the beginning portion of the address with the wildcard * which indicates that the MAX should accept any value, requiring a match only on the trailing digits that you specify after the wildcard character. For outgoing calls, the MAX dials only the trailing digits specified, ignoring the beginning wildcard character.

Configuring a Connection profile

To configure a Connection profile to support AO/DI:

1. From the main Edit menu select Ethernet > Connections > *any Connection profile*.
2. Set Active to Yes.
3. Set Encaps to MP.
4. Set Dial # to the phone number that the MAX dials when additional bandwidth from a B-channel is needed.
5. Open the Telco options submenu
6. Set Call Type to AO/DI.
7. Set Group to the group number that you specified in the Ethernet > X25 > X25 profile > Nailed Grp parameter.
8. From the Connection profile menu, open the Encaps options submenu.
9. Set BACP to Yes.
10. Set *both* Base Ch Cnt and Max Ch Cnt parameters to the *maximum* number of channels allowed for the connection.
11. Set InterfaceType to X.25.
12. From the Connection profile main menu, open the Interface options submenu.
13. Set X.25 Prof to the name of the X.25 profile that the MAX uses for the connection.
14. Specify additional parameters for the X.25 connection as directed by the carrier.

If you set Call Mode to Incoming or Both, proceed as follows:

1. From the Connection profile menu, open the Interface options submenu.
2. Set Answer X.121 addr to the value specified in the X.121 src addr parameter of the X.25 profile on the MAX.

   Note: You can substitute the beginning portion of the address with the wildcard * which indicates that the MAX should accept any value, requiring a match only on the trailing digits that you specify after the wildcard character.

If you set Call Mode to Outgoing or Both, proceed as follows:

1. From the Connection profile menu, open the Interface options submenu.
2. Set Remote X.121 addr to the value specified in the X.121 source address of the remote X.25 host to which the profile connects. You should not leave Remote X.121 addr blank if you set Call Mode to Both or Outgoing. Also, for incoming calls, the MAX attempts to match the called number of the incoming call to Remote X.121 address (if specified) and the calling number of the incoming call to Answer X.121 address (if specified).

   Note: You can substitute the beginning portion of the address with the wildcard `*` which indicates that the MAX should accept any value, requiring a match only on the trailing digits that you specify after the wildcard character. For outgoing calls, the MAX dials only the trailing digits specified, ignoring the beginning wildcard character.

Exit and save the Connection profile. If you set Call Mode to Outgoing, the MAX sends a call request to the number specified in the Remote X.121 addr parameter when you enable the Connection profile. If you set Call Mode to either Both, the X.25 connection stays idle until the MAX receives a packet to be forwarded across the X.25 link.

When the session and profile are active, the Connection profile displays an asterisk to the left of the profile name on the Ethernet > Connections submenu which indicates that a call is up or is available for a call.

Note: When you modify *any* AO/DI-related X.25 profile or Connection profile, you must disable all AO/DI-related profiles and re-enable them.

Displaying AO/DI operation

To make sure AO/DI is installed and configured properly, you can display one status window to indicate whether or not the MAX supports AO/DI, another to observe active AO/DI calls, and a third to indicate how many packets the MAX processes for a particular AO/DI session.

Displaying whether or not the MAX supports AO/DI

The System > Sys Options window provides a read-only list that identifies the MAX and names each of the features (including AO/DI) which it has been equipped. Press the tab key to highlight any status window, then use the left and right arrow keys to display the Sys Options window.

When the MAX displays the Sys Options window, press the down arrow key until the AO/DI feature appears. For example, the following screen indicates that the MAX supports AO/DI:

```
|-------------------|
|00-100 Sys Options |
|ISDN Sig Installed |
|AO/DI Installed    |
|Net Mgmt Installed |
|-------------------|
```

If you ordered AO/DI but the MAX displays `AO/DI Not Inst`, contact your authorized Ascend reseller.

Displaying active AO/DI calls

The Ethernet > Dyn Stat window displays the name, quality, bandwidth, and bandwidth utilization of each online connection. For example, when the MAX establishes an AO/DI connection for DMILLER, the following window appears:

```
|-------------------|
|DMILLER            |
|Qual Good 05:07:00 |
|9k      1 channels |
|CLU  12%  ALU  30% |
|-------------------|
```

When the MAX adds a B-channel on the basis of bandwidth utilization, the following window appears:

```
|-------------------|
|DMILLER            |
|Qual Good 05:07:00 |
|56k     2 channels |
|CLU  50%  ALU  34% |
|-------------------|
```

Although the connection contains two active channels, data passes only over the B-channel as described in "How it works" on page 6-37.

When the MAX adds a second B-channel on the basis of bandwidth utilization, the following window appears:

```
|-------------------|
|DMILLER            |
|Qual Good 05:07:00 |
|112k    3 channels |
|CLU  88%  ALU  64% |
|-------------------|
```

The 112k indicates that data flows through the two B-channels only.

Displaying packet processing for a specific session

The Ethernet > WAN Stat window displays the name, number of received packets, number of transmitted packets, and number of CRC errors of each online connection. For example, when the MAX establishes an AO/DI connection for DMILLER, the following window appears:

```
|-------------------|
|DMILLER            |
|Rx Pkt:       7085 |
|Tx Pkt:        603 |
|   CRC:          0 |
|-------------------|
```

Defining Static Filters

7

Introduction to Ascend filters

A packet filter contains rules describing packets and actions to take upon those packets that match the description. After you apply a packet filter to an interface, the MAX monitors the data stream on that interface. Depending on how you define a filter, it can apply to inbound packets or outbound packets, or both. In addition, filter rules are flexible enough to specify taking an action (such as forward or drop) on those packets that match the rules, or all packets *except* those that match the rules.

Note: The MAX ships with three predefined filters. Many sites use these filters as is or add rules pertinent to their networks. For more information, see "Configuring predefined filters" on page 7-21.

Packet filters and firewalls

The MAX supports the following types of *static* packet filters:

- Generic filters
- IP filters
- IPX filters

The MAX also supports *dynamic* firewalls.

Generic filters

Generic filters examine the byte- or bit-level contents of every packet, comparing specified bytes or bits with a value defined in the filter. On the basis of this comparison, they specify a forwarding action. To use generic filters effectively, you need to know the contents of certain bytes in the packets you wish to filter. Protocol specifications are usually the best source of such information.

IP filters

IP filters examine higher-level fields specific to IP packets. They focus on known fields in IP packets (for example, the source or destination address, or the protocol number). They operate on logical information that is relatively easy to obtain. IP filters can block Address Resolution Protocol (ARP) packets as well as IP packets.

IPX filters

IPX filters examine higher-level fields specific to IPX packets. They focus on known fields in IPX packets (for example, the source or destination address, or node, or socket numbers). Like IP filters, IPX filters operate on logical information that is relatively easy to obtain.

Dynamic firewalls

The MAX also supports SecureConnect, which provides *dynamic* firewalls. A firewall differs from a filter in that it alters its behavior as traffic passes through it, whereas a filter remains unchanged through its lifetime. Unlike a static packet filter which has a limited number of rules, a SecureConnect firewall's only limitation is router memory.

If your MAX unit has SecureConnect support installed, see the *SecureConnect Manager's User's Guide* for complete instructions about how to create and apply firewalls. You can refer to a SecureConnect firewall set up in SAM in a RADIUS user profile, so that the firewall is applied for the connection defined in the user profile. For more information, see the *MAX RADIUS Configuration Guide.*

Ways to apply packet filters to an interface

After you define a packet filter, you apply it to an interface to monitor packets crossing that interface. You can apply the filter as one of the following:

- A data filter, to define the packets that can or cannot cross the interface.
- A call filter, to define the packets that can or cannot bring up a connection or reset the idle timer for an established connection (WAN interfaces only).

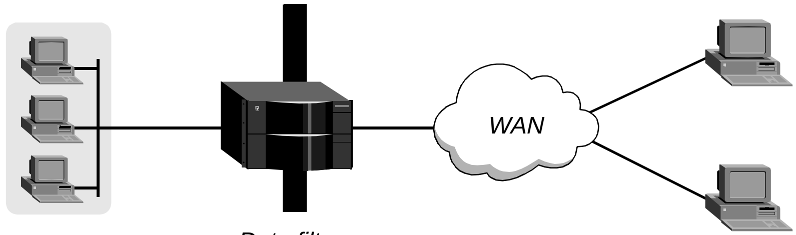
Packets can pass through both a data filter and call filter on a WAN interface. If you specify both, the MAX applies the data filter first.

Data filters for dropping or forwarding certain packets

Data filters are commonly used for security, but they can apply 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 forwarding action (forward or drop) affects the actual data stream by preventing certain packets from reaching the Ethernet from the WAN, or vice versa. Data filters do not affect the idle timer, and a data filter applied to a Connection profile does not affect the answering process. In Figure 7-1, the vertical bar represents a barrier blocking specified packets.

Figure 7-1. Data filter



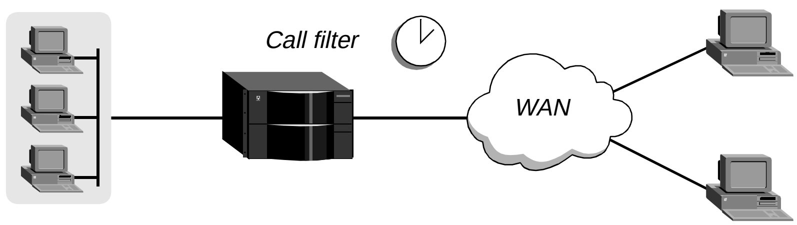
Call filters for managing connections

A call filter defines the packets that can or cannot bring up a connection or reset the idle timer for an established link. As shown in Figure 7-2, a call filter does not block the transmission of packets.

Call filters prevent unnecessary connections and help the MAX distinguish active traffic from *noise*. By default, any traffic to a remote site triggers a call, and any traffic across an active connection resets the connection's idle timer.

When you apply a call filter, its forwarding action does not affect the packets the MAX sends across an active connection. The forwarding action of a call filter determines whether or not a packet can either initiate a connection or reset a session's timer. When a session's idle timer expires, the session terminates. The default for the idle timer is 120 seconds, so if a connection is inactive for two minutes, the MAX terminates the connection.

Figure 7-2. Call filter



How packet filters work

This section provides an overview of packet filters and the processes they follow. For more details about a filter matching a value in a packet, see "Defining packet filters" on page 7-5.

A Filter profile can contain up to 12 input-filter rules and up to 12 output-filter rules. Each rule has its own forwarding action: forward or drop. At the first successful comparison between a filter and the packet being examined, the filtering process stops and the forwarding action in that rule is applied to the packet.

If no comparison succeeds, the packet does not match the filter. However, this does not mean that the MAX forwards the packet. When no filter is in use, the MAX forwards all packets, but applying a filter to an interface reverses this default. For security purposes, the MAX does not automatically forward nonmatching packets. It requires a rule that explicitly allows such packets to pass. (For an example of an input filter that forwards all packets that did not match a previous rule, see "Defining a filter to prevent IP-address spoofing" on page 7-14.)

Note: For a call filter to prevent an interface from remaining active unnecessarily, you must define rules for both input and output packets. Otherwise, if you define only input rules, output packets keep a connection active, or vice versa.

Generic filters

In a generic filter, all parameter settings in a rule work together to specify a location in a packet and a number to be compared to that location. The Compare parameter specifies whether a comparison succeeds when the contents of the packet equal the specified number or when they or do not equal that number.

IP filters

In an IP filter, a set of distinct comparisons are made in a defined order. When a comparison fails, the MAX applies the next comparison to the packet. When a comparison succeeds, the filtering process stops and the MAX applies the forwarding action in that rule to the packet. The IP filter tests proceed in the following order:

1. Apply the Src Mask value to the Src Adrs value and compare the result to the source address of the packet. If they are not equal, the comparison fails.
2. Apply the Dst Mask value to the Dst Adrs value and compare the result to the destination address in the packet. If they are not equal, the comparison fails.
3. If the Protocol parameter is 0 (zero, which matches any protocol), the comparison succeeds. If it is nonzero and not equal to the protocol field in the packet, the comparison fails.
4. If the Src Port Cmp parameter is not set to None, compare the value of the Src Port # parameter to the source port of the packet. If they do not match as specified in the Src-Port-Cmp parameter, the comparison fails.
5. If the Dst Port Cmp parameter is not set to none, compare the value of the Dst Port# parameter to the destination port of the packet. If they do not match as specified in the Dst-Port-Cmp parameter, the comparison fails.
6. If TCP Estab is set to Yes and the protocol number is 6, the comparison succeeds.

IPX filters

In an IPX filter, each rule includes a set of comparisons that are made in a defined order. When a comparison fails, the packet is allowed to go on to the next comparison. When a comparison succeeds, the filtering process stops and the forwarding action in the rule is applied to the packet. The IPX filter tests proceed in the following order:

1. Compare the Src Adrs number to the source network number of the packet. If they are not equal, the comparison fails.
2. Compare the Dst Adrs number to the destination network number in the packet. If they are not equal, the comparison fails.
3. Compare the Src Adrs number to the source number of the packet. If they are not equal, the comparison fails.

4. Compare the Dst Adrs number to the destination number in the packet. If they are not equal, the comparison fails.
5. If the Src Port Cmp parameter is not set to None, compare the Src Port number to the source socket number of the packet. If they do not match as specified in the Src Port Cmp parameter, the comparison fails.
6. If the Dst Port Cmp parameter is not set to None, compare the Dst Port number to the destination socket number of the packet. If they do not match as specified in the Dst Port Cmp parameter, the comparison fails.

Defining packet filters

Filter profiles provide parameters for defining affected packets. The parameters are the same for input or output filters. Following are the filter parameters (shown with sample settings):

```
Ethernet
  Filters
   any filter profile
      Name=filter-name
      Input filters...
         In filter 01–12
            Valid=Yes
            Type=Generic
            Generic...
               Forward=No
               Offset=14
               Length=8
               Mask=ffffffffffffffff
               Value=aaaa0300000080f3
               Compare=Equals
               More=No
            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
            Ipx...
               Forward=No
               Src Network Adrs=cfff0000
               Dst Network Adrs=cf088888
               Src Node Adrs=111222333
               Dst Node Adrs=aaabbbccc
               Src Socket Cmp=equal
               Src Socket #=0451
               Dst Socket Cmp=equal
             Dst Socket #=0015

      Output filters...
         Out filter 01–12
```

```
Valid=Yes
Type=Generic
Generic...
   Forward=No
   Offset=14
   Length=8
   Mask=ffffffffffffffff
   Value=aaaa0300000080f3
   Compare=Equals
   More=No
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
Ipx...
   Forward=No
   Src Network Adrs=cfff0000
   Dst Network Adrs=cf088888
   Src Node Adrs=111222333
   Dst Node Adrs=aaabbbccc
   Src Socket Cmp=equal
   Src Socket #=0451
   Dst Socket Cmp=equal
 Dst Socket #=0015
```

This section provides some background information about configuring packet filters. For detailed information about each parameter, see the *MAX Reference Guide*. Note that the parameters for defining the actual packet conditions are identical for Input and Output filters.

Name of the Filter profile

Each filter must be assigned a name so it can be referenced from other profiles. The names of defined filters appear in the main Filters menu.

Input and output filters

Each filter can contain up to 12 input filters and output filters, each defined individually and applied in order (1–12) to the packet stream. The MAX applies input filters to inbound packets and output filters to outbound packets. The individual input and output filters are in the In Filter and Out FIlter subprofiles, respectively. In each individual filter, the Valid parameter enables or disables that filter. When you disable a filter, none of its parameters apply. (You cannot configure a filter until you enable it.)

Type of filter

Set Type to Generic or IP. Only the parameters in the corresponding subprofile (Generic or Ip) are applicable.

Generic filter parameters

Generic filters can affect any packet, regardless of its protocol type or header fields. Following are the parameters for generic filters (shown with sample settings):

```
Generic...
   Forward=No
   Offset=14
   Length=8
   Mask=ffffffffffffff
   Value=aaaa0300000080f3
   Compare=Equals
   More=No
```

This section provides some background information about how these parameters work together.

Forward

The Forward parameter specifies whether the MAX discards or forwards packets that match the filter specification. When no filters are in use, the MAX forwards all packets by default. When a filter is in use, the default, Forward=No, discards matching packets.

Offset

Offset specifies a byte-offset from the start of a frame to the start of the data to be tested. For example, with the following filter specification:

```
Generic...
   Forward=No
   Offset=2
   Length=8
   Mask=0F FF FF FF 00 00 00 F0
   Value=07 FE 45 70 00 00 00 90
   Compare=Equals
   More=No
```

and the following packet contents:

```
2A 31 97 FE 45 70 12 22 33 99 B4 80 75
```

the first two byes in the packet (2A and 31) are ignored because of the two-byte offset.

Note: If the MAX links the current filter to the previous one (if More=Yes in the previous filter), the offset starts at the endpoint of the previous segment.

Length

The Length parameter specifies the number of bytes to test in a frame, starting with the byte specified by the Offset parameter. For example, with the following specification:

```
Generic...
   Forward=No
   Offset=2
   Length=8
   Mask=0F FF FF FF 00 00 00 F0
   Value=07 FE 45 70 00 00 00 90
   Compare=Equals
   More=No
```

and the following packet contents:

```
2A 31 97 FE 45 70 12 22 33 99 B4 80 75
```

the filter tests the value of bytes three (97) through ten (99).

The Mask parameter is a 8-bit mask to apply to the value specified by the Value parameter before the MAX compares it to the packet contents at the specified offset. You can set the parameter to specify exactly the bits you want to compare.

The MAX translates both the mask and the value specified by the Value parameter into binary format and then applies a logical AND to the results. Each binary 0 (zero) in the mask hides the bit in the corresponding position in the value. A mask of all ones (FF FF FF FF FF FF FF FF) masks no bits, so the full value must match the packet contents. For example, with this filter specification:

```
Generic...
   Forward=No
   Offset=2
   Length=8
   Mask=0F FF FF FF 00 00 00 F0
   Value=07 FE 45 70 00 00 00 90
   Compare=Equals
   More=No
```

and the following packet contents:

```
2A 31 97 FE 45 70 12 22 33 99 B4 80 75
```

The MAX applies the mask and compares the data as follows:

Value setting		07	FE	45	70	00	00	00	90			
Mask		0F	FF	FF	FF	00	00	00	F0			
Result of mask		07	FE	45	70				9			
Packet contents	2A 31	97	FE	45	70	12	22	33	99	B4	80	75
	Two-byte offset			Eight-byte comparison								

Every bit specified by the Value parameter and not masked by the Mask setting matches the corresponding bit in the packet. Therefore, the MAX drops the packet, because the Forward parameter is set to No. The comparison works as follows:

- The MAX ignores 2A and 31 because of the two-byte offset.
- The 9 in the third byte is also ignored, because the mask has a 0 (zero) in its place. The 7 in the third byte matches the Value parameter's 7 for that byte.
- In the fourth byte, F and E match the fourth byte specified by the Value parameter.

- In the fifth byte, 4 and 5 match the fifth byte specified by the Value parameter.
- In the sixth byte, 7 and 0 match the sixth byte specified by the Value parameter.
- In the seventh (12), eighth (22) and ninth (33) bytes in the seventh, eighth and ninth bytes are ignored because the mask has zeroes in those places.
- In the tenth byte, 9 matches the Value parameter's 9 for that byte. The second 9 in the packet's tenth byte is ignored because the mask has a 0 (zero) in its place.

Value

The Value parameter specifies a hexadecimal number to be compared to the packet data identified by the Offset, Length, and Mask calculations.

Compare

The Compare parameter specifies the type of comparison to make between the specified value and the packet's contents. The choices are: less than, equal, greater than, or not equal.

More

The More parameter specifies whether the MAX applies the conditions specified in the next In Filter *nn* or Out Filter *nn* subprofile before determining whether the packet matches the filter. If More is set to Yes, the MAX links the current set of filter conditions to the one immediately following it, so the filter can examine multiple noncontiguous bytes within a packet before the forwarding decision is made. In effect, this parameter *marries* the current filter to the next one, so that the MAX applies the next filter before the MAX makes the forwarding decision. The match occurs only if *both* noncontiguous bytes contain the specified values. Note that the next set of conditions must be enabled, or the MAX ignores it.

IP filter parameters

IP filter parameters affect only IP and related packets. Following are the IP filter parameters (shown with sample settings):

```
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
```

This section provides some background information about how these parameters work.

Forward

The Forward parameter specifies whether the MAX discards or forwards packets that match the filter specification. When no filters are in use, the MAX forwards all packets by default. When a filter is in use, the default setting discards matching packets.

Src Mask

The Src Mask parameter specifies a mask to apply to the Src Adrs value before comparing it to the source address in a packet. You can use it to mask out the host portion of an address, for example, or the host and subnet portion.

The MAX translates both the mask and the address into binary format and then uses a logical AND to apply the mask to the address. The mask hides the bits whose positions match those of the binary zeroes in the mask. A mask of all zeros (the default) masks all bits, so all source addresses match. A mask of all ones (255.255.255.255) masks no bits, so the full source address from a single host is compared to the Src Adrs value.

Src Adrs

The Src Adrs parameter specifies a source IP address. After you modify this value by applying the specified Src Mask, the MAX compares it to a packet's source address.

Dst Mask

The Dst Mask parameter specifies a mask to apply to the Dst Adrs value before comparing it to the destination address in a packet. You can use it to mask out the host portion of an address, for example, or the host and subnet portion. The MAX translates both the mask and the address into binary format and then uses a logical AND to apply the mask to the address. The mask hides the portion of the address that appears behind each binary 0 in the mask. A mask of all zeros (the default) masks all bits, so all destination addresses are matched. A mask of all ones (255.255.255.255) masks no bits, so the full destination address to a single host is compared to the Dst Adrs value.

Dst Adrs

The Dst Adrs parameter specifies a destination IP address. After modifying this value by applying the specified Dst Mask value, the MAX compares it to a packet's destination address.

Protocol

If you specify a protocol number, the MAX compares it to the protocol field in each packet. The default protocol number of zero matches all protocols. A list of common protocols appears below. For a complete list of protocol numbers, see "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

Src Port #

The Src Port # parameter specifies a value to compare with the source port number in a packet. The default setting (zero) indicates that the MAX disregards the source port in this filter. Port 25 is reserved for SMTP. This socket is dedicated to receiving mail messages. Port 20 is reserved for FTP data messages, port 21 for FTP control sessions, and port 23 for Telnet.

The Src Port Cmp parameter specifies the type of comparison to be made.

Dst Port #

The Dst Port # parameter specifies a value to compare with the destination port number in a packet. The default setting (zero) indicates that the MAX disregards the destination port in this filter. Port 25 is reserved for SMTP; that socket is dedicated to receiving mail messages. Port 20 is reserved for FTP data messages, port 21 for FTP control sessions, and port 23 for telnet.

The Dst Port Cmp parameter specifies the type of comparison to be made.

TCP Estab

If the Protocol parameter (which specifies the protocol number) has been set to 6 (TCP), you can set TCP Estab to restrict the filter to packets in an established TCP session. Otherwise, the parameter is not applicable.

Example filter specifications

This section shows some examples of generic and IP filter specifications.

Defining a filter to drop AppleTalk broadcasts

This example shows a generic filter whose purpose is to prevent local AppleTalk AEP and NBP traffic from going across the WAN. The filter is supposed to drop packets, so it will be applied as a data filter. The filter first defines packets that should be forwarded across the WAN: AppleTalk Address Resolution Protocol (AARP) packets, AppleTalk packets that are not addressed to the AppleTalk multicast address (for example, regular traffic related to an actual AppleTalk File Server connection), and all non-AppleTalk traffic. The filter then specifies that AppleTalk Echo Protocol (AEP) and Name Binding Protocol (NBP) packets should be dropped. To define this filter:

1. Open a Filter profile and assign it a name. For example:

```
Ethernet
   Filters
    any filter profile
      Name=AppleTalk Broadcasts
```

2. Open Output Filters > Out Filter 01.
3. Set Valid to Yes and Type to Generic.

```
Output filters...
   Out filter 01
      Valid=Yes
      Type=Generic
```

4. Open the Generic subprofile and set the following values:

```
Generic...
   Forward=Yes
   Offset=14
   Length=8
   Mask=FFFFFFFFFFFFFFFF
   Value=FFFF0300000080F3
   Compare=Equals
   More=No
```

These settings define the bytes in AARP packets that contain the protocol type number (0x80F3). The Value setting specifies the same value (0x80F3), so AARP packets match these rules.

5. Close this filter. Then open Out Filter 02, and set Valid to Yes and Type to Generic.

```
Output filters...
   Out filter 02
      Valid=Yes
      Type=Generic
```

6. Open the Generic subprofile and set the following values:

```
Generic...
Forward=Yes
   Offset=32
   Length=6
   Mask=FFFFFFFFFFFF0000
   Value=090007FFFFFF0000
   Compare=NotEquals
   More=No
```

These settings specify the multicast address used by AppleTalk broadcasts. The MAX forwards any AppleTalk packet that does not match the specified values.

7. Close this filter. Then open Out Filter 03, and set Valid to Yes and Type to Generic.

```
Output filters...
   Out filter 03
      Valid=Yes
      Type=Generic
```

8 Open the Generic subprofile and set the following values:

```
Generic...
   Forward=Yes
   Offset=14
   Length=8
   Mask=FFFFFFFFFFFFFFFF
   Value=AAAA03080007809b
   Compare=NotEquals
   More=No
```

These settings include the bytes in AppleTalk packets that specify the protocol type number (0x809B).These rules define non-AppleTalk traffic (packets that do not contain that value in the specified location). The MAX forwards non-AppleTalk outbound packets.

9 Close this filter. Then open Out Filter 04, and set Valid to Yes and Type to Generic.

```
Output filters...
   Out filter 04
      Valid=Yes
      Type=Generic
```

10 Open the Generic subprofile and set the following values:

```
Generic...
   Forward=No
   Offset=32
   Length=3
   Mask=FFFFFFFFFFFFFFFF
   Value=0404040000000000
   Compare=Equals
   More=No
```

These settings specify AEP packets as described in, for example, *Inside AppleTalk* published by Addison Wesley, Inc.

11 Close this filter. Then open Out Filter 05, and set Valid to Yes and Type to Generic.

```
Output filters...
   Out filter 05
      Valid=Yes
      Type=Generic
```

12 Open the Generic subprofile and set the following values:

```
Generic...
   Forward=No
   Offset=32
   Length=4
   Mask=FF00FFF000000000
   Value=0200022000000000
   Compare=Equals
   More=Yes
```

Notice that More=Yes, linking Out Filter 05 with the Out Filter 06. Together, these two Out filters specify NBP lookup packets with a wildcard entity name.

13 Close this filter. Then open Out Filter 06, and set Valid to Yes and Type to Generic.

```
Output filters...
   Out filter 06
      Valid=Yes
      Type=Generic
```

14 Open the Generic subprofile and set the following values:

```
Generic...
   Forward=No
   Offset=42
   Length=2
   Mask=FFFF000000000000
   Value=013D000000000000
   Compare=Equals
   More=No
```

15 Close this filter.

16 Close the Filter profile.

Defining a filter to prevent IP-address spoofing

IP-address spoofing typically occurs when a remote device illegally acquires a local address and uses it to try to break through a firewall. This example shows a filter that prevents IP-address spoofing. The sample filter first defines input filters that drop packets whose source address is on the local IP network or is the loopback address (127.0.0.0). The third input filter accepts all remaining source addresses (by specifying a source address of (0.0.0.0) and forwards them to the local network.

Note: If you apply this filter to the Ethernet interface, the MAX drops IP packets it receives from the local LAN, and therefore you cannot Telnet to the unit.

The filter then defines an output filter that defines the following rule: 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 nonlocal source address. In this example, the filter uses a local IP network address of 192.100.50.128, with a subnet mask of 255.255.255.192. The following procedure defines the IP filter:

1 Open a Filter profile and assign it a name. For example:

```
Ethernet
   any filter profile
      Filters
        Name=IP Spoofing
```

2 Open Input Filters > In Filter 01.

3 Set Valid to Yes and Type to IP:

```
Input filters...
   In filter 01
      Valid=Yes
      Type=IP
```

4 Open the IP subprofile and set the following values:

```
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 mask for the local subnet. 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.

5 Close this filter. Then open In Filter 02, and set Valid to Yes and Type to IP:

```
Input filters...
   In filter 02
      Valid=Yes
      Type=IP
```

6 Open the IP subprofile and set the following values:

```
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 settings 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.

7 Close this filter. Then open In filter 03, and set Valid to Yes and Type to IP:

```
Input filters...
   In filter 03
      Valid=Yes
      Type=IP
```

8 Open the IP subprofile and set the following values:

```
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 settings specify every source address (0.0.0.0). The MAX forwards, onto the Ethernet, every incoming packet that has not been dropped by the preceding filter.

9 Close this In Filter and the Input Filters subprofile. Then, open the Output Filters subprofile and select the first Out Filter in the list (01).

10 Set Valid to Yes and Type to IP:

```
Output filters...
   Out filter 01
      Valid=Yes
      Type=IP
```

11 Open the IP subprofile and set the following values:

```
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 mask for the local subnet. The Src Adrs parameter specifies the local IP address. If an outgoing packet has a local source address, the MAX forwards it.

12 Close the Filter profile.

Defining a filter for more complex IP security issues

This example illustrates some of the issues you need to consider when writing your own IP filters. The sample filter presented here does not address the fine points of network security. You can use this example as a starting point and augment it to address your security requirements. For details, see the MAX *Security Supplement.*

In this example, the local network supports a Web server and the administrator needs to carry out the following 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 filter will be applied in Connection profiles as a data filter.

The following procedure defines the filter:

1 Open a Filter profile and assign it a name. For example:

```
Ethernet
   any filter profile
     Filters
        Name=Web Safe
```

2 Open Input Filters > In Filter 01.

3 Set Valid to Yes and Type to IP:

```
Input filters...
   In filter 01
      Valid=Yes
      Type=IP
```

4 Open the IP subprofile and set the following values:

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

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

5 Close this filter. Then open In Filter 02, and set Valid to Yes and Type to IP.

```
Input filters...
   In filter 02
      Valid=Yes
      Type=IP
```

6 Open the IP subprofile and set the following values:

```
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=6
   Src Port Cmp=None
   Src Port #=N/A
   Dst Port Cmp=Gtr
   Dst Port #=1023
   TCP Estab=No
```

These settings specify TCP packets (Protocol=6) *from* any address and *to* any address. The filter forwards them if the destination port number is higher than that of the source port. For example, Telnet requests go out on port 23, and responses come back on some random port above 1023. So, this filter defines packets coming back in response to a user's request to Telnet to a remote host.

7 Close this filter. Then open In Filter 03, and set Valid to Yes and Type to IP.

```
Input filters...
   In filter 03
      Valid=Yes
      Type=IP
```

8 Open the IP subprofile and set the following values:

```
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=17
   Src Port Cmp=None
   Src Port #=N/A
   Dst Port Cmp=Gtr
   Dst Port #=1023
   TCP Estab=No
```

These settings specify UDP packets (Protocol=17) *from* any address and *to* any address. The filter forwards them if the destination port number is higher than that of 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 above port 1023.

9 Close this filter. Then open In Filter 04, and set Valid to Yes and Type to IP.

```
Input filters...
   In filter 04
      Valid=Yes
      Type=IP
```

10 Open the IP subprofile and set the following values:

```
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=1
   Src Port Cmp=None
   Src Port #=N/A
   Dst Port Cmp=None
   Dst Port #=N/A
   TCP Estab=No
```

These rules specify unrestricted Pings and Traceroutes. Unlike TCP and UDP, ICMP does not use ports, so a port comparison is unnecessary.

11 Close the Filter profile.

Applying packet filters

A filter does not examine any packets unless it is applied to a MAX interface. Once applied, the filter examines packets that cross the interface. You can apply the filter as a data filter, to forward or drop certain packets, or as a call filter, to affect the packets that can initiate calls or reset the idle timer. For background information about these two applications, see "Introduction to Ascend filters" on page 7-1. Following are the relevant parameters (shown with sample settings):

```
Ethernet
   Answer
      Session options...
         Data Filter=0
```

```
        Call Filter=0
        Filter Persistence=No
Ethernet
   Connections
      any Connection profile
         Session options...
            Data Filter=5
            Call Filter=0
            Filter Persistence=No
Ethernet
   Mod Config
      Ether options...
         Filter=1
```

How filters are applied

This section provides some background information about the parameters for applying filters to a local or WAN interface. For detailed information about each parameter, see the *MAX Reference Guide*.

Applying filters in the Answer profile

The MAX does not apply filters referenced in the Answer profile. Apply filters in the Answer profile only if configured profiles are not required for callers, or if the caller is authenticated with a Name/Password profile if a caller has a Connection profile. If the Answer profile applies filters, they have the same effect as those ordinarily specified in a Connection profile.

Specifying a data filter

A data filter affects the actual data stream on the WAN interface, forwarding or dropping packets according to its rules (as described in "Data filters for dropping or forwarding certain packets" on page 7-2.) When you apply a filter to a WAN interface, the filter takes effect when the MAX brings up a connection on that interface.

Specifying a call filter

A call filter does not forward or drop packets. When the filter rules specify *forward*, the call filter lets matching packets initiate the connection or, if the connection is active, reset the idle timer (as described in "Call filters for managing connections" on page 7-3.)

If you apply both a data filter and call filter, the data filter acts first. Only those packets that pass the data filter reach the call filter.

Filter persistence

Before the MAX supported Secure Connect Firewall, it constructed a filter on a WAN interface when the connection was established and destroyed the filter when the connection was brought down, even if the connection just timed out momentarily. This works fine for static packet filters, but does not accommodate firewall. Filter persistence is needed to allow firewalls to persist across connection state changes, but it is not needed for filters. If you do set Filter

Persistence for a static packet filter, the filter persists across connection state changes. For details, see the *MAX Security Supplement*.

Applying a data filter on Ethernet

Call filters do not apply to the local network interface, so you need only one Filter parameter in the Ethernet profile. This is a data filter that affects the packets that are allowed to reach the Ethernet or to leave the Ethernet for another interface.

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

Note: Use caution when applying a filter to the Ethernet interface. You could inadvertently render the MAX inaccessible from the local LAN.

Examples of configurations that apply filters

This section provides a few examples of applying data filters and applying call filters.

Applying a data filter in a Connection profile

To apply a data filter in a Connection profile:

1 Open the Session Options subprofile of the Connection profile.

2 Specify the filter's number in the Data Filter parameter. For example:

```
Ethernet
   Connections
     any Connection profile
        Session options...
           Data Filter=5
           Call Filter=0
           Filter Persistence=No
```

Specify the unique portion of the number preceding the filter's name in the Filters menu.

3 Close the Connection profile.

Applying a call filter for resetting the idle timer

When you apply a call filter in a Connection profile, it determines which packets can reset the idle timer for a connection. In this example, the idle timer is reset to 20 seconds, so if no packets pass the filter's tests for 20 seconds, the MAX terminates the connection.

To apply a call filter for resetting the idle timer in a Connection profile:

1 Open Connections > *any Connection profile* > Session Options.

2 Specify the filter's number in the Call Filter parameter.

The filter's number is the unique portion of the number preceding the filter's name in the Filters menu.

3 Set the Idle parameter to 20 seconds.

```
Ethernet
   Connections
     any Connection profile
      Session options...
```

```
Data Filter=0
Call Filter=2
Filter Persistence=No
Idle=20
```

Or, if the profile specifies a terminal-server call, set the TS Idle Mode and TS Idle parameters instead. For example:

```
Ethernet
   Connections
     any Connection profile
        Session options...
           Data Filter=0
           Call Filter=2
           Filter Persistence=No
           Idle=0
           TS Idle Mode=Input/Output
           TS Idle=20
```

4 Close the Connection profile.

Applying a data filter to the Ethernet interface

To apply a data filter to the local network interface:

1 Open the Ethernet > Mod Config > Ether Options profile.

2 Set the Filter parameter to the filter's number. For example:

```
Ethernet
   Mod Config
      Ether options...
         Filter=1
```

(Call filters are not applicable to the local network interface.)

3 Close the Ethernet profile.

Configuring predefined filters

The MAX ships with three predefined filter profiles, one for each commonly used protocol suite. Some sites modify the predefined filters to make them more full-featured for the types of packets commonly seen at that site. As shipped, the filters provide a base that you can build on to fine-tune how the MAX handles routine traffic on your network. They are intended for use as call filters, to help keep connectivity costs down. Following are the predefined filters:

- IP Call (for managing connectivity on IP connections)
- NetWare Call (for managing connectivity on IPX connections)
- AppleTalk Call (for managing connectivity on bridged AppleTalk connections)

IP Call filter

The predefined IP Call filter prevents inbound packets from resetting the idle timer. It does not prevent any type of outbound packets from resetting the timer or placing a call. The settings for the IP Call filter parameters are:

```
Ethernet
   Filters
```

```
IP Call...
   Name=IP Call
   Input filters...
      In filter 01
         Valid=Yes
         Type=GENERIC
         Generic...
            Forward=No
            Offset=0
            Length=0
            Mask=000000000000000000
            Value=000000000000000000
            Compare=None
            More=No
   Output filters...
      Out filter 01
         Valid=Yes
         Type=GENERIC
         Generic...
            Forward=Yes
            Offset=0
            Length=0
            Mask=000000000000000000
            Value=000000000000000000
            Compare=None
            More=No
```

The IP Call filter contains one input filter that defines all inbound packets, and one output filter that defines all outbound packets (all outbound packets destined for the remote network).

NetWare Call filter

The design of predefined NetWare Call filter prevents Service Advertising Protocol (SAP) packets originating on the local IPX network from resetting the idle timer or initiating a call. NetWare servers broadcast SAP packets every 60 seconds to make sure that all routers and bridges know about available services. To prevent these packets from keeping a connection up unnecessarily, apply the predefined NetWare Call filter in the Session Options subprofile of Connection profiles in which you configure IPX routing.

The predefined NetWare Call filter contains six output filters that identify outbound SAP packets and prevent them from resetting the idle timer or initiating a call. The settings for the NetWare Call filter parameters are:

```
Ethernet
   Filters
      NetWare Call...
         Name=NetWare Call
         Output filters...
            Out filter 01
               Valid=Yes
               Type=GENERIC
               Generic...
                  Forward=No
                  Offset=14
                  Length=3
                  Mask=ffffff000000000000
```

```
      Value=e0e0030000000000
      Compare=Eqls
      More=Yes
Out filter 02
   Valid=Yes
   Type=GENERIC
   Generic...
      Forward=No
      Offset=27
      Length=8
      Mask=ffffffffffffffff
      Value=ffffffffffff0452
      More=Yes
Out filter 03
   Valid=Yes
   Type=GENERIC
   Generic...
      Forward=No
      Offset=47
      Length=2
      Mask=ffff000000000000
      Value=0002000000000000
      More=No
Out filter 04
   Valid=Yes
   Type=Generic
   Generic...
      Forward=No
      Offset=12
      Length=4
      Mask=fc00ffff00000000
      Value=0000ffff00000000
      More=Yes
Out filter 05
   Valid=Yes
   Type=Generic
   Generic...
      Forward=No
      Offset=24
      Length=8
      Mask=ffffffffffffffff
      Value=ffffffffffff0452
      More=Yes
Out filter 06
   Valid=Yes
   Type=Generic
   Generic...
      Forward=No
      Offset=44
      Length=2
      Mask=ffff000000000000
      Value=0002000000000000
      More=No
```

AppleTalk Call filter

The AppleTalk Call filter instructs the MAX to place a call and reset the idle timer on the basis of AppleTalk activity on the LAN, but to prevent inbound packets or AppleTalk Echo (AEP) packets from resetting the timer or initiating a call. The filter includes one input and five output filters.

The input filter prevents inbound packets from resetting the timer or initiating a call. The output filters identify the AppleTalk Phase II and Phase I AEP protocols. The last filter enables all other outbound packets to reset the timer or initiate a call. The settings for the AppleTalk Call filter parameters are:

```
Ethernet
   Filters
      AppleTalk Call...
         Name=AppleTalk Call
         Input filters...
            In filter 01
               Valid=Yes
               Type=Generic
               Generic...
                  Forward=No
                  Offset=0
                  Length=0
                  Mask=000000000000000000
                  Value=0000000000000000
                  More=No
         Output filters...
            Out filter 01
               Valid=Yes
               Type=Generic
               Generic...
                  Forward=No
                  Offset=14
                  Length=8
                  Mask=ffffff000000ffff
                  Value=aaaa03000000809b
                  More=Yes
            Out filter 02
               Valid=Yes
               Type=Generic
               Generic...
                  Forward=No
                  Offset=32
                  Length=3
                  Mask=ffffff0000000000
                  Value=0404040000000000
                  More=No
            Out filter 03
               Valid=Yes
               Type=Generic
               Generic...
                  Forward=No
                  Offset=12
                  Length=2
                  Mask=ffff000000000000
                  Value=809b000000000000
```

```
      More=Yes
Out filter 04
   Valid=Yes
   Type=Generic
   Generic...
      Forward=No
      Offset=24
      Length=3
      Mask=ffffff0000000000
      Value=0404040000000000
      More=No
Out filter 05
   Valid=Yes
   Type=Generic
   Generic...
      Forward=Yes
      Offset=0
      Length=0
      Mask=0000000000000000
      Value=0000000000000000
      More=No
```

Configuring Packet Bridging

8

Introduction to Ascend bridging

This section provides an overview of packet bridging and explains how the MAX brings up a bridging connection.

Bridging is useful primarily to provide connectivity for protocols other than IP, IPX, and AppleTalk, although it can also be used for joining segments of an IP, IPX, or AppleTalk network. Because a bridging connection forwards packets at the hardware-address level (link layer), it does not distinguish between protocol types, and it requires no protocol-specific network configuration.

The most common uses of bridging in the MAX are to:

- Provide nonrouted protocol connectivity with another site.
- Link two sites so that their nodes appear to be on the same LAN.
- Support protocols, such as BOOTP, that depend on broadcasts to function.

Disadvantages of bridging

Bridges examine *all* packets on the LAN (in what is termed *promiscuous mode*), so they incur greater processor and memory overhead than routers. On heavily loaded networks, this increased overhead can result in slower performance.

Routers also have other advantages over bridging. Because they examine packets at the network layer (instead of the link layer), you can filter on logical addresses, providing enhanced security and control. In addition, routers support multiple transmission paths to a given destination, enhancing the reliability and performance of packet delivery.

Note: If you have a MAX running Multiband Simulation, disable bridging.

How the MAX initiates a bridged WAN connection

When you configure the MAX for bridging, it accepts all packets on the Ethernet and forwards only those that have one of the following:

- A physical address that is not on the local Ethernet segment (the segment to which the MAX connects).
- A broadcast address.

The important thing to remember about bridging connections is that they operate on physical and broadcast addresses, not on logical (network) addresses.

Physical addresses and the bridge table

A physical address is a unique, hardware-level address associated with a specific network controller. A device's physical address is also called its Media Access Control (MAC) address. On Ethernet, the physical address is a six-byte hexadecimal number assigned by the Ethernet hardware manufacturer. For example:

```
0000D801CFF2
```

If the MAX receives a packet whose destination MAC address is not on the local network, it first checks its internal bridge table. (For a description of the table, see "Transparent bridging" on page 8-4.) If it finds the packet's destination MAC address in its bridge table, the MAX dials the connection and bridges the packet.

If the address is *not* specified in its bridge table, the MAX checks for active sessions that have bridging enabled. If there are one or more active bridging links, the MAX forwards the packet across *all* active sessions that have bridging enabled.

Broadcast addresses

Multiple nodes in a network recognize a broadcast address. For example, the Ethernet broadcast address at the physical level is:

```
FFFFFFFFFFFF
```

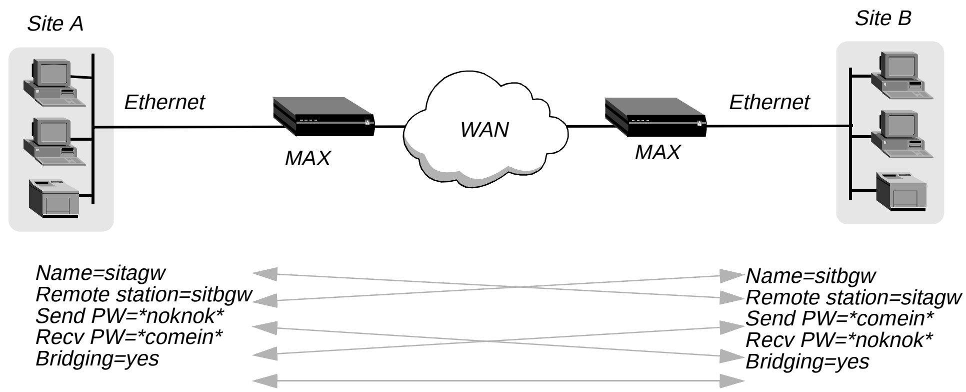
All devices on the same network receive all packets with that destination address. The MAX discards broadcast packets when you configure the MAX as a router only. When you configure the MAX as a bridge, it forwards packets with the broadcast destination address across all active sessions that have bridging enabled.

ARP broadcast packets that contain an IP address specified in the bridge table are a special case. For details, see "Configuring proxy mode on the MAX" on page 8-12.

Establishing a bridged connection

The MAX uses station names and passwords to sync up a bridging connection, as shown in Figure 8-1.

Figure 8-1. Negotiating a bridge connection (PPP encapsulation)



Note: The information exchange illustrated in Figure 8-1 differs slightly for Combinet bridging, where the bridges' MAC addresses are exchanged instead of station names, and passwords can be configured as optional. Otherwise, the way in which the MAX establishes a Combinet bridge connection across the WAN is very similar to the PPP bridged connection in Figure 8-1. For more information about Combinet, see Chapter 3, "Configuring WAN Links."

The system name assigned to the MAX in the Name parameter of System > Sys Config must *exactly* match the device name specified in the Connection profile on the remote bridge, including case changes. Similarly, the name assigned to the remote bridge must exactly match the name specified in the Station parameter of that Connection profile, including case changes.

Note: The most common cause of trouble when initially setting up a PPP bridging connection is specifying the wrong name for the MAX or the remote device. Errors often include not specifying case changes or not entering a dash, space, or underscore.

Enabling bridging

The MAX has a systemwide bridging parameter that you must enable for any bridging connection to work. The Bridging parameter directs the MAX unit's Ethernet controller to run in promiscuous mode. In promiscuous mode, the Ethernet driver accepts all packets, regardless of address or packet type, and passes them up the protocol stack for a higher-layer decision on whether to route, bridge, or reject the packets. (Even if no packets are actually bridged, running in promiscuous mode incurs greater processor and memory overhead than the standard mode of operation for the Ethernet controller.)

You enable packet bridging by opening Ethernet > Mod Config and setting the Bridging parameter to Yes:

```
Ethernet
   Mod Config
      Bridging=Yes
```

Managing the bridge table

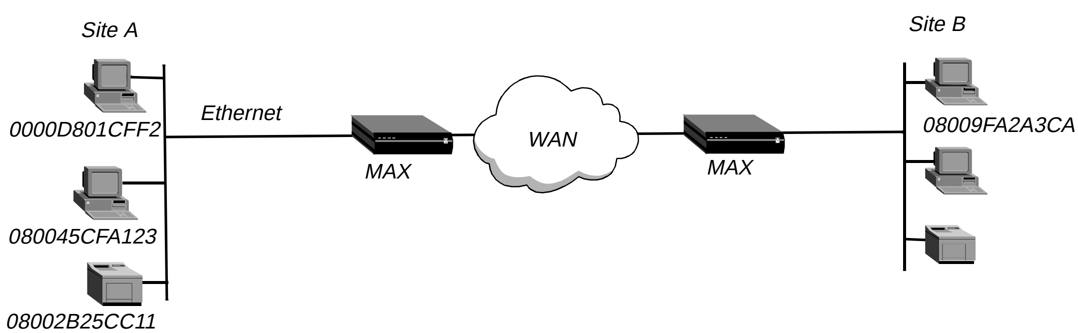
To forward bridged packets to the correct destination network, the MAX uses a bridge table that associates end nodes with particular connections. It builds this table dynamically (transparent bridging). It also incorporates the entries found in its Bridge Adrs profiles. Bridge Adrs profiles are analogous to static routes in a routing environment. You can define up to 99 destination nodes and their connection information in Bridge Adrs profiles.

Transparent bridging

As a transparent bridge (also termed a *learning bridge,* the MAX keeps track of the location of a particular address, and of the Connection profile that specifies the interface to which the packet should be forwarded. When forwarding a packet, the MAX logs the packet's source address and creates a bridge table that associates node addresses with a particular interface.

For example, Figure 8-2 shows the physical addresses of some nodes on the local Ethernet and at a remote site. The MAX at Site A has a bridge configuration.

Figure 8-2. How the MAX creates a bridging table



The MAX at Site A gradually learns addresses on both networks by looking at each packet's source address, and it develops a bridge table that includes the following entries:

```
0000D801CFF2       SITEA
080045CFA123       SITEA
08002B25CC11       SITEA
08009FA2A3CA       SITEB
```

Entries in the MAX unit's bridge table must be relearned within a fixed aging limit, or they are removed from the table.

Configuring bridged connections

Bridged connections require both Answer and Connection (or Name) profiles settings. They also require a method of recognizing when to dial the connection, which can be the dial-on-broadcast feature or a Bridge Adrs profile (Ethernet > Bridge Adrs). If a connection has an associated Bridge Adrs profile, it does not need dial-on-broadcast. You can define up to 100 Bridge Adrs profiles.

Following are the bridging parameters (shown with sample values):

```
Ethernet
   Answer
      PPP options...
         Bridge=Yes
         Recv Auth=Either

Ethernet
   Connections
      Station=farend
      Bridge=Yes
      Dial Brdcast=No
      IPX options...
         NetWare t/o=N/A
         Handle IPX=Client

Ethernet
   Names / Passwords
      Name=Brian
      Active=yes
      Recv PW=brianpw

Ethernet
   Bridge Adrs
      Enet Adrs=CFD012367
      Net Adrs=10.1.1.12
      Connection #=7
```

Understanding the bridging parameters

This section provides some background information about the bridging parameters. For discussion of IPX options, see “IPX bridged configurations” on page 8-9. For detailed information about other parameters, see the *MAX Reference Guide*.

Bridging in the Answer profile

Both the Bridge parameter and a form of password authentication must be enabled in order for the MAX to accept inbound bridged connections.

Note: Bridge = N/A in the Answer profile if the packet bridging has not already been enabled in the Ethernet profile. (For more information, see “Enabling bridging” on page 8-3.)

Station name and password

Name and password authentication is required, as described in “Establishing a bridged connection” on page 8-3.

Bridging and dial broadcast in a Connection profile

In a Connection profile, a Yes setting for the Bridge parameter specifies that the connection bridges packets at the link level, provided that a method of bringing up the connection exists. Either the Connection profile must be specified in a static bridge table entry or Dial Brdcast must be turned on. (For more information, see “Establishing a bridged connection” on page 8-3.)

Names and passwords

The MAX uses station names and passwords to sync up a bridged connection. These can be provided in a Connection profile, a Name profile, or an external authentication profile.

Bridge Adrs parameters

If a Connection profile does not use dial broadcast, it must have a bridge table entry in order for the MAX to be able to bring up the connection on demand. The Bridge Adrs profile defines a bridge table entry by specifying an Ethernet address, a network address, and a connection number.

Ethernet address

Each bridge table entry specifies an Ethernet (node) address that is not on the local segment. For details about Ethernet addresses, see “Physical addresses and the bridge table” on page 8-2.

Network address

If you are bridging between two segments *of the same IP network*, you can use the Net Adrs parameter in a Bridge Adrs profile to enable the MAX to respond to ARP requests while bringing up the bridged connection. (For more information, see “Configuring proxy mode on the MAX” on page 8-12.)

Connection number

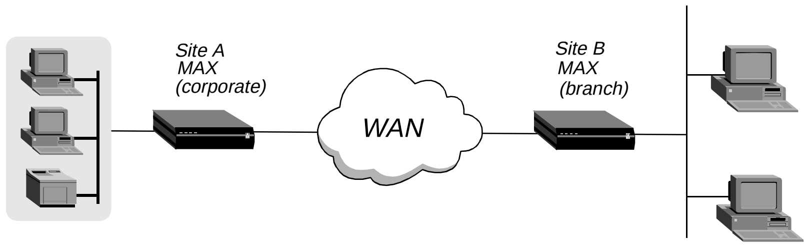
You associate Bridge Adrs profiles with one Connection profile, which the MAX uses to bring up the connection to the specified node address. You specify a Connection profile by the unique portion of its number in the Connections menu.

Example of a bridged connection

An AppleTalk connection at the link level requires a bridge at either end of the connection. This is unlike a dial-in connection using AppleTalk Remote Access (ARA) encapsulation, in which the MAX acts as an ARA server negotiating a session with ARA client software on the dial-in Macintosh.

Figure 8-3 shows an example of a bridged connection between a branch office at Site B, which supports Macintosh systems and printers, and a corporate network at Site A. Both site A and Site B support CHAP and require passwords for entry.

Figure 8-3. An example of a connection bridging AppleTalk



The most common cause of trouble when initially setting up a bridged connection is specifying the wrong name for the MAX or the remote device. Errors often include not specifying case changes, or not entering a dash, space, or underscore. Make sure you type the name exactly as it appears in the remote device.

Note: In this example, Dial Brdcast is turned off in the Connection profiles and a Bridge Adrs profile is specified. This is not required. If you prefer, however, you can turn on Dial Brdcast and omit the Bridge Adrs profile.

To configure the Site A MAX for a bridged connection:

1 If necessary, assign the MAX a station name in System > Sys Config. This example uses the name SITEAGW for the MAX.

2 Turn on bridging and specify an authentication protocol in Ethernet > Answer > PPP Options:

```
Ethernet
   Answer
      PPP options...
         Bridge=Yes
         Recv Auth=Either
```

3 Open Connection profile #5 and set the following parameters:

```
Ethernet
   Connections
      profile #5...
         Station=SITEBGW
         Active=Yes
         Encaps=PPP
         Bridge=Yes
        Dial Brdcast=No
```

Note: Dial Brdcast is not needed because of the Bridge Adrs profile configured next.

4 Configure password authentication:

```
         Encaps options...
            Send Auth=CHAP
            Recv PW=localpw
            Send PW=remotepw
```

5 Close Connection profile #5.

6 Open Ethernet > Bridge Adrs.

7 Specify a node's Ethernet address and IP address (if known) on the remote network:

```
Ethernet
   Bridge Adrs
      Enet Adrs=0080AD12CF9B
      Net Adrs=0.0.0.0
      Connection #=5
```

8 Specify the number of the Connection profile to bring up a link to the remote network.

```
Ethernet
   Bridge Adrs
      Connection#=5 ...
```

9 Close the Bridge Adrs profile.

To configure the Site B MAX unit for the bridged connection:

1 If necessary, assign the remote MAX unit a station name in its System profile. This example uses the name SITEBGW for the remote unit.

2 Turn on bridging and specify an authentication protocol in the Site B MAX unit's Answer profile. For example:

```
Ethernet
   Answer
      PPP options...
         Bridge=Yes
         Recv Auth=Either
```

3 Open Connection profile #2 on the Site B MAX and set the following parameters:

```
Ethernet
   Connections
      profile #2...
         Station=SITEAGW
         Active=Yes
         Encaps=PPP
         Bridge=Yes
         Dial Brdcast=No
```

Note: Dial Brdcast is not needed because of the Bridge Adrs profile, configured next.

4 Configure password authentication. For example:

```
         Encaps options...
            Send Auth=CHAP
            Recv PW=remotepw
            Send PW=localpw
```

5 Close Connection profile #2.

6 Open a Bridge Adrs profile.

7 Specify a node's Ethernet address and the IP address (if known) on the remote network and the number of the Connection profile to bring up a link to the remote network.

```
Ethernet
   Bridge Adrs
      Enet Adrs=0CFF1238FFFF
      Net Adrs=0.0.0.0
      Connection #=2
```

8 Specify Ethernet Bridge Adrs Connection#=2.

9 Close the Bridge Adrs profile.

IPX bridged configurations

For NetWare WANs in which NetWare servers reside only on one side of the connection, you can configure an IPX bridged connection. IPX bridging has special requirements for facilitating NetWare client-server logins across the WAN and for preventing IPX RIP and SAP broadcasts from keeping a bridged connection up indefinitely. These options vary, depending on whether the local network supports NetWare servers, NetWare clients, or both.

Understanding the IPX bridging parameters

This section focuses only on IPX issues. It does not describe the general bridging parameters explained earlier, although those parameters do apply to an IPX bridging connection.

Following are the related parameters (shown with sample settings):

```
Ethernet
   Mod Config
      Ether options...
         IPX Frame=802.2
Ethernet
   Connections
      Route IPX=No
      IPX options...
         Handle IPX=Client
         NetWare t/o=N/A
```

IPX Frame

Set the Handle IPX parameter to N/A if an IPX frame type is not specified in the Ethernet profile. For more information about IPX frame types and how they affect routing and bridging connections, see Chapter 9, “Configuring IPX Routing,”

Route IPX

If you set Route IPX to Yes in the Connection profile, the System sets the Handle IPX parameter to N/A but acts as if the parameter is set to Server.

Handle IPX

Handle IPX can be set to Server (IPX server bridging) or Client (IPX client bridging).

Use IPX server bridging when the local Ethernet supports NetWare servers (or a combination of clients and servers) and the remote network supports NetWare clients only.

Use IPX client bridging when the local Ethernet supports NetWare clients but no servers. In an IPX client bridging configuration, you want the local clients to be able to bring up the WAN connection by querying (broadcasting) for a NetWare server on a remote network. You also want to filter IPX RIP and SAP updates, so the connections should not remain up permanently.

Note: If NetWare servers are supported on both sides of the WAN connection, Ascend strongly recommends that you use an IPX routing configuration instead of bridging IPX. If you bridge IPX in this type of environment, client-server logins are lost when the MAX brings down an inactive WAN connection.

Netware T/O (watchdog spoofing)

NetWare servers send out NCP watchdog packets to monitor client connections. Only clients that respond to watchdog packets remain logged into the server.

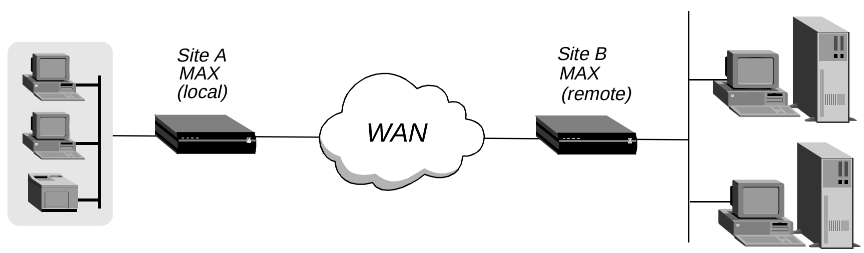
In an IPX server bridging configuration, you want the MAX to respond to NCP watchdog requests on behalf of remote clients, but to bring down inactive connections whenever possible. In this situation, you should set the Netware T/O timer. The timer begins counting down as soon as the link goes down. When the timer expires, the MAX stops responding to watchdog packets and the client-server connections can be released by the server. If the WAN session reconnects before the end of the selected time, the timer resets.

Note: The MAX performs watchdog spoofing only for packets encapsulated in the IPX frame type specified in the Ethernet profile. For example, if IPX Frame=802.3, only logins to servers using that packet frame type are spoofed.

Example of an IPX client bridge (local clients)

In this example, the local Ethernet supports NetWare clients, and the remote network supports both NetWare servers and clients, so the MAX requires IPX client bridging. When Handle IPX=Client, the MAX applies a data filter that discards RIP and SAP periodic broadcasts at its WAN interface, but forwards RIP and SAP queries. Therefore, local clients can locate a NetWare server across the WAN, but routine broadcasts do not keep the connection up unnecessarily.

Figure 8-4. An example of an IPX client bridged connection



To configure the Site A MAX in this example:

1 If necessary, assign the MAX a station name in the System profile. This example uses the name SITEAGW for the MAX.

2 Set the IPX frame type in the Ethernet profile. For example:

```
Ethernet
   Mod Config
      Ether options...
         IPX Frame=802.3
```

3 Enable bridging and specify an authentication protocol in the Answer profile. For example:

```
Ethernet
   Answer
      PPP options...
         Bridge=Yes
         Recv Auth=Either
```

4 Open a Connection profile and set the following parameters:

```
Ethernet
   Connections
      Station=SITEBGW
      Active=Yes
      Encaps=PPP
      Route IPX=No
      Bridge=Yes
      Dial Brdcast=Yes
```

Note: Enable Dial Brdcast to allow service queries to bring up the connection.

5 Configure password authentication. For example:

```
Encaps options...
   Send Auth=CHAP
   Recv PW=localpw
   Send PW=remotepw
```

6 Specify IPX client bridging:

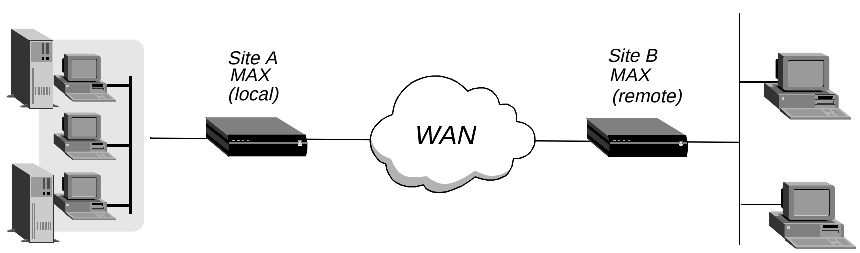
```
IPX options...
   Handle IPX=Client
```

7 Close the Connection profile.

Example of an IPX server bridge (local servers)

In this example, the local network supports a combination of NetWare clients and servers, and the remote network supports clients only, so the MAX requires IPX server bridging. When Handle IPX=Server, the MAX applies a data filter that discards RIP and SAP broadcasts at its WAN interface, but forwards RIP and SAP queries. It also uses the value specified in the NetWare T/O parameter as the time limit for responding to NCP watchdog requests on behalf of clients on the other side of the bridge.

Figure 8-5. An example of an IPX server bridged connection



To configure the Site A MAX in this example:

1 If necessary, assign the MAX a station name in the System profile. This example uses the name SITEAGW for the MAX.

2 Set the IPX frame type in the Ethernet profile. For example:

```
Ethernet
   Mod Config
      Ether options...
         IPX Frame=802.3
```

3 Enable bridging and specify an authentication protocol in the Answer profile. For example:

```
Ethernet
   Answer
      PPP options...
         Bridge=Yes
         Recv Auth=Either
```

4 Open a Connection profile and set the following parameters:

```
Ethernet
   Connections
      Station=SITEBGW
      Active=Yes
      Encaps=PPP
      Route IPX=No
      Bridge=Yes
      Dial Brdcast=Yes
```

5 Configure password authentication. For example:

```
      Encaps options...
         Send Auth=CHAP
         Recv PW=localpw
         Send PW=remotepw
```

6 Specify IPX server bridging and configure the timer for watchdog spoofing.

```
      IPX options...
         Handle IPX=Server
         Netware T/O=30
```

7 Close the Connection profile.

Configuring proxy mode on the MAX

If you are bridging between two segments of the same IP network, you can use the Net Address parameter in a Bridge Adrs profile to enable the MAX to respond to ARP requests while bringing up the bridged connection.

If an ARP packet contains an IP address that matches the Net Adrs parameter of a Bridge Adrs profile, the MAX responds to the ARP request with the Ethernet (physical) address specified in the Bridge Adrs profile, and brings up the specified connection. In effect, the MAX acts as a proxy for the node that actually has that address.

Configuring IPX Routing

9

Introduction to IPX routing

This section describes how the MAX supports IPX routing between sites that run Novell NetWare version 3.11 or newer. The MAX operates as an IPX router, with one interface to each of its two local Ethernet connections and the third across the WAN. Each IPX Connection profile defines an IPX WAN interface.

The most common use for IPX routing in the MAX is to integrate multiple NetWare LANs to form an interconnected wide-area network

The MAX supports IPX routing over PPP and Frame Relay connections. Support for both the IPXWAN and PPP IPXCP protocols makes the MAX fully interoperable with non-Ascend products that conform to these protocols and the associated RFCs.

Note: IPX transmission can use multiple frame types. The MAX, however, routes only one IPX frame type (which you configure), and it routes and spoofs IPX packets only if they are encapsulated in that type of frame. If you enable bridging and IPX routing in the same Connection profile, the MAX bridges any other IPX packet frame types. (For more information, see Chapter 8, “Configuring Packet Bridging.”)

Unlike an IP routing configuration, in which the MAX uniquely identifies the calling device by its IP address, a MAX IPX routing configuration does not include a built-in way to uniquely identify callers. For that reason, use PAP and CHAP which requires password authentication, unless you configure IP routing in the same Connection profile.

Note: If you have a MAX running Multiband Simulation, disable IPX routing.

IPX Service Advertising Protocol (SAP) tables

The MAX follows standard IPX SAP behavior for routers. However, when it connects to another Ascend unit configured for IPX routing, the two units exchange their entire SAP tables. Each unit immediately adds all remote services to its SAP table.

NetWare servers broadcast SAP packets every 60 seconds to make sure that routers (such as the MAX) know about their services. Each router builds a SAP table with an entry for each service advertised by each known server. When a router stops receiving SAP broadcasts from a server, it ages its SAP-table entry for that server and eventually removes it from the table.

Routers use SAP tables to respond to client queries. When a NetWare client sends a SAP request to locate a service, the MAX consults its SAP table and replies with its own hardware address and the internal address of the requested server. The process is analogous to proxy ARP in an IP environment. The client then transmits packets whose destination address is the internal address of the server. When the MAX receives the packets, it consults its RIP table. If it finds an entry for their destination address, it brings up the connection or forwards the packets across the active connection.

IPX Routing Information Protocol (RIP) tables

The MAX follows standard IPX RIP behavior for routers when connecting to non-Ascend units. However, when two Ascend units configured for IPX routing connect, they immediately exchange their entire RIP tables. In addition, the MAX maintains the imported RIP entries as static until you reset or power cycle the Ascend unit.

Note: In this chapter, RIP always refers to IPX RIP. IPX RIP is similar to the routing information protocol in the TCP/IP protocol suite, but it is a different protocol.

The destination of an IPX route is the internal network of a server. For example, the network administrator assigns NetWare file servers an internal IPX network number, and the servers typically use the default node address of 000000000001. This is the destination network address for file read/write requests. (If you are not familiar with internal network numbers, see your NetWare documentation for details.)

IPX routers broadcast RIP updates both periodically and each time you establish a WAN connection. The MAX receives RIP broadcasts from a remote device, increments n the hop count of each advertised route, updates its own RIP table, and broadcasts updated RIP packets on connected networks in a split-horizon fashion.

The MAX recognizes network number –2 (0xFFFFFFFE) as the IPX RIP default route. When the MAX receives a packet for an unknown destination, it forwards the packet to the IPX router advertising the default route. For example, if the MAX receives an IPX packet destined for network 77777777, and it does not have a RIP-table entry for that destination, it forwards the packet toward network number FFFFFFFE, if available, instead of simply dropping the packet. If more than one IPX router is advertising the default route, the MAX makes a routing decision based on Hop and Tick count.

IPX and PPP link compression

NetWare relies on the Data Link layer (also called Layer 2) to validate and guarantee data integrity. STAC link compression, if specified, generates an eight-bit checksum, which is inadequate for NetWare data.

If your MAX supports NetWare (either routed or bridged), and you require link compression, you should configure your MAX in one of the following ways:

- Configure either STAC-9 or MS-STAC link compression, which use a more robust error-checking method, for any connection profile supporting IPX data. Configure link compression in the Ethernet > Answer > PPP Options > Link Comp parameter and Ethernet > Connections > *Any Connection profile* > Encaps Options > Link Comp parameter.
- Enable IPX-checksums on your NetWare servers and clients. (Both server and client must support IPX-checksums. If you enable checksums on your servers but your clients do not support checksums, they will fail to log in successfully.)
- Disable link compression completely by setting Ethernet > Answer > PPP Options > Link Comp = None and Ethernet > Connections > *Any Connection profile* > Encaps Options > Link Comp = None. By disabling link compression, the MAX validates and guarantees data integrity by means of PPP.

Ascend extensions to standard IPX

NetWare uses dynamic routing and service location, so clients expect to be able to locate a server dynamically, regardless of its physical location. To help accommodate these expectations in a WAN environment, Ascend provides two IPX extensions: IPX Route profiles and IPX SAP filters.

(For information about the Handle IPX parameter and IPX bridging, see Chapter 8, “Configuring Packet Bridging.”)

IPX Route profiles

IPX Route profiles specify static IPX routes. When the MAX clears its RIP and SAP tables because of a reset or power-cycle, it adds the static routes when it reinitializes. Each static route contains the information needed to reach one server.

If the MAX connects to another Ascend unit, some sites choose not to configure a static route. Instead, after a power-cycle or reset, the initial connection to that site must be activated manually. After the initial connection, the MAX downloads the RIP table from the remote site and maintains the routes as static until the next power-cycle or reset.

Static routes need manual updating whenever you remove the specified server or change the address. However, static routes help prevent timeouts when a client takes a long time to locate a server across a remote WAN link. (For more information, see “Configuring static IPX routes” on page 9-18, or see the *Configurator Online Help* for information about parameters in a profile.)

IPX SAP filters

Many sites do not want the MAX SAP table to include long lists of all services available at a remote site. IPX SAP filters enable you to exclude services from, or explicitly include certain services in, the SAP table.

SAP filters can be applied to inbound or outbound SAP packets. Inbound filters control the services you add to the MAX unit's SAP table from advertisements on a network link. Outbound filters control which services the MAX advertises on a particular network link. (For more information, see "Creating and applying IPX SAP filters" on page 9-20.)

WAN considerations for NetWare client software

NetWare clients on a wide area network do not need special configuration in most cases. Following are some considerations regarding NetWare clients in an IPX routing environment, and Ascend's recommendations.

Consideration	Recommendation
Preferred servers	If the local IPX network supports NetWare servers, configure NetWare clients with a preferred server on the local network, not at a remote site. If the local Ethernet does not support NetWare servers, configure local clients with a preferred server that is on the network with the lowest connection costs. (For more information, see your NetWare documentation for more information.)
Local copy of LOGIN.EXE	Because of possible performance issues, executing programs remotely is not recommended. You should put LOGIN.EXE on each client's local drive.
Packet Burst (NetWare 3.11)	Packet Burst lets servers send a data stream across the WAN before a client sends an acknowledgment. The feature is enabled by default in server and client software for NetWare 3.12 or later. If local servers are running NetWare 3.11, they should have PBURST.NLM loaded. (For more information, see your NetWare documentation.)
Macintosh or UNIX clients	Both Macintosh and UNIX clients can use IPX to communicate with servers. But they also support native communications via AppleTalk or TCP/IP, respectively. If Macintosh clients must use AppleTalk software (rather than MacIPX) to access NetWare servers across the WAN, the WAN link must support bridging. Otherwise, AppleTalk packets do not make it across the connection. If UNIX clients access NetWare servers via TCP/IP (rather than UNIXWare), the MAX must be configured as either a bridge or an IP router. Otherwise, TCP/IP packets do not make it across the connection.

Enabling IPX routing in the MAX

The Ethernet profile configures system-global parameters that affect all IP interfaces in the MAX. Following are the related parameters (shown with sample settings):

```
Ethernet
   Mod Config
      IPX Routing=Yes
      Ether options…
         IPX Frame=802.2
         IPX Enet #=00000000
         IPX Pool #=CCCC1234
```

Understanding the global IPX parameters

This section provides some background information about IPX routing in the Ethernet profile. For detailed information about each parameter, see the *MAX Reference Guide*.

IPX Routing

When you set to Yes, the IPX Routing parameter enables IPX routing mode. When you enable IPX routing in the MAX and close the Ethernet profile, the MAX comes up in IPX routing mode, uses the default frame type 802.2 (which is the suggested frame type for NetWare 3.12 or later), and listens on the Ethernet to acquire its IPX network number from other IPX routers on that segment.

IPX Frame

The MAX routes and spoofs only one IPX frame type (IEEE 802.2 by default), as specified in the IPX Frame parameter. If some NetWare software transmits IPX in a frame type other than the type specified here, the MAX drops those packets or, if you enable bridging, bridges them. If you are not familiar with the concept of packet frames, see the Novell documentation.

IPX Enet #

The IPX Enet # parameter specifies the IPX network number for the Ethernet interface of the MAX. The easiest way to ensure that the number is correct is to leave the default null address. The null address causes the MAX to listen for its network number and acquire it from another router on the same interface. If you enter a number other than zero, the MAX becomes a *seeding* router, and other routers can learn their IPX network number from the MAX. (For details about seeding routers, see the Novell documentation.)

IPX Pool #

The IPX Pool # parameter specifies a virtual IPX network to be assigned to dial-in NetWare clients. Dial-in clients do not belong to an IPX network, so they must be assigned an IPX network number to establish a routing connection with the MAX. The MAX advertises the route to this virtual network and assigns it as the network address for dial-in clients.

The dial-in Netware client must accept the network number, although it can provide its own node number or accept a node number provided by the MAX. If the client does not have a unique node address, the MAX assigns the node address as well.

Examples of IPX routing configuration

This section shows the simple configuration in which the MAX uses the default frame type and learns its network number from other routers on the Ethernet. It also shows a more complex router configuration whose values you enter explicitly.

A basic configuration using default values

In this example, the MAX routes IPX packets in 802.2 frames and learns its IPX network number from other routers on the Ethernet. It does not define a virtual network for dial-in clients. To configure the MAX Ethernet profile:

1 Open the Ethernet profile.

2 Set IPX Routing to Yes:

```
Ethernet
   Mod Config
      IPX Routing=Yes
```

3 Close the Ethernet profile.

When you close the Ethernet profile, the MAX comes up in IPX routing mode, uses the default frame type of 802.2, and acquires its IPX network number from other routers.

A more complex example

In this example, the MAX routes IPX packets in 802.3 frames (other frame types are bridged), and uses the IPX network number CF0123FF. It also supports a virtual IPX network for assignment to dial-in clients.

To verify that the MAX should use 802.3 frames, go to the NetWare server's console and type LOAD INSTALL to view the AUTOEXEC.NCF file. Look for lines similar to the following:

```
internal network 1234
Bind ipx ipx-card net=CF0123FF
Load 3c509 name=ipx-card frame=ETHERNET_8023
```

The last line specifies the 802.3 frame type. To verify that the IPX network number you assign to the MAX Ethernet interface is compatible with other servers and routers on that interface, check the BIND line in the AUTOEXEC.NCF file. The second line in the example above specifies the number CF0123FF.

Note: Every IPX network number on each network segment and internal network within a server on the *entire WAN* must be unique. So you should know both the external and internal network numbers in use at all sites.

To configure the Ethernet profile:

1 Open Ethernet > Mod Config and set IPX Routing to Yes:

```
Ethernet
   Mod Config
      IPX Routing=Yes
```

2 Open the Ether Options subprofile.

3 Specify the 802.3 frame type and set the IPX network number for the Ethernet interface. For example:

```
Ether options…
   IPX Frame=802.2
   IPX Enet #=00000000
```

4 Assign a network number for assignment to dial-in clients.

```
   IPX Pool #=CCCC1234
```

Note: The most common configuration mistake on NetWare internetworks is in assigning duplicate network numbers. Make sure that the network number you specify in the IPX Pool# field is unique within the entire IPX routing domain of the MAX unit.

5 If more than one frame type needs to cross the WAN, make sure that you enable Bridging (as described in Chapter 8, "Configuring Packet Bridging.").

```
Bridging=Yes
```

6 Close the Ethernet profile.

Verifying the router configuration

You can IPXPING a NetWare server or client from the MAX to verify that it is up and running on the IPX network. To do so:

1 Invoke the terminal-server command-line interface.

2 Enter the IPXPING command with the advertised name of a NetWare server. For example:

```
ascend% ipxping server-1
```

3 Terminate IPXPING at any time by pressing Ctrl-C.

Configuring IPX routing connections

You configure IPX routing connections, by setting parameters in the Answer profile and in Connection profiles. Following are the related parameters (shown with sample settings):

```
Ethernet
   Answer
      PPP options...
         Route IPX
         Recv Auth=Either

   Session options…
      IPX SAP Filter=1

Ethernet
   Connections
     any Connection profile
       Station=device-name
       Route IPX=Yes
       Encaps options...
         Recv PW=localpw

       IPX options...
         Peer=Router
         IPX RIP=None
         IPX SAP=Send
         Dial Query=No
```

```
  IPX Net#=cfff0003
  IPX Alias#=00000000
  Handle IPX=None
  Netware t/o=30
  SAP HS Proxy=N/A
  SAP HS Proxy Net#1=N/A
  SAP HS Proxy Net#2=N/A
  SAP HS Proxy Net#3=N/A
  SAP HS Proxy Net#4=N/A
  SAP HS Proxy Net#5=N/A
  SAP HS Proxy Net#6=N/A
Sessions options…
  IPX SAP Filter=1
```

Understanding the IPX connection parameters

This section provides some background information about IPX connections. For detailed information about each parameter, see the *MAX Reference Guide*.

Enabling IPX routing in the Answer profile

You must enable IPX routing in the Answer profile for the MAX to pass IPX packets to the bridge/router software.

Authentication method used for passwords received from the far end

The Recv Auth parameter specifies the protocol to use for authenticating the password sent by the far end during PPP negotiation. IPX connections require this parameter, because the MAX cannot verify Connection profiles by address as it does for IP connections.

IPX SAP filters

You can apply an IPX SAP filter to exclude or explicitly include certain remote services from the MAX unit's SAP table. If you apply a SAP filter in a Connection profile, you can exclude or explicitly include services in both directions (as described in "Creating and applying IPX SAP filters" on page 9-20).

Station name and Recv PW in a Connection profile

The MAX requires name and password authentication for IPX connections, because the MAX cannot verify Connection profiles by address as it does for IP connections.

Peer dialin for routing to NetWare clients

Dial-in NetWare clients do not have IPX network addresses. To establish an IPX routing connection to the local network, such a client must dial in with PPP software and the Connection profile must specify Peer=Dialin. In addition, the MAX must have a virtual IPX network defined for assignment to these clients (as described in IPX Pool # on page 9-5).

Peer=Dialin causes the MAX to assign the virtual IPX network number to the dial-in client during PPP negotiation. If the client does not provide its own unique node number, the MAX assigns a unique node number to the client. The MAX does not send RIP and SAP advertisements across the connection, and it ignores RIP and SAP advertisements received from the far end. However, it does respond to RIP and SAP queries received from dial-in clients. See “An example dial-in client connection” on page 7-18.

Controlling RIP and SAP transmissions across the WAN connection

The IPX RIP and IPX SAP parameters in a Connection profile define how the MAX handles RIP and SAP packets across this WAN connection.

Set IPX RIP to Both (the default), indicating that RIP broadcasts will be exchanged in both directions. You can disable the exchange of RIP broadcasts across a WAN connection, or specify that the MAX only send or only receive RIP broadcasts on that connection.

Set IPX SAP to Both (the default), indicating that SAP broadcasts will be exchanged in both directions. If you enable SAP to both send and receive broadcasts on the WAN interface, the MAX broadcasts its entire SAP table to the remote network and listens for SAP table updates from that network. Eventually, both networks have a full table of all services on the WAN. To control which services are advertised and where, you can disable the exchange of SAP broadcasts across a WAN connection, or specify that the MAX only send or only receive SAP broadcasts on that connection.

Dial Query for bringing up a connection based on service queries

Setting the Dial Query parameter to Yes configures the MAX to bring up a connection when it receives a SAP query for service type 0004 (File Server), if that service type is not present in the MAX SAP table. If the MAX has no SAP table entry for service type 0004, it brings up every connection that has Dial Query set. If 20 Connection profiles have Dial Query set, the MAX brings up all 20 connections in response to the query.

Note: If the MAX unit has a static IPX route for even one remote server, it brings up that connection instead of choosing the more costly solution of bringing up every connection that has Dial Query set.

IPX network and alias

IPX Net # specifies the IPX network number of the remote-end router. Rarely needed, it is provided only for those remote-end routers that require the MAX to know their router’s network numbers before connecting. IPX Alias specifies a second IPX network number, to be used only when connecting to non-Ascend routers that use numbered interfaces.

Handle IPX client or server bridging

The Handle IPX parameter defines the handling of bridged connections. When you enable IPX routing for a connection, IPX Routing = N/A. (For more information, see Chapter 8, “Configuring Packet Bridging.”)

Netware T/O watchdog spoofing

The Netware T/O parameter defines the number of minutes the MAX enables clients to remain logged in after losing a connection.

NetWare servers send out NCP watchdog packets to determine which logins are active so that they can log out inactive clients. Only clients that respond to watchdog packets remain logged in.

Watchdog packets can cause a WAN connection to stay up unnecessarily. But if the MAX simply filtered them, the remote server would drop active as well as inactive client logins. To prevent unwanted client logouts while enabling WAN connections to be brought down in times of inactivity, the MAX local to IPX servers responds to NCP watchdog requests as a proxy for clients on the other side of an IPX routing or IPX bridging connection. Responding to such requests is commonly called watchdog spoofing.

To the server, a spoofed connection looks like a normal, active client login session, so it does not log the client out. The timer begins counting down as soon as the link goes down. At the end of the selected time, the MAX stops responding to watchdog packets and the server can release the client-server connections. If the WAN session reconnects before the end of the selected time, the MAX resets the timer.

Note: The MAX filters watchdog packets automatically on all IPX routing connections and all IPX bridging connections that have watchdog spoofing enabled. The MAX applies a call filter implicitly, which prevents the idle timer from resetting when the MAX sends or receives IPX watchdog packets. You apply this filter after the standard data and call filters.

SAP HS Proxy (NetWare SAP Home Server Proxy)

By setting SAP HS Proxy parameters, you can configure the MAX to forward SAP broadcasts to specified IPX networks, thus ensuring that remote users access the same resources as local users.

By default, when you initially load any IPX client software on your PC, the MAX broadcasts a SAP Request packet asking for any servers to reply. The MAX takes the first SAP reply received to be the nearest server, and attaches your PC to that server.

If you load your client software from another PC, or use the same PC when traveling, the response to the initial SAP Request could attach you to a different server. With SAP HS Proxy, you can direct SAP Requests to specific networks. The SAP Responses come from servers on these specified networks rather than the server nearest the MAX. To configure the parameters, see “Configuring the NetWare SAP Home Server Proxy” on page 9-17.

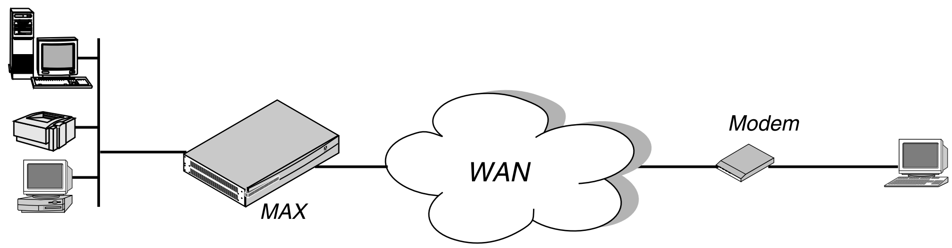
Examples of IPX routing connections

This section shows sample WAN connections using IPX routing. If the MAX has not yet been configured for IPX routing, see "Enabling IPX routing in the MAX" on page 9-5.

Configuring a dial-in client connection

In this example, a NetWare client dials into a corporate IPX network by using PPP dial-in software. Figure 9-1 shows corporate network supporting both NetWare servers and clients.

Figure 9-1. A dial-in NetWare client



To configure an IPX routing connection for the client:

1 Open Ethernet > Mod Config > Ether Options and verify that an IPX Pool assignment exists. For example:

```
Ethernet
   Mod Config
      Ether options…
         IPX Pool #=CCCC1234
```

2 Close the Ethernet profile.

3 Open Answer > PPP Options.

4 Enable IPX routing and PAP/CHAP authentication:

```
Ethernet
   Answer
      PPP options...
         Route IPX
         Recv Auth=Either
```

5 Close the Answer profile.

6 Open the Connection profile for the dial-in user.

7 Specify the dial-in client's login name and activate the profile. For example:

```
Ethernet
   Connections
      Station=scottpc
      Active=Yes
```

8 Enable IPX routing:

```
      Route IPX=Yes
```

9 Select PPP encapsulation and configure the dial-in client's password. For example:

```
      Encaps=PPP
      Encaps options...
         Recv PW=scottpw
```

10 Open the IPX Options subprofile and specify a dial-in client:

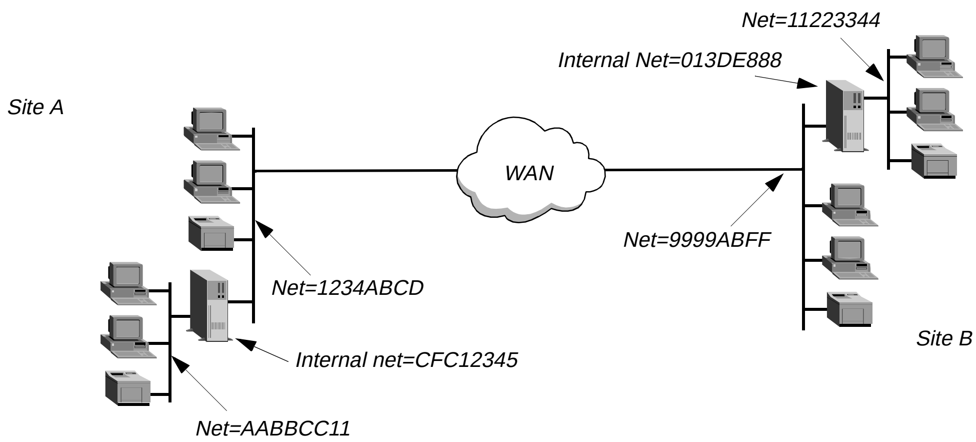
```
IPX options...
   Peer=Dialin
   IPX RIP=None
```

11 Close the Connection profile.

Configuring a connection between two LANs

In this example, the MAX connects to an IPX network that supports both servers and clients and connects with a remote site that also supports both servers and clients as shown in Figure 9-2.

Figure 9-2. A connection with NetWare servers on both sides



Site A and Site B both have Novell LANs that support NetWare 3.12 and NetWare 4 servers, NetWare clients, and a MAX. The NetWare server at Site A has the following configuration settings:

```
Name=SERVER-1
internal net CFC12345
Load 3c509 name=ipx-card frame=ETHERNET_8023
Bind ipx ipx-card net=1234ABCD
```

The NetWare server at Site B has the following configuration settings:

```
Name=SERVER-2
internal net 013DE888
Load 3c509 name=net-card frame=ETHERNET_8023
Bind ipx net-card net=9999ABFF
```

To establish the connection shown in Figure 9-2, you would configure the MAX at Site A, enable IPX routing for its Ethernet interface, and configure a static route to the remote server. The same procedures would apply to Site B.

Configuring the MAX at Site A:

At Site A:

1. Make sure you assign the MAX a system name in the System profile. This example uses the name SITEAGW.
2. If you have not done so already, configure the Ethernet profile (as described in “Enabling IPX routing in the MAX” on page 9-5).
3. In Answer > PPP Options, enable IPX routing and PAP/CHAP authentication, and then close the Answer profile.

```
Ethernet
   Answer
      PPP options...
         Route IPX
         Recv Auth=Either
```

   (If the MAX needs to support multiple IPX frame types, you must also enable bridging in the Answer profile.)

4. Open the Connection profile for Site B.

   In this example, the Connection profile for Site B is profile #5. A profile’s number is the unique part of the number you assign in the Connections menu. For example, the Connection profile defined as 90-105 is #5.

5. Set up the Connection profile as follows:

```
Ethernet
   Connections
      profile 5...
         Station=SITEBGW
         Active=Yes
         Encaps=MPP
         PRI # Type=National
         Dial #=555-1212
         Route IPX=Yes

         Encaps options...
            Send Auth=CHAP
            Recv PW=*SECURE*
            Send PW=*SECURE*

         IPX options...
            IPX RIP=None
            IPX SAP=Both
            NetWare t/o=30
            SAP HS Proxy=N/A
            SAP HS Proxy Net#1=N/A
            SAP HS Proxy Net#2=N/A
            SAP HS Proxy Net#3=N/A
            SAP HS Proxy Net#4=N/A
            SAP HS Proxy Net#5=N/A
           SAP HS Proxy Net#6=N/A
```

6. Close Connection profile #5.
7. Open an IPX Route profile.
8. Set IPX RIP to None in the Connection profile, and configure a static route to the remote server.
9. Set up a route to the remote NetWare server (SERVER-2). Use the following settings:

```
Ethernet
   IPX Routes
      Server Name=SERVER-2
      Active=Yes
      Network=013DE888
      Node=000000000001
      Socket=0451
      Server Type=0004
      Connection #=5
```

Note: The Connection # parameter in the IPX Route profile must match the number of the Connection profile you configured for that site. If you specify the internal network number of a server, make sure you specify Server Name and Server Type. If you specify an external network, do not specify Server Name or Server Type.

10 Close the IPX Route profile.

Configuring the MAX at Site B:

At Site B:

1 Assign a system name to the Ascend unit at Site B in the unit's System profile. This example uses the name SITEBGW.

2 Verify that the Site B unit's Ethernet interface has a configuration defined for IPX routing (For instructions, see "Enabling IPX routing in the MAX" on page 9-5.)

3 Verify that the Site B unit's Answer profile enables IPX routing and PAP/CHAP authentication.

4 Open the Connection profile for Site A.

   In this example, the Connection profile for site A is profile #2. A profile's number is the unique part of the number you assign in the Connections menu. For example, the Connection profile defined as 90-102 is #2.

5 Set up the Connection profile as follows:

```
Ethernet
   Connections
      profile 2...
         Station=SITEAGW
         Active=Yes
         Encaps=MPP
         PRI # Type=National
         Dial #=555-1213
         Route IPX=Yes

         Encaps options...
            Send Auth=CHAP
            Recv PW=*SECURE*
            Send PW=*SECURE*

         IPX options...
            IPX RIP=None
            IPX SAP=Both
            NetWare t/o=30
            SAP HS Proxy=N/A
            SAP HS Proxy Net#1=N/A
            SAP HS Proxy Net#2=N/A
            SAP HS Proxy Net#3=N/A
            SAP HS Proxy Net#4=N/A
```

```
      SAP HS Proxy Net#5=N/A
      SAP HS Proxy Net#6=N/A
```

6 Close Connection profile #2.

7 Open an IPX Route profile.

Set IPX RIP to None in the Connection profile, and configure a static route to the remote server.

8 Set up a route to the remote NetWare server (SERVER-1). Use the following settings:

```
Ethernet
   IPX Routes
      Server Name=SERVER-1
      Active=Yes
      Network=CFC12345
      Node=000000000001
      Socket=0451
      Server Type=0004
      Connection #=2
```

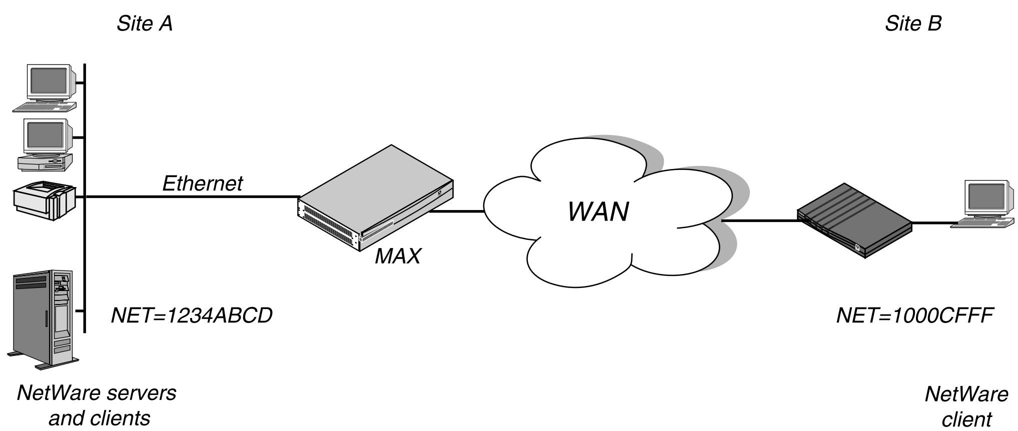
Note: The Connection # parameter in the IPX Route profile must match the number of the Connection profile you configured for that site. If you specify the internal network number of a server, make sure you specify Server Name and Server Type. If you specify an external network, do not specify Server Name or Server Type.

9 Close the IPX Route profile.

Configuring a connection with local servers only

In this example, the MAX connects to a local IPX network that supports both servers and clients, and connects to a geographically remote network that supports one or more NetWare clients. Figure 9-3 shows the setup.

Figure 9-3. A dial-in client that belongs to its own IPX network



In this example, Site A supports NetWare 3.12 servers, NetWare clients, and a MAX. The NetWare server at Site A has the following configuration settings:

```
Name=SERVER-1
internal net CFC12345
Load 3c509 name=ipx-card frame=ETHERNET_8023
Bind ipx ipx-card net=1234ABCD
```

Site B is a home office that consists of one PC and an Ascend unit. It is not an existing Novell LAN, so the Ascend unit configuration creates a new IPX network (1000CFFF, for example).

Note: The new IPX network number assigned to Site B in this example cannot be in use *anywhere* on the entire IPX wide-area network. That is, it cannot be in use at Site A or any network that connects to Site A.

This example assumes that the Ethernet profile and Answer profile have already been set up to enable IPX routing. The initial connection between the two Ascend units should be manually dialed (using the DO menu) because you do not use static routes.

To configure the MAX at Site A

At Site A:

1 Assign a system name in the System profile for the MAX. This example uses the name SITEAGW.

2 Open the Connection profile for Site B.

3 Set up the Connection profile as follows:

```
Ethernet
   Connections
      Station=SITEBGW
      Active=Yes
      Encaps=MPP
      PRI # Type=National
      Dial #=555-1212
      Route IPX=Yes

      Encaps options...
         Send Auth=CHAP
         Recv PW=*SECURE*
         Send PW=*SECURE*
      IPX options...

         IPX RIP=Both
         IPX SAP=Both
         NetWare t/o=30
         SAP HS Proxy=N/A
         SAP HS Proxy Net#1=N/A
         SAP HS Proxy Net#2=N/A
         SAP HS Proxy Net#3=N/A
         SAP HS Proxy Net#4=N/A
         SAP HS Proxy Net#5=N/A
        SAP HS Proxy Net#6=N/A
```

4 Close the Connection profile.

To configure the Ascend unit at Site B

At Site B:

1. Assign a system name in the System profile for the MAX. This example uses the name SITEBGW.
2. Open the Connection profile for Site B.
3. Set up the Connection profile as follows:

```
Ethernet
   Connections
      Station=SITEBGW
      Active=Yes
      Encaps=MPP
      PRI # Type=National
      Dial #=555-1213
      Route IPX=Yes

      Encaps options...
         Send Auth=CHAP
         Recv PW=*SECURE*
         Send PW=*SECURE*

      IPX options...
         IPX RIP=Both
         IPX SAP=Both
         NetWare t/o=30
         SAP HS Proxy=N/A
         SAP HS Proxy Net#1=N/A
         SAP HS Proxy Net#2=N/A
         SAP HS Proxy Net#3=N/A
         SAP HS Proxy Net#4=N/A
         SAP HS Proxy Net#5=N/A
        SAP HS Proxy Net#6=N/A
```

4. Close the Connection profile.

Configuring the NetWare SAP Home Server Proxy

To configure the NetWare SAP Home Server Proxy parameters:

1. Open the Ethernet > Connections > *any Connection Profile* > IPX Options menu.
2. Set the SAP HS Proxy parameter to Yes.
3. Specify the IPX network address to which SAP broadcasts will be directed. For example:

   `SAP HS Proxy Net#1=CB1123BC`

   This specifies that any SAP Broadcast Requests received from this user will be directed to IPX network CB1123BC.
4. If you want to define other networks, repeat Step 3 for `SAP HS Proxy Net#2`.

Configuring static IPX routes

A static IPX route includes all of the information needed to reach one NetWare server on a remote network. When the MAX receives an outbound packet for that server, it finds the referenced Connection profile and dials the connection. You configure the static route in an IPX Route profile.

You do not need to create IPX static routes to servers that are on the local Ethernet.

Most sites configure only a few IPX routes and rely on RIP for most other connections. If you have servers on both sides of the WAN connection, you should define a static route to the remote site even if your environment requires dynamic routes. If you have one static route to a remote site, it should specify a *master* NetWare server that knows about many other services. NetWare workstations can then learn about other remote services by connecting to that remote NetWare server.

Note: Remember that you manually configure static IPX routes, so you must update them if there is a change to the remote server.

To configure a static route, set the following parameters (shown with sample settings):

```
Ethernet
   IPX Routes
      Server Name=server-name
      Active=Yes
      Network=CC1234FF
      Node=000000000001
      Socket=0000
      Server Type=0004
      Hop Count=2
      Tick Count=12
      Connection #=0
```

Understanding the static route parameters

This section provides some background information about static route configurations. For detailed information about each parameter, see the *MAX Reference Guide*.

Parameter	Usage
Server's name	Each IPX Route profile contains the information needed to reach one NetWare server on a remote network. Server Name is the remote server's name.
Active	Must be set to Yes for the MAX to read this route into its internal IPX RIP table.
Network and Node	Specify the remote server's internal network number and node number. (If you are not familiar with internal network numbers, see the Novell documentation.) The node number for the NetWare file servers is typically 0000000000001 (the default Node setting).

Parameter	Usage
Socket	Typically, Novell file servers use socket 0451. The number you specify must be a well-known socket number. Services that use dynamic socket numbers can use a different socket each time they load and will not work with IPX Route profiles. To bring up a connection to a remote service that uses a dynamic socket number, specify a *master* server that uses a well-known socket number on the remote network.
Type	SAP advertises services by a type number. For example, NetWare file servers are SAP service type 0004 or 0x0004.
Hop Count and Tick Count	Usually, the default Hop Count and Tick Count settings of 2 and 12 respectively, are appropriate, but you can increase these value, for very distant servers. Ticks are IBM PC clock ticks (1/18 second). Note that the MAX calculates the best routes on the basis of on tick count, not hop count.
Connection	When the MAX receives a query for the specified server or a packet addressed to that server, it finds the referenced Connection profile and dials the connection. Identify a Connection profile by the unique part of its number in the Connections menu.

Examples of static-route configuration

This example shows a static route configuration to a remote NetWare server. Remember that you manually configure static IPX routes, so you must update them if there is a change to the remote server. To define an IPX Route profile:

1 Open an IPX Route profile.

2 Specify the name of the remote NetWare server and activate the route:

```
Ethernet
   IPX Routes
      Server Name=SERVER-1
      Active=Yes
```

3 Because this is a route to a server's internal network, specify the server's internal network number, node, socket, and service type. For example:

```
      Network=CC1234FF
      Node=000000000001
      Socket=0451
      Server Type=0004
```

4 Specify the distance to the server in hops and IBM PC clock ticks. (The default values are appropriate unless the server is very distant.)

```
      Hop Count=2
      Tick Count=12
```

5 Specify the number of the Connection profile. For example:

```
      Connection #=2
```

6 Close the IPX Route profile.

Creating and applying IPX SAP filters

IPX SAP filters specify which services to include in the MAX service table or in SAP response packets sent across the WAN. (You can also prevent the MAX from sending its SAP table or receiving a remote site's SAP table by turning off IPX SAP in a Connection profile as described in "Understanding the IPX connection parameters" on page 9-8.)

To configure IPX SAP filters, you set the following parameters (shown with sample settings):

```
Ethernet
 IPX SAP Filters
   any filter profile
      Name=optional
      Input SAP filters...
         In SAP filter 01–08
            Valid=Yes
            Type=Exclude
            Server Type=0004
            Server Name=SERVER-1
      Output SAP filters
   any filter profile
         Out SAP filter 01–08
            Valid=Yes
            Type=Exclude
            Server Type=0004
            Server Name=SERVER-1

Ethernet
   Mod Config
      Ether options...
         IPX SAP Filter=1

Ethernet
   Answer
      Session options...
         IPX SAP Filter=2

Ethernet
   Connections
      Session options...
         IPX SAP Filter=2
```

Understanding the IPX SAP filter parameters

This section provides some background information about SAP filters. For detailed information about each parameter, see the *MAX Reference Guide*.

Input SAP Filters and Output SAP Filters

Each filter contains up to eight Input filters and output filters, which you define individually and apply in order (1–8) to the packet stream. Apply the input filters to all SAP packets the MAX receives. They screen advertised services and exclude them from or include them in the MAX service table as specified by the filter conditions.

Apply output filters to SAP response packets the MAX transmits. If the MAX receives a SAP request packet, it applies output filters before transmitting the SAP response, and excludes services from or includes services in the response packet as specified by the output filters.

Valid

In an individual input or output filter, set the Valid parameter to Yes to enable the filter for use.

Type

In an individual input or output filter, set the Type parameter to specify whether the filter includes the service or excludes it.

Server Type

Server Type specifies a hexadecimal number representing a type of NetWare service to be included or excluded as specified by the Type parameter. For example, the number for file services is 0004.

In an input filter, the Type parameter specifies whether to include remote services of the specified type in the MAX service table or exclude them.

In an output filter, the Type parameter specifies whether to include advertisements for the specified service type in SAP response packets or to exclude them.

Server Name

In an individual input or output filter, the Server Name parameter identifies a local or remote NetWare server by name.

If the server is on the local network, you might name it in an output filter in which the Type parameter specifies whether or not to include advertisements for this server in SAP response packets.

If the server is on the remote IPX network, you might name it in an input filter in which the Type parameter specifies whether or not to include this server in the MAX service table.

Applying IPX SAP filters

You can apply an IPX SAP filter to the local Ethernet or to WAN interfaces, or both.

When applied in the Ethernet profile, a SAP filter either includes specific servers or services in the MAX unit’s SAP table or includes them from the table. If directory services is not supported, servers or services that are not in the MAX table are inaccessible to clients across the WAN. A filter applied to the Ethernet interface takes effect immediately.

When applied in the Answer profile, a SAP filter screens service advertisements from across the WAN.

When applied in a Connection profile, a SAP filter screens service advertisements to and from a specific WAN connection.

Example of IPX SAP filter configuration

This example shows how to create an IPX SAP filter that prevents local NetWare users from having access to a remote NetWare server. The example also shows how to apply the filter to the Answer profile and the Connection profile used to reach the server's remote network.

To define an IPX SAP filter that excludes a remote file server from the MAX SAP table:

1 Open IPX SAP Filter profile #1 (for this example) and then open the list of Input filters:

```
Ethernet
   IPX SAP Filters
      profile #1...
         Name=NOSERVER-1
         Input SAP filters...
            In SAP filter 01
            In SAP filter 02
            In SAP filter 03
            In SAP filter 04
            In SAP filter 05
            In SAP filter 06
            In SAP filter 07
            In SAP filter 08
```

2 Open Input SAP filter 01, activate it by setting Valid to Yes, and set Type to Exclude.

3 Specify the NetWare server's name and service type (for a file server, 0004):

```
            In SAP filter 01
               Valid=Yes
               Type=Exclude
               Server Type=0004
               Server Name=SERVER-1
```

4 Close the IPX SAP Filter profile.

To apply the IPX SAP Filter in the Answer profile and in a Connection profile:

1 Open Answer > Session Options.

2 Specify IPX SAP Filter profile #1, and then close the Answer profile.

```
Ethernet
   Answer
      Session options...
         IPX SAP Filter=1
```

3 Repeat the same assignment in Connections > Session Options.

```
Ethernet
   Connections
      Session options...
         IPX SAP Filter=1
```

4 Close the Connection profile.

Configuring IP Routing

10

Introduction to IP routing and interfaces

The first task in this chapter, setting up the IP network, involves setting parameters in the MAX unit's Ethernet profile. The parameters define the unit's Ethernet IP interface, network services (such as DNS), and routing policies.

In the next task, configuring IP routing connections, you configure Connection profiles (or similar profiles in an external authentication server) to define destinations across WAN interfaces and to add routes to the routing table.

For configuring IP routes and preferences and configuring the MAX for dynamic route updates, you configure the IP profile and individual Connection profiles to set up the IP routing table, which determines the paths over which IP packets are forwarded and specifies the connections to be brought up.

To perform the tasks described in this chapter, you have to understand how the MAX uses IP addresses and subnet masks, IP routes, and IP interfaces.

IP addresses and subnet masks

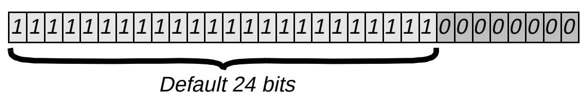
In the MAX, you specify IP addresses in dotted decimal format (not hexadecimal). If you specify no subnet mask, the MAX assumes that the address contains the default number of network bits for its class. In other words, in Table 10-1 shows the classes and the default number of network bits for each class corresponds to the default subnet mask for that class.

Table 10-1. IP address classes and number of network bits

Class	**Address range**	**Network bits**
Class A	0.0.0.0 — 127.255.255.255	8
Class B	128.0.0.0 — 191.255.255.255	16
Class C	192.0.0.0 — 223.255.255.255	24

For example, a class C address, such as 198.5.248.40, has 24 network bits, so its default mask is *24*. The 24 network bits leave 8 bits for the host portion of the address. So one class C network supports up to 253 hosts.

Figure 10-1. Default mask for class C IP address

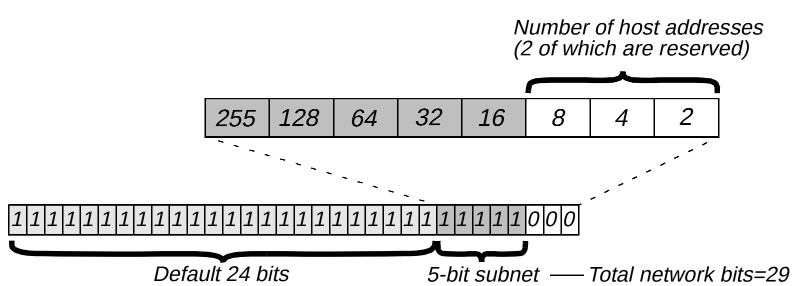


As shown in Figure 10-1, a mask has a binary 1 in each masked position. Therefore, the default, 24-bit, subnet mask for a class C address can be represented in dotted decimal notation as 255.255.255.0. For specifying a different subnet mask, the MAX supports a modifier consisting of a slash followed by a decimal number that represents the number of network bits in the address. For example, 198.5.248.40/29 is equivalent to:

```
IP address = 198.5.248.40
Mask = 255.255.255.248
```

That is, the mask specification indicates that the first 29 bits of the address specify the network. This is a 29-bit subnet. The three remaining bits specify unique hosts, as shown in Figure 10-2.

Figure 10-2. A 29-bit subnet mask and the number of supported hosts



In Figure 10-2, three available bits present eight possible bit combinations. Of the eight possible host addresses, two are reserved, as follows:

000 — Reserved for the network (base address)
001
010
011
100
101
110
111—Reserved for the broadcast address of the subnet

Zero subnets

Early implementations of TCP/IP did not allow zero subnets. That is, subnets could not have the same base address that a class A, B, or C network would have. For example, the subnet 192.168.8.0/30 was illegal because it had the same base address as the class C network 192.168.8.0/24, while 192.168.8.4/30 was legal. The first example (192.168.8.0/30 is called a zero subnet, because like a class C base address, its last octet is zero). Modern implementations of TCP/IP enable subnets to have base addresses that can be identical to the class A, B, or C base addresses. Ascend's implementations of RIP 2 and OSPF treat these so-called zero subnetworks the same as any other network. You should decide whether or not to support and configure zero subnetworks for your environment. If you configure them in some cases and treat them as unsupported in other cases, you encounter routing problems.

Table 10-2 shows how the standard subnet address format relates to Ascend notation for a class C network number.

Table 10-2. Standard subnet masks

Subnet mask	Number of host addresses
255.255.255.128	126 hosts + 1 broadcast, 1 network (base)
255.255.255.192	62 hosts + 1 broadcast, 1 network (base)
255.255.255.224	30 hosts + 1 broadcast, 1 network (base)
255.255.255.240	14 hosts + 1 broadcast, 1 network (base)
255.255.255.248	6 hosts + 1 broadcast, 1 network (base)
255.255.255.252	2 hosts + 1 broadcast, 1 network (base)
255.255.255.254	invalid netmask (no hosts)
255.255.255.255	1 host — a host route

The broadcast address of any subnet has the host portion of the IP address set to all ones. The network address (or base address) represents the network itself, with the host portion of the IP address set to all zeros. Therefore, these two addresses define the address range of the subnet.

For example, if the MAX configuration assigns the following address to a remote router:

```
IP address = 198.5.248.120
Mask = 255.255.255.248
```

the Ethernet attached to that router has the following address range:

```
198.5.248.120 — 198.5.248.127
```

A host route is a special case IP address with a subnet mask of 32 bits. It has a subnet mask of `255.255.255.255` (32 bits).

IP routes

At system startup, the MAX builds an IP routing table that contains configured routes. When the system is up, it can use routing protocols such as RIP or OSPF to learn additional routes dynamically. In each routing table entry, the Destination field specifies a destination network address that can appear in IP packets, and the Gateway field specifies the address of the next-hop router to reach that destination. Each entry also has a preference value and a metric value, which the MAX evaluates when comparing multiple routes to the same destination.

How the MAX uses the routing table

The MAX relies on the routing table to forward IP packets, as follows:

- If the MAX finds a routing table entry whose Destination field matches a packet's destination address, it routes the packet to the specified next-hop router, whether through its WAN interface or through its Ethernet interface.
- If the MAX does not find a matching entry, it looks for the Default route, which is identified in the routing table by a destination of 0.0.0.0. If that route has a specified next-hop router, the MAX forwards the packet to that router.
- If the MAX does not find a matching entry and does not have a valid Default route, it drops the packet.

Static routes

A static route is a manually configured path from one network to another. It specifies the destination network and the gateway (router) to use to get to that network. If a path to a destination must be reliable, the administrator often configures more than one static route to the destination. In that case, the MAX chooses the route on the basis of metrics and availability. Each static route has its own Static Rtes profile.

The Ethernet > Mod Config profile specifies a static connected route, which states, in effect, "to reach system X, send packets out this interface to system X." Connected routes are low-cost, because no remote connection is involved.

Each IP-routing Connection profile specifies a static route that states, in effect, "to reach system X, send packets out this interface to system Y," where system Y is another router.

Dynamic routes

A dynamic route is a path, to another network, that is learned from another IP router rather than configured in one of the MAX unit's local profiles. A router that uses RIP broadcasts its entire routing table every 30 seconds, updating other routers about the usability of particular routes. Hosts that run ICMP can also send ICMP Redirects to offer a better path to a destination network. OSPF routers propagate link-state changes as they occur. Routing protocols such as RIP and OSPF all use some mechanism to propagate routing information and changes through the routing environment.

Route preferences and metrics

The MAX supports route preferences, because different protocols have different criteria for assigning route metrics. For example, RIP is a distance-vector protocol, which uses a virtual hop count to select the shortest route to a destination network. OSPF is a link-state protocol, which means that OSPF can take into account a variety of link conditions, such as the reliability or speed of the link, when determining the best path to a destination network.

When choosing a route to put into the routing table, the router first compares preference values, preferring the lowest number. If the preference values are equal, the router compares the metric fields and uses the route with the lowest metric. Following are the preference values for the various types of routes:

Route	**Default preference**
Connected	0
OSPF	10
ICMP	30
RIP	100
Static	100
ATMP, PPTP	100

Note: You can configure the DownMetric and DownPreference parameters to assign different metrics and preferences, respectively, to routes on the basis of whether the routes are in use or are down. You can direct the MAX to use active routes, if available, rather than routes that are down.

MAX IP interfaces

The MAX supports routing on Ethernet and WAN interfaces. It can function as either a system- or interface-based router. Interface-based routing uses numbered IP interfaces.

Ethernet interfaces

The following example shows the routing table for a MAX configured to enable IP routing:

```
** Ascend MAX Terminal Server **

ascend% iproute show

Destination        Gateway   IF      Flg   Pref   Met    Use    Age
10.10.0.0/16       -         ie0     C        0     0      3    222
10.10.10.2/32      -         local   CP       0     0      0    222
127.0.0.0/8        -         bh0     CP       0     0      0    222
127.0.0.1/32       -         local   CP       0     0      0    222
127.0.0.2/32       -         rj0     CP       0     0      0    222
224.0.0.0/4        -         mcast   CP       0     0      0    222
224.0.0.1/32       -         local   CP       0     0      0    222
224.0.0.2/32       -         local   CP       0     0      0    222
224.0.0.5/32       -         local   CP       0     0      0    222
224.0.0.6/32       -         local   CP       0     0      0    222
224.0.0.9/32       -         local   CP       0     0      0    222
255.255.255.255/32 -         ie0     CP       0     0      0    222
```

In this example, the Ethernet interface has the IP address 10.10.10.2 (with a subnet mask of 255.255.0.0). No Connection profiles or static routes are configured. At startup, the MAX creates the following interfaces:

Interface	Description
Ethernet IP	Always active, because it is always connected. You assign its IP address in Ethernet > Mod Config > Ether Options. The MAX creates two routing table entries: one with a destination of the network (`ie0`), and the other with a destination of the MAX (`local`).
Black-hole (`bh0`)	Always up. The black-hole address is 127.0.0.0. Packets routed to this interface are discarded silently.
Loopback (`local`)	Always up. The loopback address is 127.0.0.1/32.
Reject (`rj0`)	Always up. The reject address is 127.0.0.2. Packets routed to this interface are sent back to the source address with an ICMP *host unreachable* message.
Multicast	Have a destination address with a value of 224 for the first octet. (For information about multicast addresses, see Chapter 12, “Setting Up IP Multicast Forwarding.”)
Not shown in the example	Inactive `wanidle0`. when you configure a Connection profile. Created by the MAX when WAN connections are down, all routes point to the inactive interface.

WAN IP interfaces

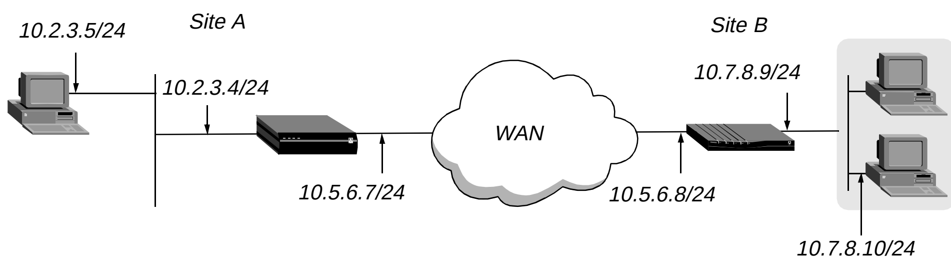
The MAX creates WAN interfaces as they are brought up. WAN interfaces are labeled wan*N*, where *N* is a number assigned in the order in which the interfaces become active. The WAN IP address can be a local address assigned dynamically when the caller logs in, an address on a subnet of the local network, or a unique IP network address for a remote device.

Numbered interfaces

The MAX can operate as both a system-based and an interface-based router. Interface-based routing uses numbered interfaces. Some routers or applications require numbered interfaces. Also, some sites use them for trouble-shooting leased point-to-point connections and forcing routing decisions between two links going to the same final destination. More generally, interface-based routing enables the MAX to operate in much the same way as a multihomed Internet host.

Figure 10-3 shows an example of an interface-based routing connection.

Figure 10-3. Interface-based routing example



At Site A, The MAX assigns IP addresses 10.5.6.7 and 10.5.6.8 to the WAN interfaces. The MAX route and uses these interface addresses to route packets to the remote network 10.7.8.0.

With system-based routing, the MAX does not assign interface addresses. It routes packets to the remote network through the WAN interface it created when the connection was brought up.

Interface-based routing requires that, in addition to the systemwide IP configuration, the MAX and the far end of the link have link-specific IP addresses, for which you specify the following parameters:

- Connections > IP Options > IF Adrs (the link-specific address for the MAX)
- Connections > IP Options > WAN Alias (the far end link-specific address)

Or, you can omit the remote side's system-based IP address from the Connection profile and use interface-based routing exclusively. This is an appropriate mechanism if, for example, the remote system is on a backbone net that can be periodically reconfigured by its administrators, and you want to refer to the remote system only by its mutually agreed-upon interface address. In this case, the following parameters specify the link-specific IP addresses:

- Connections > IP Options > IF Adrs (the near-end numbered interface)
- Connections > IP Options > LAN Adrs (the far-end numbered interface)

Note that the IP Adrs parameter, so if the only known address is the interface address, you must place it in the IP Adrs parameter rather than the WAN Alias parameter. In this case, the MAX creates a host route to the interface address (IP Adrs) and a net route to the subnet of the remote interface, and incoming calls must report their IP Addresses as the value of the IP Adrs parameter.

It is also possible, although not recommended, to specify the local numbered interface (Interface Address) and use the far end device's systemwide IP address (IP Adrs). In this case, the remote interface must have an address on the same subnet as the local, numbered interface.

If a MAX uses a numbered interface, note the following differences and similarities in operation as compared to unnumbered (system-based) routing:

- IP packets generated in the MAX and sent to the remote address have an IP source address corresponding to the numbered interface, not the systemwide (Ethernet) address.
- The MAX adds all numbered interfaces to its routing table as host routes.
- The MAX accepts IP packets addressed to a numbered interface, considering them to be destined for the MAX itself. (The packet can actually arrive over any interface, and the numbered interface corresponding to the packet's destination address need not be active.)

Configuring the local IP network setup

The Ethernet profile consists of system-global parameters that affect all IP interfaces in the MAX. Following are the related parameters (shown with sample settings):

```
Ethernet
   Mod Config
      Ether options…
         IP Adrs=10.2.3.1/24
         2nd Adrs=0.0.0.0/0
         RIP=Off
         Ignore Def Rt=Yes
         Proxy Mode=Off
      WAN options...
         Pool#1 start=100.1.2.3
         Pool#1 count=128
         Pool#1 name=Engineering Dept.
         Pool#2 start=0.0.0.0
         Pool#2 count=0
         Pool#2 name=
         Pool#3 start=10.2.3.4
         Pool#3 count=254
         Pool#3 name=Marketing Dept.
         Pool#4 start=0.0.0.0
         Pool#4 count=0
         Pool#4 name=
         Pool#5 start=0.0.0.0
         Pool#5 count=0
         Pool#5 name=
         Pool#6 start=0.0.0.0
         Pool#6 count=0
         Pool#6 name=
```

```
   Pool#7 start=0.0.0.0
   Pool#7 count=0
   Pool#7 name=
   Pool#8 start=0.0.0.0
   Pool#8 count=0
   Pool#8 name=
   Pool#9 start=0.0.0.0
   Pool#9 count=0
   Pool#9 name=
   Pool#A start=0.0.0.0
   Pool#A count=0
   Pool#A name=
   Pool only=No
   Pool Summary=No

Shared Prof=No
Telnet PW=Ascend

BOOTP Relay...
   BOOTP Relay Enable=No
   Server=N/A
   Server=N/A

DNS...
   Domain Name=abc.com
   Sec Domain Name=
   Pri DNS=10.65.212.10
   Sec DNS=12.20 7.23.51
   Allow As Client DNS=Yes
   Pri WINS=0.0.0.0
   Sec WINS=0.0.0.0
   List Attempt=No
   List Size=N/A
   Client Pri DNS=0.0.0.0
   Client Sec DNS=0.0.0.0

SNTP Server...
   SNTP Enabled=Yes
   Time zone-UTC+0000
   SNTP host#1=0.0.0.0
   SNTP host#2=0.0.0.0
   SNTP host#3=0.0.0.0

UDP Cksum=No
Adv Dialout Routes=Always
```

Understanding the IP network parameters

This section provides some background information about the IP network configuration. For detailed information about each parameter, see the *MAX Reference Guide*.

Primary IP address for each Ethernet interface

The IP Adrs parameter specifies the MAX unit's IP address for each local Ethernet interface. When specifying the IP addresses for a MAX Ethernet interface, you must specify the subnet mask. IP address and subnet mask are required settings for the MAX to operate as an IP router.

Second IP address for each Ethernet interface

The MAX can assign two unique IP addresses to *each* physical Ethernet port and route between them. This feature, referred to as *dual IP*, can give the MAX a logical interface on each of two networks or subnets on the same backbone.

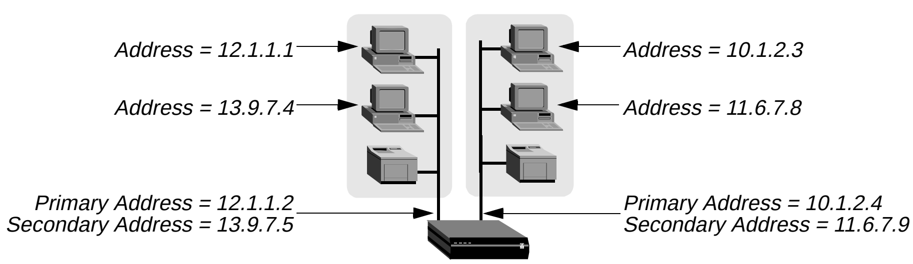
Usually, devices connected to the same physical wire all belong to the same IP network. With dual IP, a single wire can support two separate IP networks, with devices on the wire assigned to one network or the other and communicating by routing through the MAX.

Dual IP is also used to distribute the routing of traffic to a large subnet, by assigning IP addresses on that subnet to two or more routers on the backbone. When a router has a direct connection to the subnet as well as to the backbone network, it routes packets to the subnet and includes the route in its routing table updates.

Dual IP also enables you to make a smooth transition when changing IP addresses. That is, a second IP address can act as a placeholder while you are making the transition in other network equipment.

Figure 10-4 shows two IP addresses assigned to each of the MAX unit's Ethernet interfaces. 10.1.2.4 and 11.6.7.9 are assigned to one interface, and 1. 12.1.1.2 and 13.9.7.5 are assigned to the other. In this example, the MAX routes between all displayed networks. For example, the host assigned 12.1.1.1 can communicate with the host assigned 13.9.7.4, the host assigned 10.1.2.3 and the host assigned 11.6.7.8. The host assigned 12.1.1.1 and the host assigned 13.9.7.4 share a physical cable segment, but cannot communicate unless the MAX routes between the 12.0.0.0 network and the 13.0.0.0 network.

Figure 10-4. Sample dual IP network



Enabling RIP on the Ethernet interface

You can configure each IP interface to send RIP updates (inform other local routers of its routes), receive RIP updates (learn about networks that can be reached through other routers on the Ethernet), or both.

Note: Ascend recommends that you run RIP version 2 (RIP-v2) if possible. You should not run RIP-v2 and RIP-v1 on the same network in such a way that the routers receive each other's advertisements. RIP-v1 does not propagate subnet mask information, and the default-class network mask is assumed, while RIP-v2 handles subnet masks explicitly. Running the two versions on the same network can result in RIP-v1 class subnet mask assumptions overriding accurate subnet information obtained via RIP-v2.

Ignoring the default route

You can configure the MAX to ignore default routes advertised by routing protocols. This configuration is recommended, because you typically do not want the default route changed by a RIP update. The default route specifies a static route to another IP router, which is often a local router such as an Ascend GRF400 or other kind of LAN router. When you configure the MAX to ignore the default route, RIP updates do not modify the default route in the MAX routing table.

Proxy ARP and inverse ARP

You can configure the MAX to respond to an ARP request with its own MAC address. Typically, you enable Proxy ARP when the MAX supplies IP addresses dynamically to dial-in users and both of the following conditions exist:

- The MAX-supplied IP addresses are in the same local subnet as the MAX.
- Hosts on the local subnet must send packets to the dial-in clients.

Normally, you should not need to enable Proxy ARP, because most routing protocols (including those used over the Internet) are designed to propagate subnet mask information.

The MAX also supports Inverse Address Resolution Protocol (Inverse ARP). Inverse ARP enables the MAX to resolve the protocol address of another device when the hardware address is known. The MAX does not issue any Inverse ARP requests, but it does respond to Inverse ARP requests that have the protocol type of IP (8000 hexadecimal), or in which the hardware address type is the two-byte Q.922 address (Frame Relay). All other types are discarded. The Inverse ARP response packet sent by the MAX includes the following information:

- ARP source-protocol address (the MAX unit's IP address on Ethernet)
- ARP source-hardware address (the Q.922 address of the local DLCI)

(For the details about Inverse ARP, see RFCs 1293 and 1490.)

Specifying address pools

You can define up to ten address pools in the Ethernet profile, with each pool supporting up to 254 addresses. The Pool#*N* Start parameter specifies the first address in a block of contiguous addresses on the local network or subnet. The Pool#*N* Count parameter specifies how many addresses are in the pool (up to 254). Addresses in a pool do not accept a submask, because they are advertised as host routes. If you allocate IP addresses on a separate IP network or subnet, make sure you inform other IP routers about the route to that network or subnet, either by statically configuring those routes or configuring the MAX to dynamically send updates.

Forcing callers configured for a pool address to accept dynamic assignment

During PPP negotiation, a caller can reject the IP address offered by the MAX and present its own IP address for consideration. Connection profiles compare IP addresses as part of authentication, so the MAX would automatically reject such a request if the caller has a Connection profile. However, Name-Password profiles have no such authentication mechanism, and could potentially enable a caller to spoof a local address. The Pool Only parameter can instruct the MAX to hang up if a caller rejects the dynamic assignment.

Summarizing host routes in routing table advertisements

IP addresses assigned dynamically from a pool are added to the routing table as individual host routes. You can summarize this network (the entire pool), cutting down significantly on route flappage and the size of routing table advertisements.

The Pool Summary setting enables or disables route summarization, which summarizes a series of host routes into a network route advertisement. The MAX routes packets destined for a valid host address on the summarized network to the host, and the MAX rejects packets destined for an invalid host address with an ICMP *host unreachable* message.

To use the pool summary feature, create a network-aligned pool and set the Pool Summary parameter to Yes. To be network-aligned, the Pool #*N* Start address must be the first host address. Subtract one from the Pool #*N* Start address to determine the network address (the zero address on the subnet). Since the first and last address of a subnet are reserved, you must set Pool #*N* Count to a value that is two less than a power of two. For example, you can use values 2, 6, 14, 30, 62, 126 or 254. The subnet mask includes a value that is two greater than Pool #*N* Count. For example, with the following configuration:

```
Pool Summary=Yes
Pool#1 Start=10.12.253.1
Pool#1 Count=126
```

the network alignment address is (Pool Start #1 –1) 10.12.253.0 and the subnet mask is (Pool #1 Count +2 addresses) 255.255.255.128. The resulting address-pool network is:

10.12.253.0/25

For a sample configuration that shows route summarization, see “Configuring DNS” on page 10-16.

Sharing Connection profiles

The Shared Prof parameter specifies whether the MAX allows more than one incoming call to share the same Connection profile. This feature relates to IP routing because the sharing of profiles must result in two IP addresses reached through the same profile.

In low-security situations, more than one dial-in user can share a name and password for accessing the local network. This would require sharing a single Connection profile that specifies bridging only, or dynamic IP address assignment. Each call would be a separate connection. The name and password would be shared, and a separate IP address would be assigned dynamically to each caller.

If a shared profile uses an IP address, it must be assigned dynamically, because multiple hosts cannot share a single IP address.

Suppressing host route advertisements

The MAX creates host routes for Dial-in sessions and advertises them back to the backbone. Dial-in sessions can cause excessive routing updates and, consequently, network delays. You can set the Suppress Hosts Routes parameter to reduce the routing updates caused by dial-in sessions.

Telnet password

The Telnet password is required from all users attempting to access the MAX unit by Telnet. Users are allowed three tries to enter the correct password. If all three are unsuccessful, the connection attempt fails.

BOOTP Relay

By default, a MAX does not relay Bootstrap Protocol (BOOTP) requests to other networks. It can do so if you set Boot Relay Enable to Yes, but you must disable SLIP BOOTP in Ethernet > Mod Config > TServ Options. SLIP BOOTP makes it possible for a computer connecting to the MAX over a SLIP connection to use the Bootstrap Protocol. A MAX supports BOOTP on only one connection. If you enable both SLIP BOOTP and BOOTP relay, you receive an error message.

You can specify the IP address of one or two BOOTP servers but you are not required to specify a second BOOTP server.

If you specify two BOOTP servers, the MAX that relays the BOOTP request determines when to use each server. The order of the BOOTP servers in the BOOTP Relay menu does not necessarily determine which server the MAX tries first.

Local domain name

Use the Domain Name for DNS lookups. When you give the MAX a hostname to look up, it tries various combinations, including the appending of the configured domain name to the hostname. The secondary domain name (Sec Domain Name) can specify another domain that the MAX can search. The MAX searches the secondary domain only after the domain specified by the Domain Name parameter.

DNS or WINS name servers

When the MAX is informed about DNS (or WINS), Telnet and Rlogin users can specify hostnames instead of IP addresses. If you configure a primary and secondary name server, the secondary server is accessed only if the primary one is inaccessible.

DNS lists

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. To avoid tearing down physical links when a host is unavailable, you can set the List Attempt parameter to Yes. The List Size parameter specifies the maximum number of hosts listed (up to 35).

Client DNS

Client DNS configurations define DNS server addresses that will be presented to WAN connections during IPCP negotiation. They provide a way to protect your local DNS information from WAN users. Client DNS has two levels: a global configuration that applies to all PPP connections (defined in the Ethernet profile), and a connection-specific configuration that applies only to the WAN connection defined in the Connection profile. The global client addresses are used only if none are specified in the Connection profile.

SNTP service

The MAX can use Simple Network Time Protocol (SNTP)—RFC 1305) to set and maintain its system time by communicating with an SNTP server. SNTP must be enabled for the MAX to use it to communicate with the server. In addition, you must specify your time zone as an offset from Universal Time Coordinated (UTC). UTC is the same as Greenwich Mean Time (GMT). Specify the offset in hours, using a 24-hour clock. Because some time zones, such as Newfoundland, do not have an even hour boundary, the offset includes four digits and is stated in half-hour increments. For example, in Newfoundland the time is 1.5 hours behind UTC and is represented as follows:

```
UTC -0130
```

For San Francisco, which is 8 hours behind UTC, the time would be:

```
UTC -0800
```

For Frankfurt, which is 1 hour ahead of UTC, the time would be:

```
UTC +0100
```

Specifying SNTP server addresses

The Host parameter lets you specify up to three server addresses. The MAX polls the configured SNTP server at 50-second intervals. The MAX sends SNTP requests to the first address. It sends requests to the second only if the first is inaccessible, and to the third only if the second is inaccessible.

UDP checksums

If data integrity is of the highest concern for your network, and having redundant checks is important, you can turn on UDP checksums to generate a checksum whenever a UDP packet is transmitted. UDP packets are transmitted for queries and responses related to ATMP, SYSLOG, DNS, ECHOSERV, RADIUS, TACACS, RIP, SNTP, and TFTP.

Setting UDP checksums to Yes could cause a slight decrease in performance, but in most environments the decrease is not noticeable.

Poisoning dialout routes in a redundant configuration

If you have another Ascend unit backing up the MAX in a redundant configuration on the same network, you can set the Adv Dialout Routes parameter to instruct the MAX to stop advertising IP routes that use dial services if its trunks experience an alarm condition. Unless you specify otherwise, the MAX continues to advertise its dialout routes, which prevents the redundant unit from taking over the routing responsibility.

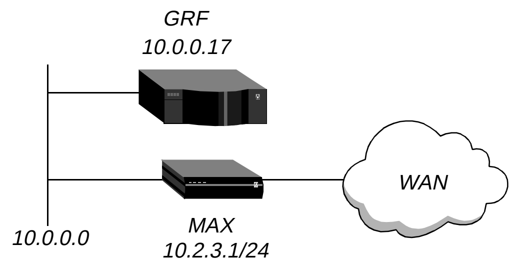
Examples of IP network configuration

This section shows some examples of Ethernet profile IP configuration. One of the examples, "Configuring DNS" on page 10-16 shows an Ethernet profile, Route profile, and Connection profile configuration that work together.

Configuring the MAX IP interface on a subnet

On a large corporate backbone, many sites configure subnets to increase the network address space, segment a complex network, and control routing in the local environment. For example, Figure 10-5 shows the main backbone IP network (10.0.0.0) supporting an Ascend GRF router (10.0.0.17).

Figure 10-5. Creating a subnet for the MAX



You can place the MAX on a subnet of that network by entering a subnet mask in its IP address specification. For example:

1. Open Ethernet > Mod Config > Ether Options.
2. Specify the IP subnet address for the MAX on Ethernet. For example:

```
Ethernet
   Mod Config
      Ether options…
         IP Adrs=10.2.3.1/24
```

3. Configure the MAX to receive RIP updates from the local GRF router:

```
         RIP=Recv=v2
```

4. Close the Ethernet profile.

With this subnet address, the MAX requires a static route to the backbone router on the main network. Otherwise, it can only communicate with devices on the subnets to which it is directly connected. To create the static route and make the backbone router the default route:

1. Open the Default IP Route profile.
2. Specify the IP address of a backbone router in the Gateway parameter. For example:

```
Ethernet
   Static Rtes
      Name=Default
      Active=Yes
      Dest=0.0.0.0/0
      Gateway=10.0.0.17
      Preference=100
      Metric=1
      DownPreference=140
      DownMetric=7
      Private=Yes
```

3. Close the Default IP Route profile.

For more information about IP Route profiles, see “Configuring IP routes and preferences” on page 10-35. To verify that the MAX is up on the local network, invoke the terminal-server interface and Ping a local IP address or hostname. For example:

```
ascend% ping 10.1.2.3
```

You can terminate the Ping exchange at any time by pressing Ctrl-C.

Configuring DNS

The DNS configuration enables the MAX to use local DNS or WINS servers for lookups. In this example of a DNS configuration, client DNS is not in use. Note that you can protect your DNS servers from callers by defining connection-specific (*client*) DNS servers and specifying that Connection profiles use those client servers. To configure the local DNS service:

1. Open Ethernet > Mod Config > DNS.
2. Specify the local domain name.
3. If appropriate, specify a secondary domain name.

4 Specify the IP addresses of a primary and secondary DNS server, and turn on the DNS list attempt feature:

```
Ethernet
   Mod Config
      DNS...
         Domain Name=abc.com
         Sec Domain Name=
         Pri DNS=10.65.212.10
         Sec DNS=12.20 7.23.51
         Allow As Client DNS=Yes
         Pri WINS=0.0.0.0
         Sec WINS=0.0.0.0
         List Attempt=Yes
         List Size=35
         Client Pri DNS=0.0.0.0
         Client Sec DNS=0.0.0.0
         Enable Local DNS Table=No
         Loc.DNSTab Auto Update=No
```

5 Close the Ethernet profile.

You can create a local DNS table to provide a list of IP addresses for a specific hostname when the remote DNS server fails to resolve the host name. If the local DNS table contains the host name for the attempted connection, it provides the list of IP addresses.

You create the DNS table from the terminal server by entering the hostnames and their IP addresses. A table can contain up to eight entries, with a maximum of 35 IP addresses for each entry. If you specify automatic updating, you only have to enter the first IP address of each host. Any others are added automatically.

Automatic updating replaces the existing address list for a host each time the remote DNS server succeeds in resolving a connection to a host that is in the table. You specify how many of the addresses returned by the remote server can be included in the new list.

On the MAX, the table provides additional information for each table entry. The information is in the following two fields, which the MAX updates when the system matches the table entry with a hostname not found by the remote server:

- # Reads— The number of reads since the MAX created the entry. The MAX updates this field each time it finds a local name query match in the local DNS table.
- Time of Last Read

You can check the list of hostnames and IP addresses in the table by entering the terminal-server command Show DNStab. Figure 10-6 shows an example of a DNS table on a MAX. Other terminal-server commands show individual entries, with a list of IP addresses for the entry.

Figure 10-6. Local DNS table example

```
Local DNS Table
Name                      IP Address      # Reads Time of last read
_________________________ _______________ _______ __________________
1: ""                     ------          ------
2: "server.corp.com."     200.0.0.0       2       Feb 10 10:40:44
3: "boomerang"            221.0.0.0       2       Feb 10  9:13:33
4: ""                     ------          -------
5: ""                     ------          -------
6  ""                     ------          -------
7: ""                     ------          -------
```

Additional terminal-server commands

The terminal-server interface includes Show and DNStab commands have been added to help you view, edit, or and add entries to the DNS table.

Show commands

- `Show ?` displays a list that includes DNStab help.
- `Show dnstab` displays the local DNS table.
- `Show dnstab ?` displays help for the DNStab editor.
- `Show dnstab` entry displays the local DNS table entry (all IP addresses in the list)

`DNStab` commands

The terminal server DNStab command has the following variations:

DNStab command	Description
DNStab	Displays help information about the DNS table.
DNStab Show	Displays the local DNS table.
DNStab Entry *N*	Displays a list for entry *N* in the local DNS table. The list displayed includes the entry and all the IP addresses stored for that entry up to a maximum number of entries specified in the List Size parameter. If List Attempt=No, no list is displayed.
DNStab Edit	Start editor for the local DNS table.

Configuring the local DNS table

To enable and configure the local DNS table:

1 Display Ethernet > Mod Config > DNS menu.

2 Select a setting for the List Attempt parameter.

3 Specify the list size by setting the List Size parameter.

4 Select Enable Local DNS Table=Yes.
The default is No.

5 Select a setting for the Loc.DNS Tab Auto Update parameter.

Criteria for valid names in the local DNS table

Each name in the local DNS table:

- Must be unique in the table.
- Must start with an alphabetic character, which can be either uppercase or lowercase.
- Must be less than 256 characters
- Can be a local name or a fully qualified name that includes the domain name.

Periods at the ends of names are ignored.

Entering IP addresses in the local DNS table

To enter IP addresses in a local DNS table, you use the DNS table editor from the terminal server. While the editor is in use, the system cannot look up addresses in the table or perform automatic updates. A table *entry* is one of the eight table indexes. It includes the hostname, IP address (or addresses), and information fields. To place the initial entries in the table:

1 At the terminal-server interface, type **`dnstab edit`**.
Before you make any entries, the table is empty. The editor initially displays zeros for each of the eight entries in the table. To exit the table editor without making an entry, press Enter.

2 Type an entry number and press Enter.
A warning appears if you type an invalid entry number. If the entry exists, the current name for that entry appears in the prompt.

3 Type the name for the current entry.
If the system accepts the name, it places the name in the table and prompts you for the IP address for the name that you just entered. (For the characteristics of a valid name, see “Criteria for valid names in the local DNS table” on page 10-19.)
If you enter an invalid name, the system prompts you to enter a valid name.

4 Type the IP address for the entry.
If you enter an address in the wrong format, the system prompts you for the correct format. If your format is correct, the system places the address in the table and the editor prompts you for the next entry.

5 When you are finished making entries, type the letter **`O`** and press Enter when the editor prompts you for another entry.

Editing the local DNS table

To edit the DNS table entries, you access the DNS table editor from the terminal server. While the editor is in use, the system cannot look up addresses in the table or perform automatic updates. A table *entry* is one of the eight table indexes. It includes the host name, IP address (or addresses), and information fields. To edit one or more entries in the local DNS table:

1 At the terminal-server interface, type **`dnstab edit`**

If the table has already been created, the number of the entry last edited appears in the prompt.

2 Type an entry number, or press Enter to edit the entry number currently displayed.

A warning appears if you type an invalid entry number. If the entry exists, the current value for that entry appears in the prompt.

3 Replace, accept, or clear the displayed name, as follows:

– To replace the name, type a new name and press Enter.

– To accept the current name, press Enter.

– To clear the name, press the spacebar, then press Enter.

If you enter a valid name, the system places it in the table (or leaves it there if you accept the current name) and prompts you for the corresponding IP address. (For the characteristics of a valid name, see "Criteria for valid names in the local DNS table" on page 10-19.)

If you clear an entry name, all information in all fields for that entry is discarded.

4 Either type a new IP address and press Enter, or leave the current address and just press Enter.

– To change the IP address, type the new IP address.

– If you are changing the name of the entry but not the IP address, just press Enter.

If the address is in the correct format, the system places it in the table and prompts you for another entry.

5 When you are finished making entries, type the letter **`O`** and press Enter when the editor prompts you for another entry.

Deleting an entry from the local DNS table

To delete an entry from the local DNS table:

1 At the terminal-server interface, type **`dnstab edit`** to display the table.

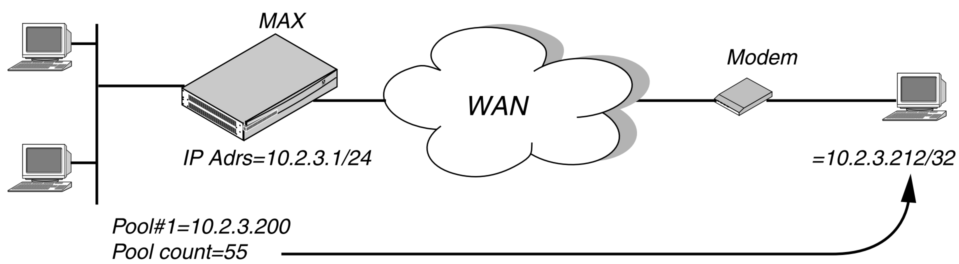
2 Type the number of the entry you want to delete and press Enter.

3 Press the spacebar, then press Enter.

Setting up address pools with route summarization

The address pool parameters enable the MAX to assign an IP address to incoming calls that are configured for dynamic assignment. These addresses are assigned on a first-come, first-served basis. After the MAX terminates a connection, its address is freed up and returned to the pool for reassignment to another connection. Figure 10-7 shows a host using PPP dial-in software to connect to the MAX.

Figure 10-7. Address assigned dynamically from a pool



This example shows how to set up network-aligned address pools and use route summarization. It also shows how to enter a static route for the pool subnet and make the Connection profile route private, both of which are requirements when using route summarization.

Following are the rules for network-aligned address pools:

- The Pool Start address must be the first host address.

  Subtract one from the Pool #*N* Start address for the base address for the subnet.
- The Pool #*N* Count value must be two less than the total number of addresses in the pool.

  Add two to Pool #*N* Count for the total number of addresses in the subnet, and calculate the netmask for the subnet the basis of this total.

For example, the following configuration is network aligned:

```
Ethernet
   Mod Config
      WAN options...
         Pool#1 start=10.12.253.1
         Pool#1 count=62
         Pool#1 name=Engineering Dept.
         Pool Summary=Yes
```

Pool #1 Start is set to 10.12.253.1. When you subtract one from this address, you get 10.12.253.0, which is a valid base address for a subnet defined by a mask of 255.255.255.192. Note that 10.12.253.64, 10.12.253.128, and 10.12.253.192 are also valid zero addresses for the same mask. The resulting address pool subnet is 10.12.253.0/26.

Pool #1 Count is set to 62. When you add two to the Pool #1 Count, you get 64. The subnet mask for 64 addresses is 255.255.255.192 (256–64 = 192). The Ascend subnet notation for a 255.255.255.192 mask is /26.

After verifying that *every one* of the configured address pools is network-aligned, you must enter a static route for each of them. These static routes handle all IP address that have not been given to users by routing them to the reject interface or the black-hole interface. (See “MAX IP interfaces” on page 10-6).

Note: The MAX creates a host route for every address assigned from the pools, and host routes override subnet routes. Therefore, packets whose destination matches an assigned IP address from the pool are properly routed and not discarded or bounced. Because the MAX advertises the entire pool as a route, and only privately knows which IP addresses in the pool are active, a remote network can improperly send the MAX a packet for an inactive IP address. Depending on the static-route specification, these packets are either bounced with an ICMP *host unreachable* message or silently discarded.

For example, the following static route specifies the black-hole interface, so it silently discards all packets whose destination falls in the pool's subnet. In addition to the Dest and Gateway parameters that define the pool, be sure you have set the Metric, Preference, Cost, and Private parameters as shown.

```
Ethernet
   Static Rtes
      Name=pool-net
      Active=Yes
      Dest=10.12.253.0/26
      Gateway=127.0.0.0
      Preference=0
      Metric=0
      Cost=0
      Private=No
```

The routing table contains the following lines:

```
Destination         Gateway    IF      Flg       Pref   Met     Use    Age
10.12.253.0/26         -          bh0    C          0      0       0   172162
127.0.0.0/32           -          bh0    CP         0      0       0   172163
127.0.0.1/32           -          lo0    CP         0      0       0   172163
127.0.0.2/32           -          rj0    CP         0      0       0   172163
```

When you configure Connection profiles that assign IP addresses from the pool, make sure you set the Private parameter to Yes. For example:

```
Ethernet
   Connections
      Ip options...
         LAN Adrs=0.0.0.0/0
         WAN Alias=0.0.0.0
         IF Adrs=0.0.0.0/0
         Preference=100
         Cost=0
         Private=Yes
         RIP=Off
         Pool=1
```

Configuring IP routing connections

When you enable IP routing and addresses are specified in a Connection profile, you define an IP WAN interface. Following are the related parameters (shown with sample settings):

```
Ethernet
   Answer
      Assign Adrs=Yes
      PPP options...
         Route IP=Yes

      Session options...
         RIP=Off

Ethernet
   Connections
      Station=remote-device

      Route IP=Yes
      IP options...
         LAN Adrs=0.0.0.0/0
         WAN Alias=0.0.0.0/0
         IF Adrs=0.0.0.0/0
         Preference=100
         Metric=7
         DownPreference=120
         DownMetric=9
         Private=No
         RIP=Off
         Pool=0

      Session options...
         IP Direct=0.0.0.0
```

Understanding the IP routing connection parameters

This section provides some background information about enabling IP routing in the Answer profile and Connection profiles. For detailed information about each parameter, see the *MAX Reference Guide.*

Assign Adrs

In the Answer profile, the Assign Adrs parameter must be set to Yes, to enable the MAX to allocate IP addresses dynamically from a pool of designated addresses on the local network. The caller's PPP software must be configured to accept an address dynamically. If the Pool Only parameter is set to Yes in the Ethernet profile, the MAX terminates connections that reject the assigned address during PPP negotiation. For related information, see "Configuring dynamic address assignment to a dial-in host" on page 10-27.

Route IP

Set Route IP in Answer > PPP Options to Yes to enable the MAX to negotiate a routing connection.

Enabling IP routing for a WAN interface

To enable IP packets to be routed for this connection, set the Route IP parameter to Yes in the Connection profile. When you enable IP routing, IP packets are always routed, they are never bridged.

Configuring the remote IP address

The LAN Adrs parameter specifies the IP address of the remote device. Before accepting a call from the far end, the MAX matches this address to the source IP address presented by the calling device. It can be one of the following values:

Value	How to specify
IP address of a router	If the remote device is an IP router, specify its address, including its subnet mask identifier. (For background information, see "IP addresses and subnet masks" on page 10-2.) If you omit the mask, the MAX inserts a default subnet mask that makes the entire far-end network accessible.
IP address of a dial-in host	If the remote device is a dial-in host running PPP software, specify its address, including a subnet mask identifier of /32 (for example, 10.2.3.4/32).
The null address (0.0.0.0)	If the remote device is a dial-in host that accepts dynamic address assignment, leave the LANS Adrs parameter blank.

Note: The most common cause of trouble in initially establishing an IP connection is incorrect configuration of the IP address or subnet specification for the remote host or calling device.

WAN Alias

A WAN alias is another IP address for the remote device, used for numbered-interface routing. The WAN alias will be listed in the routing table as a gateway (next hop) to the Lan Adrs value. The caller must use a numbered interface, and its interface address must agree with the WAN Alias setting.

Specifying a local IP interface address

The IF Adrs parameter specifies another local IP-interface address, to be used as the local numbered interface instead of Ethernet IP Adrs (the default).

Assigning metrics and preferences

Connection profiles often represent switched connections, which have an initial cost that you avoided if you use a nailed-up link to the same destination. To favor nailed-up links, you can assign a higher metric to switched connections than to any of the nailed-up links to the same destination.

Each connection represents a static route, which has a default preference of 100. (For other preferences, see “Route preferences and metrics” on page 10-5.) For each connection, you can fine-tune the route preference or assign a completely different preference.

Note: You can configure the DownMetric and DownPreference parameters to assign different metrics or preferences to routes on the basis of whether the route is in use or is down. You can direct the MAX to use active routes, if available, rather than choose routes that are down.

Private routes

The Private parameter specifies whether the MAX discloses the existence of the route when queried by RIP or another routing protocol. The MAX uses private routes internally. They are not advertised.

Assigning the IP address dynamically

The Pool parameter specifies an IP-address pool from which the MAX assigns the caller an IP address. If the Pool parameter is null but all other configuration settings enable dynamic assignment, the MAX gets IP addresses from the first defined address pool.

IP direct configuration

An IP Direct configuration bypasses routing and bridging tables for all incoming packets and sends each packet received to the specified IP address. All outgoing packets are treated as normal IP traffic. They are not affected by the IP Direct configuration.

Note: Typically, you configure IP Direct connections with RIP turned off. If you set the IP Direct configuration with RIP set to receive, the MAX forwards all RIP updates to the specified address. Typically, this is not desirable, because RIP updates are designed to be stored locally by the IP router (in this case, the MAX).

Configuring RIP on this interface

You can configure an IP interface to send RIP updates, receive RIP updates or both.

Ascend recommends that you run RIP version 2 (RIP-v2) if possible. Ascend does not recommend running RIP-v2 and RIP-v1 on the same network in such a way that the routers receive each other’s advertisements. RIP-v1 does not propagate subnet mask information, and the default class network mask is assumed, while RIP-v2 handles subnet masks explicitly. Running the two versions on the same network can result in RIP-v1 *guesses* overriding accurate subnet information obtained via RIP-v2.

Checking remote host requirements

IP hosts, such as UNIX systems, Windows or OS/2 PCs, or Macintosh systems, must have appropriately configured TCP/IP software. A remote host calling into the local IP network must also have PPP software.

UNIX software

UNIX systems typically include a TCP/IP stack, DNS software, and other software, files, and utilities used for Internet communication. UNIX network administration documentation describes how to configure these programs and files.

Window or OS/2 software

PCs running Windows or OS/2 need TCP/IP networking software. The software is included with Windows 95, but the user might need to purchase and install it separately if the computer has an earlier version of Windows, or OS/2.

Macintosh software

Macintosh computers need MacTCP or Open Transport software for TCP/IP connectivity. Apple system software versions 7.1 or later include MacTCP. To see if a Macintosh has the software, the user should open the Control Panels folder and look for MacTCP or MacTCP Admin.

Software configuration

For any platform, the TCP/IP software must be configured with the host's IP address and subnet mask. If the host obtains its IP address dynamically from the MAX, the TCP/IP software must be configured to enable dynamic allocation. If your local network supports a DNS server, you should also configure the host software with the DNS server's address.

Typically, the host software is configured with the MAX as its default router.

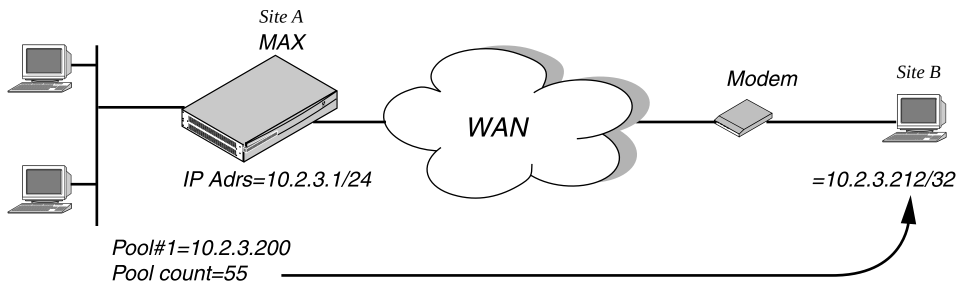
Examples of IP routing connections

This section provides sample Connection profile configurations for IP routing. The examples presume that you have configured the Ethernet profile correctly, as described in "Configuring the local IP network setup" on page 10-8.

Configuring dynamic address assignment to a dial-in host

In this example, the dial-in host is a PC that accepts an IP address assignment from the MAX dynamically. Figure 10-8 shows a sample network.

Figure 10-8. A dial-in user requiring dynamic IP address assignment



In this example, Site A is a backbone network and Site B is a single dial-in host with a modem, TCP/IP stack, and PPP software. The PPP software running on the PC at Site B must be configured to acquire its IP address dynamically. For example, the following a sample software configuration presumes that the PC has a modem connection to the MAX:

```
Username=victor
Accept Assigned IP=Yes
IP address=Dynamic (or Assigned or N/A)
Netmask=255.255.255.255 (or None or N/A)
Default Gateway=None or N/A
Name Server=10.2.3.55
Domain suffix=abc.com
Baud rate=38400
Hardware handshaking ON
VAN Jacobsen compression ON
```

To configure the MAX to accept dial-in connections from Site B and assign an IP address:

1 Open Ethernet > Mod Config > WAN Options.

2 Enter the start address of the pool and the number of contiguous addresses it includes. For example:

```
Ethernet
   Mod Config
      WAN options…
         Pool#1 start=10.12.253.1
         Pool#1 count=126
         Pool#1 name=Engineering Dept.
         Pool only=Yes
         Pool Summary=Yes
```

3 Open the Ether Options subprofile and turn on Proxy Mode:

```
      Ether options…
         Proxy Mode=Yes
```

4 Close the Ethernet profile.

5 Open the Answer profile and enable both dynamic address assignment and IP routing:

```
Ethernet
   Answer
      Assign Adrs=Yes
      PPP options…
         Route IP=Yes
```

6 Close the Answer profile.

7 Open a Connection profile for the dial-in user.

8 Specify the user's name, activate the profile, and set encapsulation options. For example:

```
Ethernet
   Connections
      Station=victor
      Active=Yes
      Encaps=PPP
      Encaps options...
         Send Auth=CHAP
         Recv PW=*SECURE*
```

9 Configure IP routing and address assignment:

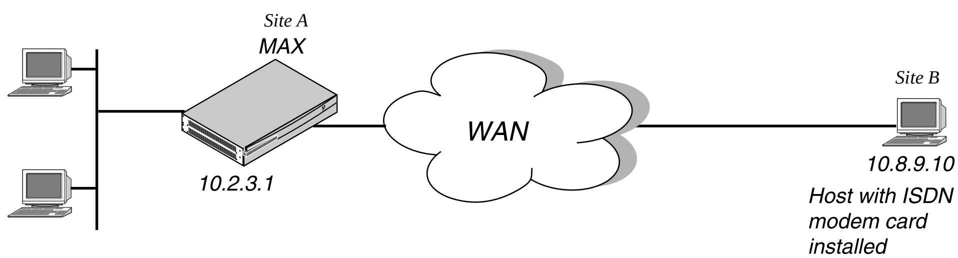
```
      Route IP=Yes
      IP options…
         LAN Adrs=0.0.0.0/0
         RIP=Off
         Pool=1
```

10 Close the Connection profile.

Configuring a host connection with a static address

A host connection with a static address enables the dial-in host to keep its own IP address when logging into the MAX IP network. For example, if a PC user telecommutes to one IP network and uses an ISP on another IP network, one of the connections can assign an IP address dynamically and the other can configure a host route to the PC. This example shows how to configure a host connection with a static address. For details about the /32 subnet mask, see "IP addresses and subnet masks" on page 10-2.)

Figure 10-9. A dial-in user requiring a static IP address (a host route)



In this example, the PC at Site B is running PPP software that includes settings like these:

```
Username=patti
Accept Assigned IP=N/A (or No)
IP address=10.8.9.10
Subnet mask=255.255.255.255
Default Gateway=N/A (or None)
Name Server=10.7.7.1
```

```
Domain suffix=abc.com
VAN Jacobsen compression ON
```

To configure the MAX to accept dial-in connections from Site B:

1 Open the Answer profile and enable IP routing:

```
Ethernet
   Answer
      PPP options…
         Route IP=Yes
```

2 Close the Answer profile.

3 Open a Connection profile for the dial-in user.

4 Specify the user's name, activate the profile, and set encapsulation options. For example:

```
Ethernet
   Connections
      Station=patti
      Active=Yes
      Encaps=PPP
      Encaps options...
         Send Auth=CHAP
         Recv PW=*SECURE*
```

5 Configure IP routing:

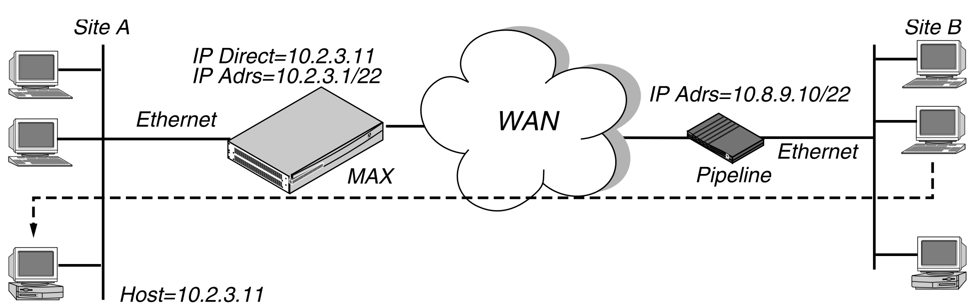
```
      Route IP=Yes
      IP options…
         LAN Adrs=10.8.9.10/32
         RIP=Off
```

6 Close the Connection profile.

Configuring an IP Direct connection

You can configure a Connection profile to automatically redirect incoming IP packets to a specified host on the local IP network without having the packets pass through the routing engine on the MAX as shown in Figure 10-10.

Figure 10-10. Directing incoming IP packets to one local host



Note: IP Direct connections typically turn off RIP. If the connection is configured to receive RIP, all RIP packets from the far side are kept locally and forwarded to the IP address you specify for IP Direct.

To configure an IP Direct connection:

1 Open the Answer profile and enable IP routing:

```
Ethernet
   Answer
      PPP options…
         Route IP=Yes
```

2 Close the Answer profile.

3 Open a Connection profile for the dial-in connection.

4 Specify the remote device's name, activate the profile, and set encapsulation options. For example:

```
Ethernet
   Connections
      Station=Pipeline1
      Active=Yes
      Encaps=MPP
      Encaps options...
         Send Auth=CHAP
         Recv PW=localpw
         Send PW=remotepw
```

5 Configure IP routing:

```
      Route IP=Yes
      IP options…
         LAN Adrs=10.8.9.10/22
         RIP=Off
```

6 Open the Session Options subprofile and specify the IP Direct host. For example:

```
      Session options…
         IP Direct=10.2.3.11
```

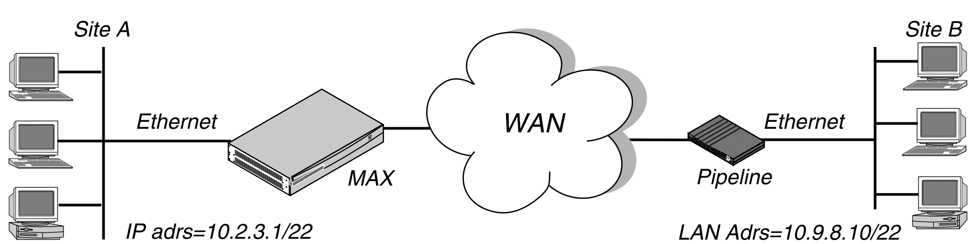
7 Close the Connection profile.

Note: The IP Direct address you specify in Connections > Session Options is the address to which the MAX directs all incoming packets on this connection. When you use the IP Direct feature, a user cannot Telnet directly to the MAX from the far side. The MAX directs all incoming IP traffic to the specified address on the local IP network.

Configuring a router-to-router connection

In this example, the MAX connects to a corporate IP network and needs a switched connection to another company that has its own IP configuration. Figure 10-11 shows the network diagram.

Figure 10-11. A router-to-router IP connection



This example assumes that the Answer profile in each of the two devices enable IP routing. To configure the Site A MAX for a connection to Site B:

1 Open a Connection profile for the Site B device.

2 Specify the remote device's name, activate the profile, and set encapsulation options. For example:

```
Ethernet
   Connections
      Station=PipelineB
      Active=Yes
      Encaps=MPP
      Encaps options...
         Send Auth=CHAP
         Recv PW=localpw
         Send PW=remotepw
```

3 Configure IP routing:

```
      Route IP=Yes
      IP options…
         LAN Adrs=10.9.8.10/22
         RIP=Off
```

4 Close the Connection profile.

To configure the Site B Pipeline:

5 Open the Connection profile for the Site A MAX.

6 Specify the Site A MAX unit's name, activate the profile, and set encapsulation options. For example:

```
Ethernet
   Connections
      Station=MAXA
      Active=Yes
      Encaps=MPP
      Encaps options...
         Send Auth=CHAP
         Recv PW=localpw
         Send PW=remotepw
```

7 Configure IP routing.

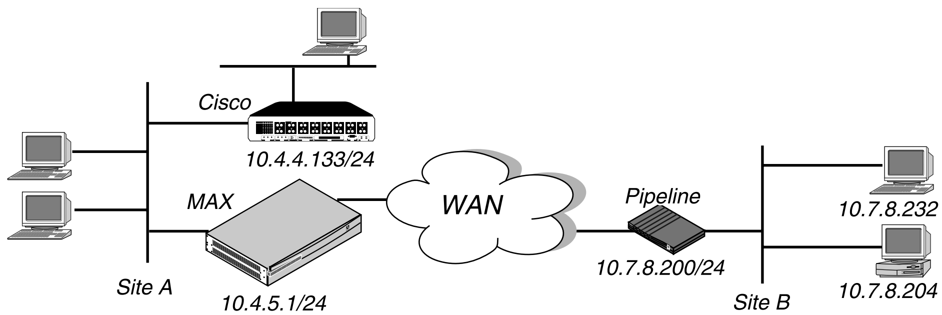
```
      Route IP=Yes
      IP options…
         LAN Adrs=10.2.3.1/22
         RIP=Off
```

8 Close the Connection profile.

Configuring a router-to-router connection on a subnet

In the sample network illustrated in Figure 10-12, the MAX connects telecommuters with their own Ethernet networks to the corporate backbone. The MAX is on a subnet, and assigns subnet addresses to the telecommuters' networks.

Figure 10-12. A connection between local and remote subnets



This example assumes that the Answer profile in each of the two devices enables IP routing. Because the MAX specifies a subnet mask as part of its own IP address, the MAX must use other routers to reach IP addresses outside that subnet. To forward packets to other parts of the corporate network, the MAX either must have a default route configuration to a router in its own subnet (for example the Cisco router in Figure 5-12) or must enable RIP on Ethernet.

To configure the MAX at Site A with an IP routing connection to Site B:

1 Open a Connection profile for the Site B device.

2 Specify the remote device's name, activate the profile, and set encapsulation options. For example:

```
Ethernet
   Connections
      Station=PipelineB
      Active=Yes
      Encaps=MPP
      Encaps options...
         Send Auth=CHAP
         Recv PW=localpw
         Send PW=remotepw
```

3 Configure IP routing:

```
      Route IP=Yes
      IP options…
         LAN Adrs=10.7.8.200/24
         RIP=Off
```

4 Close the Connection profile.

To specify the local Cisco router as the MAX unit's default route:

1 Open the Default IP Route profile.

2 Specify the Cisco router's address as the gateway address.

```
Ethernet
   Static Rtes
      Name=Default
```

```
        Active=Yes
        Dest=0.0.0/0
        Gateway=10.4.4.133
        Metric=1
        Preference=10
        Private=Yes
```

3 Close the IP Route profile.

To configure the Site B Pipeline unit for a connection to Site A:

4 Open the Connection profile in the Pipeline unit for the Site A MAX.

5 Specify the Site A MAX unit's name, activate the profile, and set encapsulation options. For example:

```
Ethernet
   Connections
      Station=MAXA
      Active=Yes
      Encaps=MPP
      Encaps options...
         Send Auth=CHAP
         Recv PW=localpw
         Send PW=remotepw
```

6 Configure IP routing:

```
      Route IP=Yes
      IP options…
         LAN Adrs=10.4.5.1/24
         RIP=Off
```

To make the MAX the default route for the Site B Pipeline unit:

1 Open the Default IP Route profile in the Site B Pipeline.

2 Specify the MAX unit at the far end of the WAN connection as the gateway address:

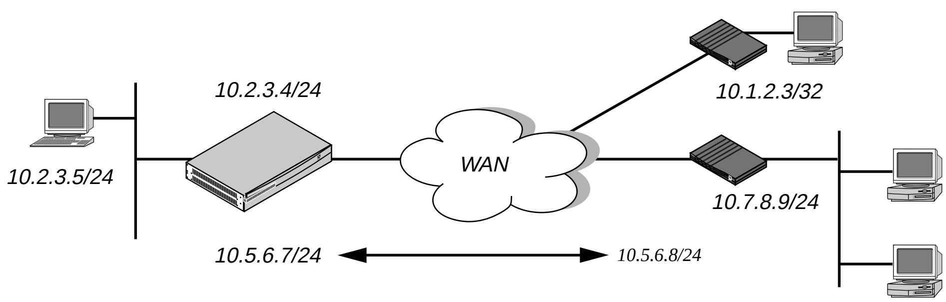
```
Ethernet
   Static Rtes
      Name=Default
      Active=Yes
      Dest=0.0.0/0
      Gateway=10.4.5.1
      Metric=1
      Preference=100
      Private=Yes
```

3 Close the IP Route profile.

Configuring a numbered interface

In the following example, the MAX is a system-based router but supports a numbered interface for one of its connections. (If you are not familiar with numbered interfaces, see “Numbered interfaces” on page 10-7.) The double-headed arrow in Figure 10-13 indicates the numbered interface for this connection.

Figure 10-13. Example of a numbered interface



The numbered interface addresses are:

- IF Adrs=10.5.6.7/24
- WAN Alias=10.5.6.8/24

An unnumbered interface is also shown in Figure 10-13. The 10.1.2.3/32 connection uses a single system-based address for both the MAX itself and the dial-in user. To configure the unnumbered interface:

1 Open Ethernet > Mod Config > Ether Options and verify that the IP Adrs parameter is set to the IP address of the Ethernet interface of the MAX:

```
Ethernet
   Mod Config
      Ether options...
         IP Adrs=10.2.3.4/24
```

2 Close the Ethernet profile.

3 Open the Connection profile and configure the required parameters, then open the IP Options subprofile.

4 Specify the IP address of the Ethernet interface of the remote device by setting the LAN Adrs parameter.

```
Ethernet
      Connections
      IP options...
         LAN Adrs=10.3.4.5/24
```

5 Specify the numbered interface address for the remote device in the WAN Alias parameter.

```
      IP options...
         WAN Alias=10.7.8.9/24
```

6 Close the Connection profile.

Configuring IP routes and preferences

The IP routing table contains routes that are configured (static routes) and routes that are learned dynamically from routing protocols such as RIP or OSPF. Configuration of static routes involve the following parameters (shown with sample settings):

```
Ethernet
   Static Rtes
      Name=route-name
      Active=Yes
      Dest=10.2.3.0/24
      Gateway=10.2.3.4
      Metric=2
      Preference=100
      Private=No
      Ospf-Cost=1
      LSA-ASE7=ExternalType1
      NSSA-ASE7=N/A
      ASE-tag=c000000
      Third-Party=No
```

```
Ethernet
   Connections
      Route IP=Yes
      IP options...
         LAN Adrs=10.2.3.4/24
         WAN Alias=10.5.6.7/24
         IF Adrs=10.7.8.9/24
         Preference=100
         Metric=7
         DownPreference=120
         DownMetric=9
         Private=No
         SourceIP Check=No
         RIP=Off
         Pool=0
         Multicast Client=No
         Multicast Rate Limit=100
         Multicast Grp Leave Delay=0
         Client Pri DNS=
```

```
Ethernet
   Mod Config
      Ether options…
         IP Adrs=10.2.3.1/24
         2nd Adrs=0.0.0.0/0
         RIP=Off
         RIP2 Use Multicast=No
         Ignore Def Rt=Yes
         Proxy Mode=Off
         Filter=0
         IPX Frame=N/A


      Route Pref…
         Static Preference=100
         Rip Preference-100
         RIP Queue Depth=
```

```
RipAseType=Type2
Rip Tag=c8000000
OSPF Preference=10
OSPF ASE Preference=150
```

Understanding the static route parameters

This section provides some background information about static routes. For detailed information about each parameter, see the *MAX Reference Guide.*

2nd Adrs

The 2nd Adrs parameter assigns a second IP address to the Ethernet interface. With a second address, the MAX has a logical interface on two networks or two subnets on the same backbone. The configuration is sometimes called *dual IP.*.. The default value is 0.0.0.0/0.

Active

A route must be active to affect packet routing. If Active=No, the route is ignored.

ASE-tag

The ASE-tag parameter specifies the OSPF ASE tag of this link. The tag is a 32-bit hexadecimal number attached to each external route. The OSPF protocol does not use the value of ASE-tag. Border routers can use ASE-tag to filter this record. You can specify a 32-bit hexadecimal number. c0:00:00:00 is the default.

Client Pri DNS

The Client Pri DNS parameter specifies a primary DNS server address that the MAX sends to any IP-routing PPP client connecting to the MAX. The client DNS feature has two levels: a global configuration that applies to all PPP connections, and a connection-specific configuration that applies to that connection only. The MAX uses global client addresses only if you specify none in the Connection profile. Also, you can choose to present your local DNS servers if there are no defined or available client servers. You can specify the IP address of a DNS server to be used for all connections that do not have a DNS server defined. The default value is 0.0.0.0.

Dest

The destination address of a route is the target network (the destination address in a packet). Packets destined for that host use this static route to bring up the right connection. The zero address (0.0.0.0) represents the default route (the destination to which packets are forwarded when there is no route to the packet's destination).

DownMetric

The DownMetric parameter specifies the metric for a route whose associated WAN connection is down. The higher the metric, the less likely that the MAX will use the route. You can specify an integer. The default is 7.

DownPreference

The DownPreference parameter specifies the preference value for a route whose associated WAN connection is down. A higher preference number represents a less desirable route. You can specify an integer. The default is 120.

Filter

The Filter parameter specifies the number of a data filter that applies to the Ethernet interface. You can define the data filter to help manage data flow to and from the Ethernet interface. The filter examines every packet, and forwards or discards the packet on the basis of the configured Filter profile. You can specify a number from 0 to 199. The number you enter depends on the whether you are applying a filter created using the VT100 interface, or a firewall created using Secure Access Manager (SAM).

IF Adrs

The IF Adrs parameter specifies another local IP-interface address, to be used as the local numbered interface instead of the default (the Ethernet IP Adrs).

Gateway

The Gateway parameter specifies the IP address of the router or interface through which to reach the target network.

Ignore Def Rt

The Ignore Def Rt parameter specifies whether the MAX ignores the default route when updating its routing table via RIP updates. The default route specifies a static route to another IP router, which is often a local router such as a Cisco router or another kind of LAN router. When the MAX is configured to ignore the default route, RIP updates will not modify the default route in the MAX routing table. You can specify either Yes or No. No is the default.

IP Adrs

The IP Adrs parameter specifies the MAX unit's IP address on the local Ethernet. The MAX creates a route for this address at system startup.

IPX Frame

The IPX Frame parameter specifies the packet frame used by the majority of NetWare servers on Ethernet. The MAX routes and spoofs only one IPX frame type (IEEE 802.2 by default), which is specified in the IPX Frame parameter. If some NetWare software transmits IPX in a frame type other than the type specified here, the MAX drops those packets, or if bridging is enabled, it bridges them.

LAN Adrs

The LAN Adrs parameter specifies the IP address of Ethernet interface of the remote-end host or router. You can specify a valid IP address and subnet mask.

LSA-ASE7

The LSA-ASE7 parameter specifies the OSPF ASE type of this link-state advertisement (LSA). You can specify ExternalType-1, ExternalType-2, or Internal.

Metric

In a Connection or Route profile, Metric specifies a RIP metric associated with the IP route. In the Answer profile, it specifies the RIP metric of the IP link when the MAX validates an incoming call using RADIUS or TACACS and Use Answer as Default is enabled.

Multicast Client

The Multicast Client parameter enables the MAX to respond to multicast clients on the WAN link. Clients cannot be supported on the MBONE interface, so this means another WAN link or the local Ethernet supports a multicast router.

When you set Multicast Client to Yes, the MAX begins handling IGMP requests and responses on the interface. It does not begin forwarding multicast traffic until the rate limit is set. You can specify either Yes or No. The default is No.

Multicast GRP Leave Delay

The Multicast GRP Leave Delay parameter specifies the amount of seconds the MAX waits before forwarding any IGMP, version 2, `leave group` message from any multicast client. If you specify a value other than 0, and the MAX receives a leave group message, the MAX sends a igmp query to the WAN interface from which it received the `leave group` message. If the MAX does not receive a response from an active multicast client from the same group from the WAN interface, it sends a leave group message when the time you specified in the Multicast GRP Leave Delay parameter has expired.

If you specify the default value of zero, the MAX forwards any `leave group` message immediately. If users might establish multiple multicast sessions for identical groups, you should set Multicast GRP Leave Delay to a value from 10 to 120 seconds.

Multicast Rate Limit

The Multicast Rate Limit parameter specifies the rate at which the MAX accepts multicast packets from clients on this interface. It does not affect the MBONE interface.

Note: By default, the Rate Limit t parameter is set to 100, *which disables multicast forwarding on the interface.* The forwarder handles IGMP packets, but does not accept packets from clients or forward multicast packets from the MBONE router.

To begin forwarding multicast traffic on the interface, you must set the rate limit to a number less than 100. For example if you set it to 5, the MAX accepts a packet from multicast clients on the interface every 5 seconds. Any subsequent packets received in that 5-second window are discarded. You can specify a number lower than the default 100 to begin forwarding multicast traffic on the interface.

Name

IP routes are indexed by name. You can assign any name of less than 31 characters.

NSSA-ASE7

The NSSA-ASE 7 parameter specifies that area border routers convert ASE type-7 LSA to an ASE type-5 LSA. ASE type-7s can be imported only from static route definitions. NSSAs are described in RFC 1587. You can specify Advertise, or DoNotAdvertise.

OSPF ASE Preference

The OSPF ASE Preference parameter specifies the OSPF ASE Preference the MAX uses when importing an ASE. You can specify a number from 0 to 255. A value of 255 specifies that the MAX never puts any ASEs into its routing table.

OSPF-Cost

The OSPF-Cost parameter specifies the cost of an OSPF link. Cost is a configurable metric that takes into account the speed of the link and other issues. The lower the cost, the more likely is the interface to be used to forward data traffic. (For details, see Chapter 11, “Configuring OSPF Routing.”)

OSPF Preference

The OSPF Preference parameter specifies the OSPF ASE Preference the MAX uses when importing an ASE. You can specify a number from 0 to 255. A value of 255 specifies that the MAX never puts any ASEs into its routing table.

Pool

The Pool parameter specifies an IP address pool that the MAX assigns to incoming calls. If the Pool parameter is null but all other configuration settings enable dynamic assignment, the MAX gets IP addresses from the first defined address pool. You can define up to 10 IP address pools in the VT100 interface. Specify the number of the pool. The default is 1.

Preference

The Preference parameter specifies the Preference value for a route. RIP is a distance-vector protocol, which uses a hop count to select the shortest route to a destination network. OSPF is a link-state protocol, which means that OSPF can take into account a variety of link conditions, such as the reliability or speed of the link, when determining the best path to a destination network. Because these two metrics are incompatible, the MAX supports route preferences.

Private

The Private parameter specifies whether the MAX will disclose the existence of this route when queried by RIP or another routing protocol. Private routes are used internally but are not advertised. You can specify Yes or No. The default is No.

Proxy Mode

The Proxy Mode parameter specifies under what conditions the MAX responds to ARP requests for remote devices. When you enable Proxy Mode, the MAX responds to the ARP request with its own MAC address. You can specify one of the following values:

- Off—Disables proxy ARP. The default is Off.
- Always—Specifies that the MAX responds to any ARP request with its own MAC address if the ARP request is sent to a host to which the MAX has a route.
- Active—Specifies that the MAX responds to any ARP request with its own MAC address if the ARP request is sent to a host to which the MAX has an *active* connection.
- Inactive—Specifies that the MAX responds to an ARP request with its own MAC address if the ARP request is sent to a host to which the MAX has an *inactive* connection.

RIP2 Use Multicast

Specifies that Multicast IP is to be used for RIP 2 packets. You can specify Yes or No. No is the default.

RIP

The RIP parameter specifies how the MAX handles RIP update packets on the interface. RIP applies only if the MAX supports IP routing.

Note: You should configure all routers and hosts to run RIP-v2 instead of RIP-v1. The IETF has voted to move RIP version 1 into the *historic* category and its use is no longer recommended.

You can specify one of the following values:

- Off—Specifies that the MAX does not transmit or receive RIP updates. Off is the default.
- Recv-v2—Specifies that the MAX receives RIP-v2 updates on the interface but does not send RIP updates.
- Send-v2—Specifies that the MAX sends RIP-v2 updates on the interface but does not receive RIP updates.
- Both-v2—Specifies that the MAX sends and receives RIP-v2 updates on the interface.
- Recv-v1—Specifies that the MAX receives RIP-v1 updates on the interface but does not send RIP updates.
- Send-v1—Specifies that the MAX sends RIP-v1 updates on the interface but does not receive RIP updates.
- Both-v1—Specifies that the MAX sends and receives RIP-v1 updates on the interface.

RipAseType

The RipAseType parameter can specify Type-1 or Type-2. Type-1 is a metric expressed in the same units as the link-state metric (that is, the same units as interface cost). Type-2 is considered larger than any link-state path. It assumes that routing between autonomous systems is the major cost of routing a packet, and it eliminates the need for conversion of external costs to internal link-state metrics.

RIP Preference

The RIP Preference parameter specifies the preference value for routes learned from the RIP protocol. When choosing which routes to put in the routing table, the router first compares the Rip Preference values, preferring the lower number. If the Rip Preference values are equal, the router compares the Metric values, using the route with the lower Metric. You can specify a number between 0 and 255. The default value is 100. Zero is the default for connected routes (such as the Ethernet). The value of 255 means *Do not use this route*.

RIP Queue Depth

The maximum number of unprocessed RIP requests which the MAX saves. If RIP requests arrive at a rate faster than they can be processed, then a backlog builds up. This parameter sets the maximum depth of the queue. If the queue fills, further packets destined for it are discarded. This limit applies to each RIP socket, so if RIP is running on multiple interfaces, this parameter limits the number of requests stored per interface. You can enter a number from 0 to 1024. If you specify 0, the MAX saves RIP requests until it runs out of memory. The default is 50.

RIP Tag

The Rip Tag parameter is *attached* to all routes learned from RIP in OSPF updates. The tag is a hexadecimal number that can be used by border routers to filter the record.

SourceIP Check

The SourceIP Check parameter enables and disables anti-spoofing for this session. When set to Yes, the system checks all packets received on this interface to ensure that the source IP address in the packets matches the far-end remote address or the address agreed upon in IPCP negotiation. If the addresses do not match, the system discards the packet. You can specify Yes or No. No is the default.

Static Preference

By default, static routes and RIP routes have the same preference, so they compete equally. ICMP redirects take precedence over both, and OSPF routes take precedence over everything. If a dynamic route's preference is lower than that of the static route, the dynamic route can overwrite (*hide)* a static route to the same network. In the IP routing table, the hidden static route has an *h* flag, indicating that it is inactive. The active, dynamically learned route is also in the routing table. However, dynamic routes age and, if no updates are received, eventually expire. In that case, the hidden static route reappears in the routing table.

Third-Party

The Third-Party parameter enables OSPF third-party routing for a static route. When enabled, the gateway address is used as the third-party router for this route. Third-party routing enables an OSPF router to advertise a route to a destination network through a remote router (Router-A advertises a route to Network-B via Router-C). This is accomplished by specifying the address of the remote router (Router-C) in the next-hop field of an LSA.

Note: In some cases, third-party routing results in more efficient routes, because other OSPF routers (such as Router-D and Router-E) might be able to trim one hop off of the packet's path and send it to the specified address (Router-C) directly. In practice, it requires that the third-party router is on an Ethernet that is running OSPF, and that its designated router is advertising that network into the OSPF cloud.

WAN Alias

The WAN Alias parameter is another IP address for the remote device, used for numbered-interface routing. The WAN alias will be listed in the routing table as a gateway (next hop) to the Lan Adrs value. The caller must use a numbered interface, and its interface address must agree with the WAN Alias setting.

Examples of static route configuration

This section discusses configuring the default static route, a static route to a remote subnet, a method to make sure the MAX uses the static routes before RIP routes.

For sample Connection profile configurations, see "Configuring IP routing connections" on page 10-23. Each of the configurations shown in that section. For an example of the Ethernet profile configuration of the MAX unit's local IP interface, see "Configuring the MAX IP interface on a subnet" on page 10-15.

Configuring the default route

If no routes exist for the destination address of a packet, the MAX forwards the packet to the default route. Most sites use the default route to specify a local IP router (such as a Cisco router or a UNIX host running the route daemon) to offload routing tasks to other devices.

Note: If the MAX does not have a default route, it drops packets for which it has no route.

To configure the default route:

1. Open the first IP Route profile (the route named Default) and activate it:

   ```
   Ethernet
      Static Rtes
         Name=Default
         Active=Yes
         Dest=0.0.0.0/0
   ```

   Note: The name of the first IP Route profile is always Default, and its destination is always 0.0.0.0. You cannot change these values.

2. Specify the router to use for packets with unknown destinations. For example:

   ```
   Gateway=10.9.8.10
   ```

3. Specify a metric for this route, the route's preference, and whether the route is private. For example:

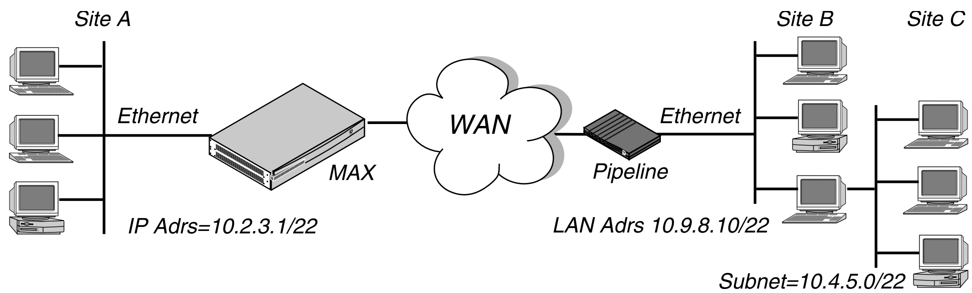
   ```
   Metric=1
   Preference=100
   Private=Yes
   ```

4. Close the IP Route profile.

Defining a static route to a remote subnet

If the connection does not enable RIP, the MAX does not learn about other networks or subnets that might be reachable through the remote device. The remote network shown in Figure 10-14 is an example of such a network.

Figure 10-14. Two-hop connection that requires a static route when RIP is off



To enable the MAX to route to Site C without using RIP, you must configure an IP Route profile similar to the following example:

```
Ethernet
   Static Rtes
      Name=SITEBGW
      Active=Yes
      Dest=10.4.5.0/22
      Gateway=10.9.8.10
      Metric=2
      Preference=100
      Private=Yes
      Ospf=Cost=1
      ASE-type=Type1
      ASE=tag=c0000000
```

Example of route preferences configuration

The following example increases the preference value of RIP routes, instructing the router to use a static route first if one exists:

1 Open Ethernet > Mod Config > Route Pref.

2 Set Rip Preference to 150:

```
Ethernet
   Mod Config
      Route Pref…
         Rip Preference=150
```

3 Close the Ethernet profile.

Configuring the MAX for dynamic route updates

You can configure each active interface to send or receive RIP or OSPF updates. (For information about OSPF updates, see Chapter 11, "Configuring OSPF Routing.") You can also configure the Ethernet interface to accept or ignore ICMP redirects. All of these routing mechanisms modify the IP routing table dynamically.

Following are the parameters that enable the MAX to receive updates from RIP or ICMP, (the settings shown are examples.)

```
Ethernet
   Mod Config
      Ether options…
         RIP=On
         Ignore Def Rt=Yes
      RIP Policy=Poison Rvrs
      RIP Summary=Yes
      ICMP Redirects=Accept
```

```
Ethernet
   Answer
      Session options...
         RIP=On
```

```
Ethernet
   Connections
    any Connection profile
      IP options...
         Private=No
         RIP=On
```

Understanding the dynamic routing parameters

This section provides some background information about the dynamic routing options. For complete information about each parameter, see the *MAX Reference Guide.*

RIP (Routing Information Protocol)

You can configure the MAX to send or receive, or send and receive, RIP updates on the Ethernet interface and on each WAN interface. The RIP parameter in Ethernet > Answer > Session options profile applies to local profiles and profiles retrieved from RADIUS. You can also select between RIP-v1 and RIP-v2 on any interface. Many sites turn off RIP on WAN connections to keep their routing tables from becoming very large.

Note: The IETF has voted to move RIP-v1 into the *historic* category and its use is no longer recommended. Ascend recommends that you upgrade all routers and hosts to RIP-v2. If you must maintain RIP-v1, Ascend recommends that you create a separate subnet and place all RIP-v1 routers and hosts on that subnet.

Ignore Def Rt

You can configure the MAX to ignore default routes advertised by routing protocols. This configuration is recommended, because you typically do not want the default route changed by a RIP update. The default route specifies a static route to another IP router, which is often a local router such as a Cisco or kind of LAN router. When you configure the MAX to ignore the default route, RIP updates do not modify the default route in the MAX routing table.

RIP Policy and RIP Summary

The RIP Policy and RIP Summary parameters have no affect on RIP-v2.

If the MAX is running RIP-v1, the RIP Policy parameter specifies a split horizon or poison reverse policy to handle update packets that include routes that are received on the same interface on which the update is sent. Split-horizon means that the MAX does not propagate routes back to the subnet from which they were received. Poison-reverse means that it propagates routes back to the subnet from which they were received, but with a metric of 16.

The RIP Summary parameter specifies whether to summarize subnet information when advertising routes. If the MAX summarizes RIP routes, it advertises a route to all the subnets in a network of the same class. For example, the route to 200.5.8.13/28 (a class C address subnetted to 28 bits) would be advertised as a route to 200.5.8.0. When the MAX does not summarize information, it advertises each route in its routing table as-is. For the subnet in the preceding example, the MAX would advertise a route only to 200.5.8.13.

Ignoring ICMP Redirects

The design for ICMP enables the MAX to dynamically find the most efficient IP route to a destination. ICMP Redirect packets are one of the oldest route discovery methods on the Internet. They are also one of the least secure methods, because it is possible to counterfeit ICMP Redirects and change the way a device routes packets.

Private routes

If you configure a Connection profile with Private=Yes, the router does not disclose its route in response to queries from routing protocols.

Examples of RIP and ICMP configurations

The following sample configuration instructs the MAX to ignore ICMP redirect packets, to receive (but not send) RIP updates on Ethernet, and to send (but not receive) RIP updates on a WAN connection.

1 Open Ethernet > Mod Config > Ether Options.

2 Configure the MAX to receive (but not send) RIP updates on Ethernet.

```
Ethernet
   Mod Config
      Ether options…
         RIP=Recv-v2
```

Receiving RIP updates on Ethernet means that the MAX learns about networks that are reachable via other local routers. However, it does not propagate information about all of its remote connections to the local routers.

3 Close the Ether Options subprofile, and set ICMP Redirects to Ignore.

```
ICMP Redirects=Ignore
```

4 Close the Ethernet profile.

5 Open Connections > IP Options, and configure the MAX to send (but not receive) RIP updates on this link.

```
Ethernet
   Connections
      IP options...
         RIP=Send-v2
```

Sending RIP on a WAN connection means that the remote devices are able to access networks that are reachable via other local routers. However, the MAX does not receive information about networks that are reachable through the remote router.

6 Close the Connection profile.

Translating Network Addresses for a LAN

Network Address Translation (NAT) functionality makes it possible for the MAX to translate private IP addresses on its local LAN to IP addresses temporarily supplied by a remote access router.

To connect to the Internet or any other TCP/IP network, a host must have an IP address that is unique within that network. The Internet and other large TCP/IP networks guarantee the uniqueness of addresses by creating central authorities that assign official IP addresses. However, many local networks use private IP addresses that are unique only on the local network. To enable a host with a private address to communicate with the Internet or another network that requires an official IP address, a MAX performs a service known as Network Address Translation (NAT). The service works as follows:

- When the local host sends packets to the remote network, the MAX automatically translates the host’s private address on the local network to an official address on the remote network.
- When the local host receives packets from the remote network, the MAX automatically translates the official address on the remote network to the host’s private address on the local network.

NAT can be implemented to use a single address or multiple addresses. To use multiple IP addresses, the MAX must have access to a DHCP server through the remote network.

Single-address NAT and port routing

A MAX can perform single-address NAT in the following ways:

- For more than one host on the local network, without borrowing IP addresses from a DHCP server on the remote network.
- When the remote network initiates the connection to the MAX.
- By routing packets it receives from the remote network for up to 10 different TCP or UDP ports to specific hosts and ports on the local network.

Note: You can use single-address NAT by setting the Ethernet > NAT > Lan parameter to Single IP Addr.

With single-address NAT, the only host on the local network that is visible to the remote network is the MAX.

Outgoing connection address translation

For outgoing calls, the MAX performs NAT for multiple hosts on the local network after getting a single IP address from the remote network during PPP negotiation.

Any number of hosts on the local network can make any number of simultaneous connections to hosts on the remote network. The network is limited only to the size of the translation table. The translations between the local network and the Internet or remote network are dynamic and do not need to be preconfigured.

Incoming connection address translation

For incoming calls, the MAX can perform NAT for multiple hosts on the local network by using its own IP address. The MAX routes incoming packets for up to 10 different TCP or UDP ports to specific servers on the local network. Translations between the local network and the Internet or remote network are static and need to be preconfigured. You need to define a list of local servers and the UDP and TCP ports each should handle. You can also define a local default server that handles UDP and TCP ports not listed.

For example, you can configure the MAX to route all incoming packets for TCP port 80 (the standard port for HTTP) to port 80 of a World Wide Web server on the local network. The port you route to does not have to be the same as the port specified in the incoming packets. For example, you can route all packets for TCP port 119, the well known port for Network News Transfer Protocol, to port 1119 on a Usenet News server on the local network. You can also specify a default server that receives any packets that are not sent to one of the routed ports. If you do not specify any routed ports but do specify a default server, the default server receives all packets sent to the MAX from the remote network.

When you configure the MAX to route incoming packets for a particular TCP or UDP port to a specific server on the local network, multiple hosts on the remote network can connect to the server at the same time. The number of connections is limited by the size of the translation table.

Note: NAT automatically turns RIP off, so the address of the MAX is not propagated to the Internet or remote networks.

Translation table size

NAT has an internal translation table limited to 500 active addresses. A translation-table entry represents one TCP or UDP connection.

Note: A single application can generate many TCP and UDP connections.

A translation table entry is reused as long as traffic includes packets that match the entry. All the entries for a connection are freed (expire) when the connection disconnects. For Nailed connections, the connection is designed not to disconnect.

The MAX removes entries from the translation-table on the basis of the following timeouts:

- Non-DNS UDP translations timeout after 5 minutes.
- DNS times out in one minute.
- TCP translations time out after 24 hours.

Multiple-address NAT

When translating addresses for more than one host on the local network, the MAX can perform multiple-address NAT by borrowing an official IP address for each host from a Dynamic Host Configuration Protocol (DHCP) server on the remote network or accessible from the remote network.

The advantage of multiple-address NAT is that hosts on the remote network can connect to specific hosts on the local network, not just specific services such as Web or FTP service. This advantage can be realized only if the remote DHCP server is configured to assign the same address whenever a particular local host requests an address. Another reason for using multiple-address NAT is that network service providers might require it for networks with more than one host.

When you use multiple-address NAT, hosts on the remote network can connect to any of the official IP addresses that the MAX borrows from the DHCP server. If the local network must have more than one IP address that is visible to the remote network, you must use multiple-address NAT. If hosts on the remote network need to connect to a specific host on the local network, you can configure the DHCP server to always assign the same address when that local host requests an address.

When multiple-address NAT is enabled, the MAX attempts to perform IP address translation on all packets received. (It cannot distinguish between official and private addresses.)

The MAX acts as a DHCP client on behalf of all hosts on the LAN and relies on a remote DHCP server to provide addresses from a pool of addresses suitable for the remote network. On the local network, the MAX and the hosts all have *local* addresses that are only used for local communication between the hosts and the MAX over the Ethernet.

When the first host on the LAN requests access to the remote network, the MAX obtains an address through PPP negotiation. When subsequent hosts request access to the remote network, the MAX sends a DHCP request packet asking for an IP address from the DHCP server. The server then sends an address from its IP address pool to the MAX. The MAX uses the dynamic addresses it receives from the server to translate IP addresses on behalf of local hosts.

As packets are received on the LAN, the MAX determines whether the source IP address has been assigned a translated address. If so, the packet is translated and forwarded to the wide area network. If no translation has been assigned (and none is pending), the MAX issues a DHCP request for the packet's IP address. While waiting for an IP address to be offered by the server, the MAX drops corresponding source packets. Similarly, for packets received from the WAN, the MAX checks the destination address against its table of translated addresses. If the destination address is in the table and is active, the MAX forwards the packet. If the destination address is not in the table, or is not active, the MAX drops the packet.

IP addresses are typically offered by the DHCP server only for a limited duration, but the MAX automatically renews the leases on them. If the connection to the remote server is dropped, all leased addresses are considered revoked. Therefore, TCP sessions do not persist if the WAN call disconnects.

The MAX itself does not have an address on the remote network. Therefore, the MAX can only be accessed from the local network, not from the WAN. For example, you can Telnet to the MAX from the local network, but not from a remote network.

In some installations, the DHCP server could be handling both NAT DHCP requests and ordinary DHCP requests. In this situation, if the ordinary DHCP clients are connecting to the server over a nonbridged connection, you must have a separate DHCP server to handle the ordinary DHCP requests. The NAT DHCP server only handles NAT DHCP requests.

Configuring single or multiple address NAT

To configure NAT on the MAX:

1 Open the Ethernet > NAT > NAT menu. For example:

```
50-C00 NAT
 50-C01 NAT...
   >Routing=Yes
   Profile=NATprofile
   Lan=Single IP addr
   FR address=10.10.10.10
   Static Mappings...
   Def Server=N/A
   Reuse last addr=N/A
   Reuse addr timeout=N/A
```

2 Enable NAT by setting Routing to Yes. Without this setting, no other setting is valid.

3 Set Profile to the name of a Connection profile you want to use NAT.

4 If applying NAT to Frame Relay connections, set FR Address and other parameters as described in "NAT for Frame Relay" on page 10-50.

5 Optionally, configure NAT port routing in the Static Mapping *nn* submenus, as described in "Configuring NAT port routing (Static Mapping submenu)" on page 10-50.

6 Optionally set Def Server to the IP address of a local server to which the MAX routes incoming packets that are *not* routed to a specific server and port. (For more information, see "Routing all incoming sessions to the default server" on page 10-51.)

7 Optionally set Reuse Last Addr to Yes to continue to use a dynamically assigned IP address. The Reuse Addr Timeout value specifies the time for which to use the address. Set it to a number of minutes (up to 1440). Limitations apply, as described in the *MAX Reference Guide*.

8 Exit and save the NAT profile.

Note: If you have additional routers on your local area network, open Ethernet > Mod Config > Ether Options, and set the value of Ignore Def Rt to Yes. This avoids the possibility that a default route from the ISP overwrites the NAT route.

NAT for Frame Relay

The single-IP address implementation of NAT extends to Frame Relay. For connections using Frame Relay encapsulation, a MAX running single-IP address NAT translates the local addresses into a single, official address specified by the FR Address parameter. You must set the Routing parameter in the NAT profile to enable NAT, set the Lan parameter to Single IP Addr, and set FR Address to a valid, official IP address:

```
50-C00 NAT
 50-C01 NAT...
    Routing=Yes
    Profile=max4
    Lan=Single IP addr
    FR address=10.10.10.10
    Static Mapping...
    Def Server=181.81.8.1
    Reuse last addr=No
    Reuse addr timeout=N/A
```

Configuring NAT port routing (Static Mapping submenu)

The Static Mappings menu includes 10 Static Mapping *nn* submenus, where *nn* is a value from 1 to 10. Each of these submenus contains parameters for controlling the translation of the private IP addresses to TCP or UDP port numbers when operating in single-address NAT mode. You only need to specify static mappings for connections initiated by devices calling into the private LAN. For sessions initiated by hosts on the private LAN, the MAX generates a mapping dynamically if one does not already exist in the Static Mappings parameters.

Each Static Mapping *nn* menu contains the following parameters (shown with sample settings):

```
50-C00 NAT
 50-C01 NAT...
  Static Mappings...
   Static Mapping 01
      Valid=Yes
      Dst Port #=21
      Protocol=TCP
      Loc Port #=21
      Loc Adrs=181.100.100.102
```

You can configure a NAT port routing

- to define a default server on the local private LAN

  The MAX routes incoming packets to the default server when their destination port number does not match an entry in Static Mappings nor does it match a port number dynamically assigned when a local host initiates a TCP / UDP session.
- to define a list of up to 10 servers & services on the local private LAN

  The MAX routes incoming packets to hosts on the local private LAN when their destination port matches one of the 10 destination ports in Static Mappings. .

Note: You need to configure port routing only for sessions initiated by hosts outside the private LAN. For sessions initiated by hosts on the private LAN, the MAX generates the port mapping dynamically.

For port routing in single-address NAT to work, if firewalls are present, they must be configured to enable the MAX to receive packets for the routed ports.

Routing all incoming sessions to the default server

To configure the MAX to perform NAT and to define a single server which handles all sessions initiated by callers from outside the private LAN:

1 Open the Ethernet > NAT > NAT menu.

2 Set the Routing parameter to Yes.

3 Set the Profile parameter to the name of an existing Connection profile.

The MAX performs NAT whenever a connection is made with this Connection profile. The connection can be initiated either by the MAX or by the remote network.

4 Set the Lan parameter to Single IP Addr.

5 To ensure that all incoming sessions are routed to the default server, open each Ethernet > NAT > Static Mappings > Static Mapping *NN* menu (where *NN* is a number from 1 to 10) and make sure to set the Valid parameter in each menu is set to No.

6 Set the Def Server parameter to the IP address of the server on the local network to receive all incoming packets from the remote network.

7 Press the Esc key to exit the menu.

8 Save the changes when prompted.

The changes take effect the next time a connection specified in the NAT profile is established. To activate the changes immediately, close the connection specified by the Profile parameter and then reopen it.

Routing incoming sessions to up to ten servers on the private LAN

To configure the MAX to perform NAT and to define up to ten servers, and optionally a default server, to handle sessions initiated by callers from outside the private LAN:

1 Open the Ethernet > NAT > NAT menu.

2 Set the Routing parameter to Yes.

3 Set the Profile parameter to the name of an existing Connection profile.

The MAX performs NAT whenever a connection is made with this Connection profile. The connection can be initiated either by the MAX or by the remote network.

4 Set the Lan parameter to Single IP Addr.

5 Open the Ethernet > NAT > NAT > Static Mappings menu.

6 Open a Static Mapping *nn* menu, where *nn* is a number from 1 to 10.

You use the parameters in each Static Mapping *nn* menu to specify routing for incoming packets sent to a particular TCP or UDP port.

7 Set the Valid parameter to Yes.

This enables the port routing specified by the remaining parameters in the menu. Setting this parameter to No disables routing for the specified port.

8 Set the Dst Port # parameter to the number of a TCP or UDP port that users outside the private network can access.

Each Dst Port # corresponds to a service provided by a server on the local private network. You can use the actual port number as given by the Loc Port # parameter as long as that address is unique for the local private network. For information about obtaining port number, see “Well-known ports” on page 10-53.

The MAX routes incoming packets it receives from the remote network for this port to the local server and port you are about to specify.

9 Set the Protocol parameter to TCP or UDP.

This parameter determines whether the Dst Port # and Loc Port # parameters specify TCP ports or UDP ports.

10 Set the Loc Port # to a port corresponding to a service provided by the local servers.

11 Set the Loc Adrs parameter to the address of the local server providing the service specified by Loc Port #.

12 Exit and save the profile.

Repeat steps 6 through 12 for any additional ports whose packets you want to route to a specific server and port on the local network.

13 Optionally, open the Ethernet > NAT > NAT menu and set the Def Server parameter to the IP address of a server, on the local network, that is to receive any remaining incoming packets from the remote network (that is, any that are not for ports you have specified in Static Mapping *nn* menus).

14 Exit and save the profile.

The changes take effect the next time a connection specified in the NAT profile is established. To activate the changes immediately, close the connection specified by the Profile parameter and then reopen it.

Disabling routing for specific ports

To disable routing of incoming packets destined for specific TCP or UDP ports:

1 Open the Ethernet > NAT > Static Mappings menu.

2 Open a Static Mapping *nn* menu, where *nn* is a number from 1 to 10.

The parameters in each Static Mapping *nn* menu specify the routing for incoming packets sent to a particular TCP or UDP port.

3 Set the Valid parameter to No.

This disables routing for the port specified by the Dst Port # and Protocol parameters in this menu.

4 Exit and save the profile.

Repeat steps 2 through 4 to disable routing for any additional ports.

5 Exit and save the profile.

The changes take effect the next time the MAX makes a connection specified in the NAT profile. To make the changes immediately, close the connection specified by the Profile parameter and then reopen it.

Well-known ports

TCP and UDP ports numbered 0–1023 are the Well Known Ports. The Internet Assigned Numbers Authority (IANA) assigns these ports, which include the ports for the most common services available on the Internet. In almost all cases, the TCP and UDP port numbers for a service are the same.

You can obtain current lists of Well Known Ports and Registered Ports (ports in the range 1024–4915 that have been registered with the IANA) via FTP from:

`ftp://ftp.isi.edu/in-notes/iana/assignments/port-numbers`

Proxy-QOS and TOS support in the MAX

You can configure the MAX to set priority bits and Type-of-Service (TOS) classes of service on behalf of customer applications. The MAX does not implement priority queuing, but it does set information that can be used by upstream routers to prioritize and select links for particular data streams.

You can enable proxy-QOS and TOS by setting parameters that define a policy in a Connection profile or RADIUS profile. The parameters in the profile set bits in the TOS byte of IP packet headers that are received, transmitted, or both, on the WAN interface. You can then configure other routers to interpret the bits accordingly.

You can also specify proxy-QOS and TOS policy in a TOS filter, which you apply to any number of Connection or RADIUS profiles. Like other kinds of Ascend packet filters, a TOS filter can affect incoming packets, outgoing packets, or both, depending on how you define the filter.

For a Connection profile or RADIUS profile that has both its own local policy and an applied TOS filter, the policy defined in the TOS filter takes precedence. For example, applying a TOS filter to a TOS-enabled connection allows you to define one priority setting for incoming packets on a connection and another policy for incoming packets addressed to a particular destination specified in a TOS filter.

Defining QOS and TOS policy within a profile

To provide service-based TOS or to set precedence for the traffic on a particular WAN connection, you can define the policy directly in a Connection profile or RADIUS profile.

Settings in a Connection profile

Following are the relevant Connection profile parameters:

Parameter	Description
TOS Enabled	Enables Type of Service (TOS) for this connection. If you set Active to No, none of the other TOS options apply.
Precedence	Specifies the priority level of the data stream. The three most significant bits of the TOS byte are priority bits used to set precedence for priority queuing. When you enable TOS, you can set three most significant bits to one of the following values (most significant bit first): 000: Normal priority. 001: Priority level 1. 010: Priority level 2. 011: Priority level 3. 100: Priority level 4. 101: Priority level 5. 110: Priority level 6. 111: Priority level 7 (the highest priority).
TOS	Specifies the Type of Service of the data stream. When TOS is enabled, you can set TOS to one of the following values: Normal—Normal service. Cost—Minimize monetary cost. Reliability—Maximize reliability. Throughput—Maximize throughput. Latency—Minimize delay. **Note:** The four bits adjacent to the most significant bits of the TOS byte specify Type of Service of the data stream.
Apply To	Specifies the direction in which the MAX supports TOS. If you set Apply To to Input, the MAX sets TOS bits in packets received on the interface. If you set Apply To to Output, the MAX sets TOS bits in outbound packets. If you set Apply To to Both, the MAX set TOS bits for incoming *and* outgoing packets.

Settings in a RADIUS profile

Following are the relevant attribute-value pairs in RADIUS:

Attribute	Value
Ascend-IP-TOS (88)	Specifies Type of Service (TOS) of the data stream. You can specify one of the following values: Ascend-IP-TOS IP-TOS-Normal (0): Normal service. Ascend-IP-TOS IP-TOS-Disabled (1): Disables TOS. Ascend-IP-TOS IP-TOS-Cost (2): Minimize monetary cost. Ascend-IP-TOS IP-TOS-Reliability (4): Maximize reliability. Ascend-IP-TOS IP-TOS-Throughput (8): Maximize throughput. Ascend-IP-TOS IP-TOS-Latency (16): Minimize delay. **Note:** The value of this attribute sets the four bits following the three most significant bits of the TOS byte which can be used to choose a link based on the type of service.
Ascend-IP-TOS-Precedence (89)	Specifies the priority level of the data stream. The three most significant bits of the TOS byte are priority bits used to set precedence for priority queuing. When you enable TOS, you can set the three most significant bits to one of the following values (most significant bit first): IP-TOS-Precedence-Pri-Normal (0): Normal priority. IP-TOS-Precedence-Pri-One (32): Priority level 1. IP-TOS-Precedence-Pri-Two (64): Priority level 2. IP-TOS-Precedence-Pri-Three (96): Priority level 3. IP-TOS-Precedence-Pri-Four (128): Priority level 4. IP-TOS-Precedence-Pri-Five (160): Priority level 5. IP-TOS-Precedence-Pri-Six (192): Priority level 6. IP-TOS-Precedence-Pri-Seven (224): Priority level 7 (the highest priority).
Ascend-IP-TOS-Apply-To (90)	Specifies the direction in which the MAX supports TOS. If you set Ascend-IP-TOX-Apply-To to IP-TOS-Apply-To-Incoming (1024) which is the default, the MAX sets bits in packets received on the interface. If you set the attribute to IP-TOS-Apply-To-Outgoing (2048), the MAX sets bits in outbound packets. If you set the attribute to IP-TOS-Apply-To-Both (3072), the MAX sets bits in packets for incoming and outgoing packets.
Ascend-Filter (91)	A string-format filter, which can include an IP TOS filter specification. Ascend-Filter will replace binary-based filters.

Examples of connection-based proxy-QOS and TOS

The following set of commands enables TOS for incoming packets on a WAN interface. The profile sets the priority of the packets at 6 which specifies that an upstream router (that supports priority queuing) will not drop the packets until it has dropped all packets of a lower priority. The commands also set TOS to prefer maximum throughput which specifies that the upstream router (that supports priority queuing) will choose a a high bandwidth connection is one is available, even if it is higher cost, higher latency, or less reliable than another available link.

```
Ethernet
   Connections
      sampleProf
         IP options
            LAN Adrs = 10.168.6.120/24
            TOS Enabled = Yes
            Precedence = 110
            TOS = Throughput
```

Following is a comparable RADIUS profile:

```
sampleProf Password = "mypasswd", User-Service = Framed-User
    Framed-Protocol = PPP,
    Framed-IP-Address = 10.168.6.120
    Framed-IP-Netmask = 255.255.255.0
    Framed-Routing = 3
    Ascend-IP-TOS = IP-TOS-Throughput
    Ascend-IP-TOS-Precedence = IP-TOS-Precedence-Pri-Six
    Ascend-IP-TOS-Apply-To = IP-TOS-Apply-To-Incoming
```

Defining TOS filters

To enable proxy-QOS for all packets that match a specific filter specification, administrators can define a TOS filter locally in a Filter profile, and then apply the filter to any number of Connection profiles or RADIUS profiles. (The Filter-ID attribute can apply a local Filter profile to RADIUS user profiles.) Administrators can also define TOS filters directly in a RADIUS user profile by setting the Ascend-Filter attribute.

Settings in a local Filter profile

Following are the relevant Filter parameters:

Parameter	Description
Protocol	Specifies a TCP/IP protocol number. A value of zero matches all protocols. If you specify a non-zero number, the MAX compares it to the Protocol field in packets. For a complete list of protocol numbers, see RFC 1700.

Parameter	Description
Source-Address-Mask	Specifies a subnet mask to apply to the Source-Address value before comparing the result to the source address in a packet. The MAX translates both the Source-Address-Mask and Source-Address values into binary format and then uses a logical AND to apply the Source-Address-Mask to the Source-Address. The mask hides the portion of the Source-Address that appears behind each binary 0 (zero) in the mask. A mask of all zeros (the default) masks all bits. If the Source-Address value is also all zeros, all source addresses in packets are matched. A mask of all ones (255.255.255.255) masks no bits, so the full source address for a single host is matched.
Source-Address	Specifies an IP address. After applying the Source-Address-Mask to this value, the MAX compares the result to the source address in a packet.
Dest-Address-Mask	Specifies a subnet mask to apply to the Dest-Address value before comparing the result to the destination address in a packet. The MAX translates both the Dest-Address-Mask and Dest-Address values into binary format and then uses a logical AND to apply the Dest-Address-Mask to the Dest-Address. The mask hides the portion of the Dest-Address that appears behind each binary 0 (zero) in the mask. A mask of all zeros (the default) masks all bits. If the Dest-Address value is also all zeros, all destination addresses in packets are matched. A mask of all ones (255.255.255.255) masks no bits, so the full destination address for a single host is matched.
Dest-Address	Specifies an IP address. After applying the Dest-Address-Mask to this value, the MAX compares the result to the destination address in a packet.
Src-Port-Cmp	Specifies how the MAX compares the source port number in a packet to the value specified in Source-Port. If you set Src-Port-Cmp to None, the MAX makes no comparison. You can specify that the filter matches the packet if the packet's source port number is Less (less than), Eql (equal to), Gtr (greater than), or Neq (not equal to) the Source-Port number.
Source-Port	Specifies a port number that the MAX compares to the source port in a packet. TCP and UDP port numbers are typically assigned to services. For a list of all port numbers, see RFC 1700.
Dst-Port-Cmp	Specifies how the MAX compares the destination port number in a packet to the value specified in Dest-Port. If you set it to None, the MAX makes no comparison. You can specify that the filter matches the packet if the packet's destination port number is Less (less than), Eql (equal to), Gtr (greater than), or Neq (not equal to) the Dest-Port number.
Dest-Port	Specifies a port number that the MAX compares with the destination port in a packet. See RFC 1700 for a list of port numbers.

Parameter	Description
Precedence	Specifies the priority level of the data stream. The three most significant bits of the TOS byte are priority bits used to set precedence for priority queuing. When TOS is enabled and the packet matches the filter, can be set to one of the following values (most significant bit first): 000: Normal priority. 001: Priority level 1. 010: Priority level 2. 011: Priority level 3. 100: Priority level 4. 101: Priority level 5. 110: Priority level 6. 111: Priority level 7 (the highest priority).
Type-of-Service	Type of Service of the data stream. When TOS is enabled and the packet matches the filter, one of the following values can be set in the packet: Normal—Normal service. Cost—Minimize monetary cost. Reliability—Maximize reliability. Throughput—Maximize throughput. Latency—Minimize delay. **Note:** The four bits adjacent to the three most significant bits of the TOS byte are used to choose a link based on the type of service.

If you are not familiar with Ascend packet filters, you can find background information in the *Network Configuration Guide* for your MAX. Standard IP filters use many of the same settings as TOS filters.

Settings in RADIUS

In RADIUS, a TOS filter entry is a value of the Ascend-Filter attribute. Specify the TOS filter value in the following format:

```
iptos dir [ dstip n.n.n.n/nn ] [ srcip n.n.n.n/nn ][ proto ]
[ destport cmp value ] [ srcport cmp value ][ precedence value ]
[ type-of-service value ]
```

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

Keyword or argument	Description
iptos	Specifies an IP filter.
dir	Specifies filter direction. You can specify `in` (to filter packets coming into the MAX) or `out` (to filter packets going out of the MAX).

Keyword or argument	Description
`dstip` *n.n.n.n/nn*	If the `dstip` keyword is followed by a valid IP address, the TOS filter sets bytes only in packets with that destination address. If a subnet mask portion of the address is present, the MAX compares only the masked bits. If the `dstip` keyword is followed by the zero address (0.0.0.0), or if this keyword and its IP address specification are not present, the filter matches all IP packets.
`srcip` *n.n.n.n/nn*	If the `srcip` keyword is followed by a valid IP address, the TOS filter sets bytes only in packets with that source address. If a subnet mask portion of the address is present, the MAX compares only the masked bits. If the `srcip` keyword is followed by the zero address (0.0.0.0), or if this keyword and its IP address specification are not present, the filter matches all IP packets.
proto	Specifies a TCP/IP protocol number. A value of zero matches all protocols. If you specify a non-zero number, the MAX compares it to the Protocol field in packets. See RFC 1700 for a complete list of protocol numbers.
`dstport` *cmp value*	If the `dstport` keyword is followed by a comparison symbol and a port, the MAX compares the specified port to the destination port of a packet. The comparison symbol can be < (less-than), = (equal), > (greater-than), or != (not-equal). The port value can be one of the following names or numbers: ftp-data (20), ftp (21), telnet (23), smtp (25), nameserver (42), domain (53), tftp (69), gopher (70), finger (79), www (80), kerberos (88), hostname (101), nntp (119), ntp (123), exec (512), login (513), cmd (514), talk (517).
`srcport` *cmp value*	If the `srcport` keyword is followed by a comparison symbol and a port, the MAX compares the specified port to the source port of a packet. The comparison symbol can be < (less-than), = (equal), > (greater-than), or != (not-equal). The port value can be one of the following names or numbers: ftp-data (20), ftp (21), telnet (23), smtp (25), nameserver (42), domain (53), tftp (69), gopher (70), finger (79), www (80), kerberos (88), hostname (101), nntp (119), ntp (123), exec (512), login (513), cmd (514), talk (517).
`precedence` *value*	Specifies the priority level of the data stream. The three most significant bits of the TOS byte are priority bits used to set precedence for priority queuing. If a packet matches the filter, those bits are set to the specified value (most significant bit first): 000: Normal priority. 001: Priority level 1. 010: Priority level 2. 011: Priority level 3. 100: Priority level 4. 101: Priority level 5. 110: Priority level 6. 111: Priority level 7 (the highest priority).

Keyword or argument	Description
`type-of-service` *value*	Specifies the Type of Service of the data stream. One of the following values can be specified: Normal (0): Normal service. Disabled (1): Disables TOS. Cost (2): Minimize monetary cost. Reliability (4): Maximize reliability. Throughput (8): Maximize throughput. Latency (16): Minimize delay. **Note:** If a packet matches the filter, the system sets the four bits following the three most significant bits of the TOS byte to the specified value. Those four bits are used to choose a link based on the type of service.

Examples of defining a TOS filter

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

```
Ethernet
   Filters
      sampleTOS
      Name = sampleTOS
      Input Filters...
         In filter 01
            Valid = Yes
            Type = IPTos
            IPTos...
               Src Mask = 0.0.0.0
Src Adrs = 0.0.0.0
Dst Mask = 255.255.255.255
Dst Adrs = 10.168.6.24
Protocol = 6
Src Port Cmp = None
Src Port # = 0
Dst Port Cmp = Eql
Dst Port # = 23
Precedence = 010
Type of service = Latency
```

Following is a RADIUS user profile that contains a comparable filter specification:

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

Note: Filter specifications cannot contain newlines. The above example shows the specification on two lines for printing purposes.

Applying TOS filters to WAN connections

For a Connection or RADIUS profile that has an applied TOS filter, the system sets bits in the TOS byte according to the filter specification.

Applying a filter to a Connection profile

You apply a TOS filter in a local Connection profile by specifying the number of the Filter profile in which it is defined. Following is the relevant parameter:

Parameter	Specifies
TOS-Filter	The number of a Filter profile that defines a TOS filter.

The following set of commands applies the TOS filter to a Connection profile. When the incoming data stream contains packets destined for 10.168.6.242, the proxy-QOS and TOS settings in the filter are set in those packets.

```
Ethernet
   Connections
      sampleProf
         IP options...
            TOS Filter = 01
```

Applying a TOS filter to a RADIUS profile

In a RADIUS profile, you can use one of the following attribute-value pairs to apply a TOS filter:

Attribute	Value
Ascend-Filter (91)	A string-format filter, which can include an IP TOS filter specification within a specific user profile.
Filter-ID (11)	Name of a local Filter profile that defines a TOS filter. The next time the MAX accesses the RADIUS user profile in which this attribute appears, the referenced TOS filter is applied to the connection.

For an example of defining a TOS filter in a user profile, see "Examples of defining a TOS filter" on page 10-60. The following profile uses the Filter-ID attribute to reference a local Filter profile:

```
sampleProf Password = "mypasswd", User-Service = Framed-User
    Framed-Protocol = PPP,
    Framed-IP-Address = 10.168.6.120
    Framed-IP-Netmask = 255.255.255.0
    Filter-ID = jfans-tos-filter
```

Configuring OSPF Routing

11

Introduction to OSPF

Open Shortest Path First (OSPF) is the next generation Internet routing protocol. The *Open* in its name refers to OSPF's development in the public domain as an open specification. *Shortest Path First* refers to an algorithm developed by Dijkstra in 1978 for building a self-rooted shortest-path tree from which routing tables can be derived. (This algorithm is described in "The link-state routing algorithm" on page 11-8.)

RIP limitations solved by OSPF

The rapid growth of the Internet has pushed Routing Information Protocol (RIP) beyond its capabilities, especially because of the following problems:

Problem	Description and solution
Distance-vector metrics	RIP is a distance-vector protocol, which uses a hop count to select the shortest route to a destination network. RIP always uses the lowest hop count, regardless of the speed or reliability of a link. OSPF is a link-state protocol, which means that OSPF can take into account a variety of link conditions, such as the reliability or speed of the link, and whether the link is up or down when determining the best path to a destination network.
15-hop limitation	With RIP, a destination that requires more than 15 consecutive hops is considered unreachable, which inhibits the maximum size of a network. OSPF has no hop limitation. You can add as many routers to a network as you want.

Problem	Description and solution
Excessive routing traffic and slow convergence	RIP creates a routing table and then propagates it throughout the internet of routers, hop by hop. *Convergence* is the time it takes for all routers to receive information about a topology change. Slow convergence can result in routing loops and errors. A RIP router broadcasts its entire routing table every 30 seconds. On a 15-hop network, convergence can be as high as 7.5 minutes. In addition, a large table can require multiple broadcasts for each update, which consumes a lot of bandwidth. OSPF uses a topological database of the network and propagates only changes to the database (as described in "Exchange of routing information" on page 11-4).

Ascend implementation of OSPF

The primary goal for Ascend's current implementation of OSPF is to enable the MAX to communicate with other routers within a single Autonomous System (AS).

The MAX acts as an OSPF internal router with limited border router capability. At this release, Ascend does not recommend an Area Border Router (ABR) configuration for the MAX, so the Ethernet interface and all of the MAX WAN links should be configured in the same area.

The MAX does not function as a full AS Border Router (ASBR) at this release. However, it performs ASBR calculations for external routes such as WAN links that do not support OSPF. The MAX imports external routes into its OSPF database and flags them as Autonomous System External (ASE). It redistributes those routes by means of OSPF ASE advertisements, and propagates its OSPF routes to remote WAN routers that are running RIP.

The MAX supports null and simple password authentication.

OSPF features

This section provides a brief overview of OSPF routing to help you properly configure the MAX. For full details about how OSPF works, see RFC 1583, *OSPF Version 2*, 03/23/1994, J. Moy.

An Autonomous System (AS) is a group of OSPF routers exchanging information, typically under the control of one company. An AS can include a large number of networks, all of which are assigned the same AS number. All information exchanged within the AS is *interior.*

Exterior protocols are used to exchange routing information between Autonomous Systems. The protocols are referred to by the acronym EGP (exterior gateway protocol). Border routers can use the AS number to filter out certain EGP routing information. OSPF can make use of EGP data generated by other border routers and added into the OSPF system as ASEs, and can also use static routes configured in the MAX or RADIUS.

Security

All OSPF protocol exchanges are authenticated. This means that only trusted routers can participate in the AS's routing. A variety of authentication schemes are available. In fact, different authentication types can be configured for each area. In addition, authentication provides added security for the routers that are on the network. Routers that do not have the password cannot gain access to the routing information, because authentication failure prevents a router from forming adjacencies.

Support for variable length subnet masks

OSPF enables the flexible configuration of IP subnets. Each route distributed by OSPF has a destination and mask. Two different subnets of the same IP network number can have different sizes (different masks). This capability is commonly referred to as Variable Length Subnet Masks (VLSM), or Classless Inter-Domain Routing (CIDR). The MAX routes a packet to the best (longest, or most specific) match. The MAX considers host routes to be subnets whose masks are all ones (0xFFFFFFFF).

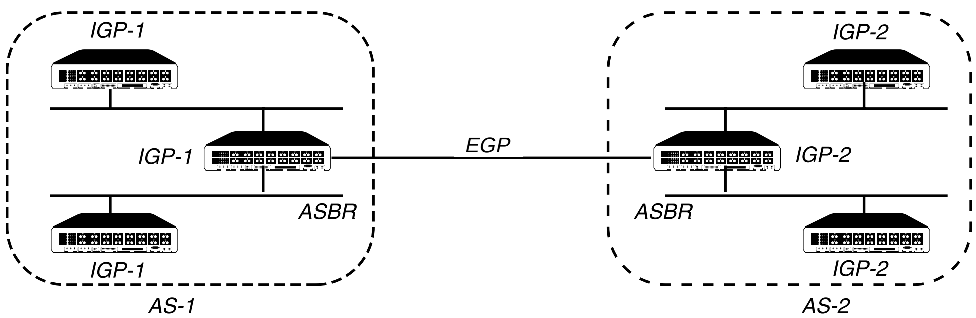
Note: Although OSPF is very useful for networks that use VLSM, Ascend recommends that you attempt to assign subnets as contiguously as possible, to prevent excessive link-state calculations by all OSPF routers on the network.

Interior gateway protocol (IGP)

OSPF keeps all AS-internal routing information within the AS. All information exchanged within the AS is *interior.*

The MAX requires an AS Border Router (ASBR) to use an external gateway protocol (EGP) for communicating with other autonomous systems, as shown in Figure 11-1. An EGP acts as a shuttle service between autonomous systems.

Figure 11-1. Autonomous system border routers



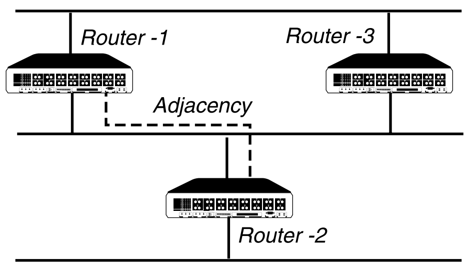
ASBRs perform calculations related to external routes. The MAX imports external routes from RIP (for example, when it establishes a WAN link with a caller that does not support OSPF) and always performs the ASBR calculations.

If you must prevent the MAX from performing ASBR calculations, you can disable them in Ethernet > Mod Config > OSPF Global Options.

Exchange of routing information

OSPF uses a topological database of the network and propagates only changes to the database. Part of the SPF algorithm involves acquiring neighbors and then forming an adjacency with one neighbor, see Figure 11-2.

Figure 11-2. Adjacency between neighboring routers



An OSPF router dynamically detects its neighboring routers by sending Hello packets to the multicast address `All SPFRouters`. It then attempts to form adjacencies with some of its newly acquired neighbors.

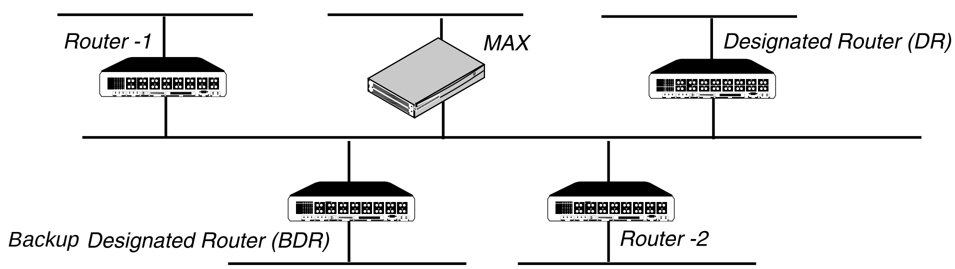
Adjacency is a relationship formed between selected neighboring routers for the purpose of exchanging routing information. Not every pair of neighboring routers becomes adjacent. Adjacencies are established during network initialization in pairs, between two neighbors. As the adjacency is established, the neighbors exchange databases and build a consistent, synchronized database between them.

When an OSPF router detects a change on one of its interfaces, it modifies its topological database and multicasts the change to its adjacent neighbor, which in turn propagates the change to its adjacent neighbor until all routers within an area have synchronized topological databases. The result is quick convergence among routers. OSPF routes can also be summarized in Link-State Advertisements (LSAs).

Designated and backup designated routers

In OSPF terminology, a broadcast network is any network that has more than two OSPF routers attached and that supports the capability to address a single physical message to all of the attached routers.

Figure 11-3. Designated and backup designated routers



The MAX can function as a Designated Router (DR) or Backup Designated Router (BDR). However, many sites choose to assign a LAN-based router for these roles in order to dedicate the MAX to WAN processing.

To reduce the number of adjacencies each router must form, OSPF calls one of the routers the designated router. A designated router is elected as routers are forming adjacencies, and then all other routers establish adjacencies only with the designated router. This simplifies the routing table update procedure and reduces the number of link-state records in the database. The designated router also plays other important roles in reduce the overhead of a OSPF link-state procedures. For example, other routers send link-state advertisements it to the designated router only by using the *all-designated-routers* multicast address of `All SPFRouters`.

To prevent the designated router from becoming a serious liability to the network if it fails, OSPF elects a backup designated router at the same time. Other routers maintain adjacencies with both the designated router and its backup router, but the backup router leaves as many of the processing tasks as possible to the designated router. If the designated router fails, the backup immediately becomes the designated router and a new backup is elected.

The administrator chooses which router is to be the designated router on the basis of the processing power, speed, and memory of the system, and then assigns priorities to other routers on the network in case the backup designated router is also down at the same time.

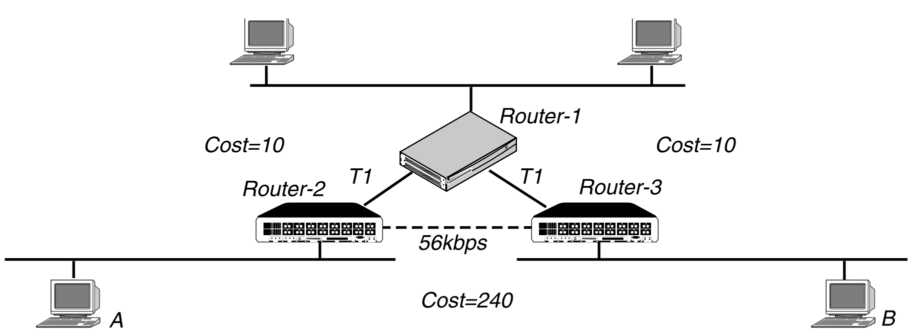
Configurable metrics

The administrator assigns a cost to the output side of each router interface. The lower the cost, the more likely the interface is to be used to forward data traffic. Costs can also be associated with the externally derived routing data.

You can also use the OSPF cost for preferred path selection. If two paths to a destination have equal costs, you can assign a higher cost to one of the paths, to configure it as a backup to be used only when the primary path is not available.

Figure 11-4 shows how costs direct traffic over high-speed links. For example, if Router-2 in Figure 11-4 receives packets destined for Host B, it routes them through Router-1, across two T1 links (Cost=20), rather than across one 56Kbps B-channel to Router-3 (Cost=240).

Figure 11-4. OSPF costs for different types of links



The MAX has a default cost of one for a connected route (Ethernet) and ten for a WAN link. If you have two paths to the same destination, the MAX selects the one with the lower cost. You might want to account for the bandwidth of a connection when assigning costs. For example, for a single B-channel connection, the cost would be 24 times greater than for a T1 link.

Note: Be careful when assigning costs. Incorrect cost metrics can cause delays and congestion on the network.

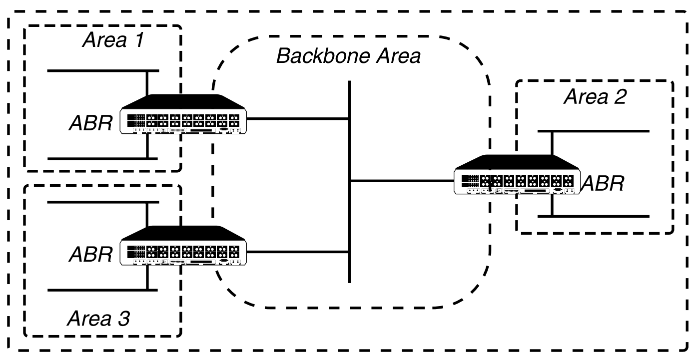
Hierarchical routing (areas)

If a network is large, the size of the database, time required for route computation, and related network traffic can become excessive. An administrator can partition an AS into areas to provide hierarchical routing connected by a backbone.

The backbone area is special and always has the area number 0.0.0.0. Other areas are assigned area numbers that are unique within the autonomous system.

Each areas acts like its own network. All area-specific routing information stays within the area, and all routers within an area must have a synchronized topological database. To tie the areas together, some routers belong to the backbone area and to another area. These routers are Area Border Routers (ABRs). In Figure 11-5, all of the routers are ABRs. If you set up the ABRs and area boundaries correctly, link-state databases are unique to an area.

Figure 11-5. Dividing an AS into areas



Note: At this release, Ascend recommends that you do not configure the MAX as an ABR. The current recommendation is that you use the same area number for the Ethernet interface of the MAX and each of its WAN links. That number does not have to be the backbone area number. The MAX can reside in any OSPF area.

Stub areas

To reduce the cost of routing, OSPF supports stub areas, in which a default route summarizes all external routes. For areas that are connected to the backbone by only one ABR (that is, the area has one exit point), there is no need to maintain information about external routes. Stub areas are similar to regular areas except that the routers do not enter external routes in the area's databases.

To prevent flooding of external routes throughout the AS, you can configure an area as a stub if the area has a single exit point or if the choice of exit point need not be made on a per-external-destination basis. You might need to specify a stub area with no default cost (StubNoDefault) if the area has more than one exit point.

In a stub area, routing to AS-external destinations is based on a per-area default cost. The per-area default cost is advertised to all routers within the stub area by a border router, and is used for all external destinations.

If the MAX supports external routes across its WAN links, you should not configure it in a stub area. Because an ABR configuration is not currently recommended for the MAX, the area in which it resides should not be a stub area if any of its links are AS-external.

Not So Stubby Areas (NSSAs)

The MAX supports OSPF Not So Stubby Areas (NSSAs) as described in RFC 1587. NSSAs enable you to treat complex networks similarly to stub areas. This can simplify your network's topology and reduce OSPF-related traffic.

NSSAs and Type-7 LSAs

NSSAs are similar to stub areas, except that they enable limited importing of AS-external routes. NSSAs use Type-7 LSAs to import external route information into an NSSA. Type-7 LSAs are similar to Type-5 LSAs except that:

- NSSAs can originate and import Type-7 LSAs; like stub areas, NSSAs cannot originate or import type-5 LSAs.
- Type-7 LSAs can only be advertised within a single NSSA; they are not flooded throughout the AS as are type-5 LSAs.

When you configure the MAX as an NSSA internal router, you define the Type-7 LSAs you want to advertise throughout the NSSA as static routes.

You must also specify whether these Type-7 LSAs should be advertised outside the NSSA. If you choose to advertise a Type-7 LSA, the NSSA Area Border Router (ABR) converts it to a Type-5 LSA, which can then be flooded throughout the AS. If you choose not to advertise a Type-7 LSA, it is not advertised beyond the NSSA.

(For complete information about NSSAs, see RFC 1587.)

Configuring the MAX as an NSSA internal router

Because the MAX cannot be an Area Border Router, when you configure OSPF on the MAX keep in mind that:

- The area-type must be the same on all MAX interfaces running OSPF.
- The area ID (configured in the Area parameter) must be the same on all MAX interfaces running OSPF.

To configure the MAX as an NSSA:

1 Select Ethernet > Mod Config > OSPF options.

2 Set AreaType to NSSA.

3 Exit and save the Mod Config profile.

4 Select Ethernet > Static Rtes > *any Static Route profile*.

5 Configure a static route to the destination outside the NSSA which include the following parameters (shown with sample settings):

```
Ethernet
     Static Rtes
     any Static Rtes profile
        Name=descriptivename
```

```
Active=Yes
Dest=20.20.20.20
Gateway=10.10.10.10
...

...
NSSA-ASE7=
```

Note: Set the NSSA-ASE7 parameter to Advertise or to DoNotAdvertise to specify whether you want to advertise this route outside the NSSA.

Configure the additional parameters to assign attributes to the route that are specific to your environment:

```
 Metric=
 Preference=
 Private=
 Ospf-Cost=
 LSA-type=
 ....
 ASE-tag=
Third-Party=
```

6 Exit and save the Static Rtes profile.

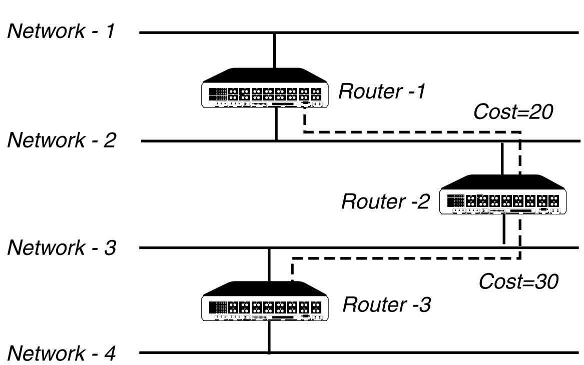
7 Reset the MAX.

The link-state routing algorithm

Link-state routing algorithms require that all routers within a domain maintain synchronized (identical) topological databases, and that the databases describe the complete topology of the domain. An OSPF router's domain can be an AS or an area within an AS.

OSPF routers exchange routing information and build link-state databases. Link-state databases are synchronized between pairs of adjacent routers (as described in "Exchange of routing information" on page 11-4). In addition, each OSPF router uses its link-state database to calculate a self-rooted tree of shortest paths to all destinations, as shown in Figure 11-6.

Figure 11-6. Sample network topology



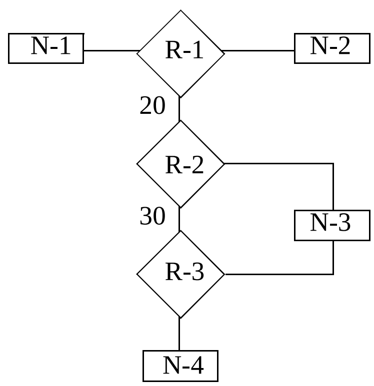
The routers then use the trees to build their routing tables, as shown in Table 11-1.

Table 11-1. Link state databases for network topology in Figure 11-6

Router-1	**Router-2**	**Router-3**
Network-1/Cost 0	Network-2/Cost0	Network-3/Cost 0
Network-2/Cost 0	Network-3/Cost0	Network-4/Cost 0
Router-2/Cost 20	Router-1/Cost 20	Router-2/Cost 30
	Router-3/Cost 30	

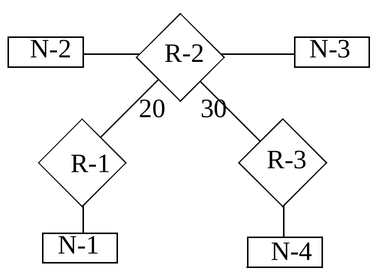
Table 11-2, Table 11-3, and Table 11-4 show another example of self-rooted shortest-path trees calculated from link-state databases, and the resulting routing tables. Actual routing tables also contain externally derived routing data, which is advertised throughout the AS but kept separate from the link-state data. Also, each external route can be tagged by the advertising router, enabling the passing of additional information between routers on the boundary of the AS.

Table 11-2. Shortest-path tree and resulting routing table for Router-1



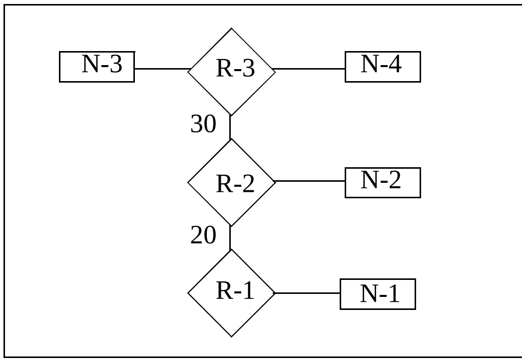
Destination	*Next Hop*	*Metric*
Network-1	Direct	0
Network-2	Direct	0
Network-3	Router-2	20
Network-4	Router-2	50

Table 11-3. Shortest-path tree and resulting routing table for Router-2



Destination	*Next Hop*	*Metric*
Network-1	Router-1	20
Network-2	Direct	0
Network-3	Direct	0
Network-4	Router-2	30

Table 11-4. Shortest-path tree and resulting routing table for Router-3



Destination	*Next Hop*	*Metric*
Network-1	Router-2	50
Network-2	Router-2	30
Network-3	Direct	0
Network-4	Direct	0

Configuring OSPF routing in the MAX

Following are the parameters related to OSPF routing in the MAX. (The settings shown are examples.)

```
Ethernet
   Mod Config
      OSPF options...
         RunOSPF=Yes
         Area=0.0.0.0
         AreaType=Normal
         HelloInterval=10
         DeadInterval=40
         Priority=5
         AuthType=Simple
         AuthKey=ascend0
         Cost=1
         ASE-type=N/A
         ASE-tag=N/A
         TransitDelay=1
         RetransmitInterval=5
      OSPF global options...
         Enable ASBR=Yes
Ethernet
   Connections
      OSPF options…
         RunOSPF=Yes
         Area=0.0.0.0
         AreaType=Normal
         HelloInterval=40
         DeadInterval=120
         Priority=5
         AuthType=Simple
         AuthKey=ascend0
         Cost=10
         ASE-type=N/A
         ASE-tag=N/A
         TransitDelay=5
         RetransmitInterval=20
```

```
Ethernet
   Static Rtes
      any Static Rtes profile…
         LSA-type=ExternalType1
```

Understanding the OSPF routing parameters

This section provides some background information about the OSPF parameters. (For detailed information about each parameter, see the *MAX Reference Guide*.)

Notice that the same configuration parameters appear in Ethernet > Mod Config > OSPF Options and Ethernet > Connections > OSPF Options. The parameters are the same, but some of the default values are different. For OSPF routing, you configure the following parameters:

Parameter	Description
RunOSPF	OSPF is turned off by default. To enable it on the interface, set RunOSPF to Yes.
Area	Sets the area ID for the interface. The format for this ID is dotted decimal, but it is not an IP address. (For a description of areas, see "Hierarchical routing (areas)" on page 11-6.)
AreaType	Specifies the type of area: Normal, Stub, or StubNoDefault. (For descriptions, see "Stub areas" on page 11-6.)
Intervals for communicating with an adjacent router	HelloInterval specifies how frequently, in seconds, the MAX sends out Hello packets on the specified interface. OSPF routers use Hello packets to dynamically detect neighboring routers in order to form adjacencies.
DeadInterval	Specifies how many seconds the MAX waits before declaring its neighboring routers down after it stops receiving their Hello packets. (For background information, see "Exchange of routing information" on page 11-4.)
Priority	Specifies a value the routers in the network use to elect a Designated Router (DR) and Backup Designated Router (BDR). Assigning a priority of 1 would place the MAX near the top of the list of possible designated routers. (Currently, you should assign a larger number.) Acting as a DR or BDR significantly increases the amount of OSPF overhead for the router. (For a discussion of the functions of DRs and BDRs, see "Designated and backup designated routers" on page 11-4.)
AuthType	Type of authentication supported. The Normal setting specifies that the MAX supports OSPF router authentication.
Auth Key	Specifies the key the MAX looks for in packets to support OSPF router authentication. (For more information, see "Security" on page 11-3.)

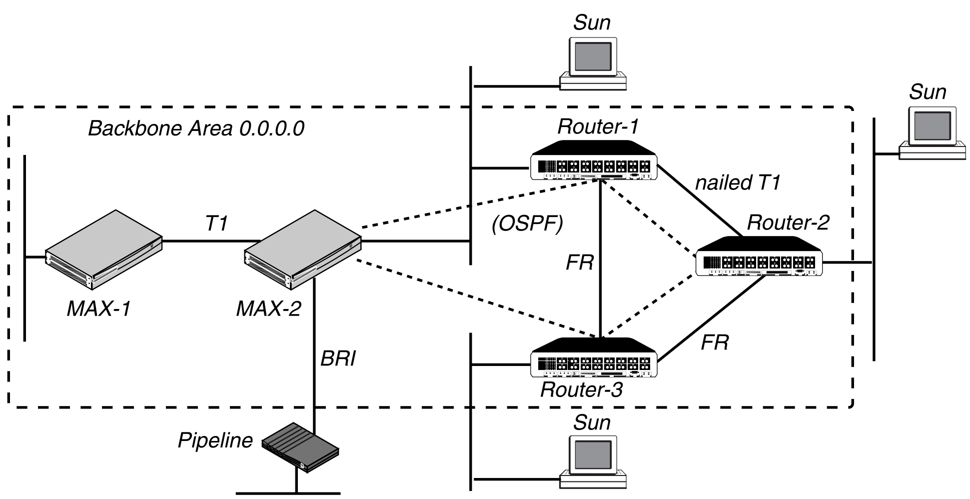
Parameter	Description
Cost	Specifies the link-state or output cost of a route. Assign realistic costs for each interface that supports OSPF. The lower the cost, the higher the likelihood of using that route to forward traffic. (For more information, see "Configurable metrics" on page 11-5.)
Autonomous System External (ASE) and their LSAs are used.	Autonomous System External routes only when OSPF is turned off on a particular interface. When OSPF is enabled, these parameters are not applicable.
ASE-Type ASE-Tag	ASE-Type specifies the type of metric that the MAX advertises for external routes. A Type-1 external metric is expressed in the same units as the link-state metric (the same units as interface cost). A Type-2 external metric is considered larger than any link- state path. Use of Type-2 external metrics assumes that routing between autonomous systems is the major cost of routing a packet, and eliminates the need for conversion of external costs to internal link-state metrics. ASE-Tag is a hexadecimal number used to tag external routes for filtering by other routers.
LSA-Type	Use LSAType to specify the OSPF ASE type of this link-state advertisement (LSA). Specify one of the following values: • ExternalType-1—A type-1 external metric is expressed in the same units as the link-state metric (the same units as interface cost). The default is Type-1. • ExternalType-2—Considered larger than any link state path. Use of type-2 external metrics assumes that routing between autonomous systems is the major cost of routing a packet, and eliminates the need for conversion of external costs to internal link-state metrics. • Internal—Indicates that this static route should be advertised in an internal LSA. The MAX advertises the static route only if the Static Route gateway has a corresponding entry in a Connection profile. When you set LSA-type to Internal, the internal LSA static route appears as a stub area to external OSPF routers.
TransitDelay	Specifies the estimated number of seconds it takes to transmit a Link State Update Packet over this interface, taking into account transmission and propagation delays. On a connected route, you can leave the default of 1.
RetransmitInterval	Specifies the number of seconds between retransmissions of Link-State Advertisements, Database Description, and Link State Request Packets.

Parameter	Description
Enable ASBR	In the OSPF Global Options submenu, you set this parameter to enable or disable Autonomous System Border Routers (ASBRs) perform calculations related to external routes. The MAX imports external routes from RIP (for example, when it establishes a WAN link with a caller that does not support OSPF) and performs the ASBR calculations. If you must prevent the MAX from performing ASBR calculations, set Ethernet > Mod Config > OSPF Global Options > Enable ASBR to No.

Examples of configurations for adding the MAX to an OSPF network

This section shows how to add a MAX to your OSPF network. It assumes that you know how to configure the MAX with an appropriate IP address, (as described in Chapter 10, “Configuring IP Routing.”) The procedures in this section are examples based on Figure 11-7. To apply one or more of the procedures to your network, enter the appropriate settings instead of the ones shown.

Figure 11-7. Example of an OSPF setup



In Figure 11-7, all OSPF routers are in the same area (the backbone area), so the units all form adjacencies and synchronize their databases together.

Note: All OSPF routers in Figure 11-7 have RIP turned off. OSPF can learn routes from RIP without the added overhead of running RIP.

Configuring OSPF on the Ethernet interface

The MAX Ethernet interface in Figure 11-7 is in the OSPF backbone area. Although there is no limitation stated in the RFC about the number of routers in the backbone area, you should keep the number of routers relatively small, because changes that occur in area zero are propagated throughout the AS.

Another way to configure the same units would be to create a second area (such as 0.0.0.1) in one of the existing OSPF routers, and add MAX-1 to that area. You could then assign the same area number (0.0.0.1) to all OSPF routers reached through the MAX across a WAN link.

After you configure MAX-1 as an IP host on that interface, you can configure it in the Ethernet profile as an OSPF router in the backbone area. To configure MAX-1 as an OSPF router on Ethernet:

1 Open Ethernet > Mod Config > Ether Options, and make sure the MAX is configured as an IP host. For example:

```
Ethernet
   Mod Config
      Ether options...
         IP Adrs=10.168.8.17/24
         2nd Adrs=0.0.0.0
         RIP=Off
         Ignore Def Rt=Yes
         Proxy Mode=Always
         Filter=0
         IPX Frame=N/A
```

Note that RIP is turned off, so it is not necessary to run both RIP and OSPF. Turning RIP off reduces processor overhead. OSPF can learn routes from RIP, incorporate them in the routing table, assign them an external metric, and tag them as external routes. (For more information, see Chapter 10, “Configuring IP Routing.”)

2 Open Ethernet > Mod Config > OSPF Options and turn on RunOSPF:

```
      OSPF options...
         RunOSPF=Yes
```

3 Specify the area number and area type for the Ethernet:

```
         Area=0.0.0.0
         AreaType=Normal
```

In this case, the Ethernet is in the backbone area. (The backbone area number is always 0.0.0.0.) The backbone area is not a stub area, so leave the setting at its default. (For background information, see “Stub areas” on page 11-6.)

4 Leave the HelloInterval, DeadInterval, and Priority values set to their defaults:

```
         HelloInterval=10
         DeadInterval=40
         Priority=5
```

5 If access to the backbone area requires authentication, specify the password. For example:

```
         AuthType=Simple
         AuthKey=ascend0
```

If authentication is not required, set AuthType=None.

6 Configure the cost for the MAX to route into the backbone area. For example:

```
         Cost=1
```

Then type a number greater than zero and less than 16777215. By default the cost of an Ethernet-connected route is 1.

7 Set the expected transit delay for Link State Update packets. For example:

```
         TransitDelay=1
```

8 Specify the retransmit interval for OSPF packets. For example:

```
RetransmitInterval=5
```

This parameter specifies the number of seconds between retransmissions of Link-State Advertisements, Database Description and Link State Request Packets.

9 Close the Ethernet profile.

When you close the Ethernet profile, the MAX comes up as an OSPF router on that interface. It forms adjacencies and begins building its routing table.

Configuring OSPF across the WAN

The WAN interface of the MAX is a point-to-point network. A point-to-point network is any network that joins a single pair of routers. Such networks typically do not provide a broadcasting or multicasting service, so all advertisements are sent point to point.

An OSPF WAN link has a default cost of ten. You can assign a higher cost to reflect a slower connection or a lower cost to set up a preferred route to a certain destination. If the cost of one route is lower than that of another to the same destination, the MAX does not select the higher-cost route unless route preferences change the equation.

OSPF on the WAN link is configured in a Connection profile. In this example, the MAX is connecting to another MAX unit across a T1 link (as in Figure 11-7 on page 11-13). To configure this interface:

1 Open the Connection profile for the remote MAX unit.

2 Turn on Route IP and configure the IP routing connection. For example:

```
Ethernet
   Connections
      IP options…
         LAN Adrs=10.2.3.4/24
         WAN Alias=0.0.0.0
         IF Adrs=0.0.0.0
         Metric=7
         Preference=N/A
         Private=No
         RIP=Off
        Pool=0
```

(For detailed information, see Chapter 10, “Configuring IP Routing.”)

3 Open Connections > OSPF Options and turn on RunOSPF.

```
OSPF options…
   RunOSPF=Yes
```

4 Specify the area number for the remote device and the area type.

The area number must always be specified in dotted-quad format similar to an IP address. For example:

```
Area=0.0.0.0
AreaType=Normal
```

You should use the same area number for the Ethernet interface of the MAX and each of its WAN links. In this example, the Ethernet interface is in the backbone area (0.0.0.0). You can use any area numbering scheme that is consistent throughout the AS and that uses this format.

5. Leave the HelloInterval, DeadInterval, and Priority values set to their defaults.

```
HelloInterval=40
DeadInterval=120
Priority=5
```

   Use the Priority value to configure the MAX as a DR or BDR.

6. If you require authentication to get into the backbone area, specify the password. For example:

```
AuthType=Simple
AuthKey=ascend0
```

   If you do not require authentication, set AuthType=None.

7. Configure the cost for the route to MAX-2.

   For example, for a T1 link the cost should be at least ten.

```
Cost=10
```

8. Close the Connection profile.

Of course, the remote MAX unit must also have a comparable Connection profile to connect to MAX-1.

Configuring a WAN link that does not support OSPF

In this example, the MAX has a Connection profile to a remote Pipeline unit across a BRI link (as in Figure 11-7 on page 11-13). The remote Pipeline is an IP router that uses RIP-v2 to transmit routes. The route to the Pipeline unit's network, and any routes the MAX learns about from the remote Pipeline, are ASEs (external to the OSPF system).

To enable OSPF to add the RIP-v2 routes to its routing table, configure RIP-v2 normally in this Connection profile. OSPF imports all RIP routes as Type-2 ASEs.

In this example, RIP is turned off on the link and ASE information is configured explicitly.

1. Open the Connection profile for the remote Pipeline unit.
2. Turn on Route IP and configure the IP routing connection. For example:

```
Ethernet
   Connections
     any Connection profile
       IP options…
         LAN Adrs=10.2.3.4/24
         WAN Alias=0.0.0.0
         IF Adrs=0.0.0.0
         Metric=7
         Preference=N/A
         Private=No
         RIP=Off
         Pool=0
```

   (For detailed information, see Chapter 10, "Configuring IP Routing.") Note that in a Connection profile, the OSPF Options subprofile includes two ASE parameters that are active only when OSPF is *not* running on a link. If you configure these parameters, the route configured in the Connection profile is advertised whenever the MAX is up.

3. Open the OSPF Options subprofile.

4 Leave RunOSPF set to No.

```
OSPF options…
   RunOSPF=No
```

5 Configure the cost for the route to the remote Pipeline.

For example, a single-channel BRI link could have a cost approximately 24 times the cost of a dedicated T1 link:

```
Cost=240
```

6 Specify the ASE type for this route.

```
ASE-type=Type 2
```

This parameter specifies the type of metric to be advertised for an external route.

A Type-1 external metric is expressed in the same units as the link state metric (the same units as interface cost). Type-1 is the default.

A Type-2 external metric is considered larger than any link-state path. Use of Type- 2 external metrics assumes that routing outside the AS is the major cost of routing a packet, and eliminates the need for conversion of external costs to internal link-state metrics.

7 Enter an ASE tag for this route.

The ASE tag is a hexadecimal number that shows up in management utilities and flags this route as external. It can also be used by border routers to filter this record. For example:

```
ASE-tag=cfff8000
```

8 Close the Connection profile.

Of course, the remote Pipeline unit must also have a comparable Connection profile to connect to the MAX.

Setting Up IP Multicast Forwarding

12

Configuring multicast forwarding

The multicast backbone (MBONE) is a virtual network layered on top of the Internet to support IP multicast routing across point-to-point links. It is used to transmit audio and video on the Internet in real time, because multicasting is a much cheaper and faster way to communicate the same information to multiple hosts.

When using the MBONE, the MAX looks like a multicast client. It responds as a client to Internet Group Membership Protocol (IGMP) packets it receives from MBONE routers. The packets can be IGMP version-1 or version-2, including IGMP multicast trace (MTRACE) packets.

To multicast clients on a WAN or Ethernet interface, the MAX looks like a multicast router. Like a router, it sends those clients IGMP queries, receives responses, and forwards multicast traffic. In this implementation, multicast clients are not allowed to source multicast packets. If they do, the MAX discards the packets.

Following are the parameters (shown with sample settings) for configuring multicast forwarding:

```
Ethernet
   Mod Config
      Multicast...
         Forwarding=Yes
         Membership Timeout=60
         Mbone Profile=
         Client=No
         Rate Limit=5
         Grp Leave Delay=
         HeartBeat Addr=224.0.1.1
         HeartBeat Udp Port=123
         HeartBeat Slot Time=10
         HeartBeat Slot Count=10
         Alarm threshold=3
         Source Addr=128.232.0.0
         Source Mask=0.0.0.0

Ethernet
   Connections
```

```
any Connection profile
   Ip options...
      Multicast Client=No
      Multicast Rate Limit=5
```

Understanding the multicast parameters

This section provides some background information about multicast parameters. For detailed information about each parameter, see the *MAX Reference Guide.*

Forwarding

The Forwarding parameter turns on multicast forwarding in the MAX.

When you change the Forwarding parameter from No to Yes, the multicast subsystem reads the values in the Ethernet profile and initiates the forwarding function.

Note: If you modify a multicast value in the Ethernet profile, you must set this parameter to No and then back to Yes again to force a read of the new value.

Membership Timeout

When you configure the Ascend unit as a multicast forwarder, it forwards polling messages generated by the multicast router and keeps track of active memberships from its client interfaces. To configure the timeout value for deactivating memberships, you can set the Membership Timeout parameter to a value from 60 seconds to 65535 seconds. The factory default is six minutes.

Mbone Profile

The multicast router resides in the MBONE interface. If it resides across the WAN, the Mbone Profile parameter must specify the name of a resident Connection profile to that router. If the Mbone Profile name is null and Multicast Forwarding is on, the MAX assumes that its Ethernet is the MBONE interface.

Client and Rate Limit

Each local or WAN interface that supports multicast clients must set the Client parameter to Yes (or set Multicast Client in each Client’s Connection profile to Yes). With this setting, the MAX begins handling IGMP requests and responses on the interface. It does not begin forwarding multicast traffic until you set the Rate Limit parameter.

Rate Limit specifies the rate at which the MAX accepts multicast packets from its clients. It does not affect the MBONE interface. The default setting is 100, which disables multicast forwarding on the interface. The forwarder handles IGMP packets, but does not accept packets from clients or forward multicast packets from the MBONE router.

To begin forwarding multicast traffic on the interface, you must set the Rate Limit parameter to a number less than 100. For example, if you set it to 5, the MAX accepts a packet from multicast clients on the interface once every five seconds. The MAX discards any subsequent packets received in that five-second window.

Grp Leave Delay

Because multiple multicast clients can have multiple active sessions for identical IGMP groups via a single WAN interface on the MAX, you can configure the MAX to query each WAN interface from which it receives a `leave group` message, to make sure there are no clients with active multicast sessions for the same group on that interface.

When the MAX receives a `leave group` message for a WAN interface for which you configure a value for Grp Leave Delay, it sends a query to the WAN interface, requesting that any active members of the group respond. If the MAX receives a response within the time period of time you specify in the Grp Leave Delay parameter, it does not forward the leave group message to the MBONE. Otherwise, it sends a `leave group` message to the MBONE, and it clears the IGMP group session from its tables.

HeartBeat

When running as a multicast forwarder, the MAX continually receives multicast traffic. The heartbeat-monitoring feature enables the administrator to monitor possible connectivity problems by continuously polling for this traffic and generating an SNMP alarm trap in the event of a traffic breakdown. Following is the SNMP alarm trap:

```
Trap type: TRAP_ENTERPRISE
Code: TRAP_MULTICAST_TREE_BROKEN (19)
Arguments:
1) Multicast group address being monitored (4 bytes),
2) Source address of last heartbeat packet received (4 bytes),
3) Slot time interval configured in seconds (4 bytes),
4) Number of slots configured (4 bytes).
5) Total number of heartbeat packets received before the MAX
started sending SNMP Alarms (4bytes).
```

Note: Heartbeat monitoring is optional. It is not required for multicast forwarding.

To set up heartbeat monitoring, you configure several parameters that define the packets to be monitored, how often and for how long to poll for multicast packets, and the threshold for generating an alarm. Following are the parameters you use to specify these settings:

Setting	Parameters
Packets to be monitored	HeartBeat Address specifies a multicast address. If set, causes the MAX to listen for packets to and from the specified address. HeartBeat UDP Port specifies a UDP port number. If set, causes the MAX to listen only to packets received through the specified port. Source Addr and Source Mask specify an IP address and subnet mask. If you specify an address, the MAX ignores packets from that source for monitoring purposes.
How often and for how long to poll for multicast packets	HeartBeat Slot Time specifies an interval (in seconds). The MAX polls for multicast traffic, waits for the duration of the interval, then polls again. HeartBeat Slot Count specifies how many times to poll before comparing the number of heartbeat packets received to the Alarm Threshold.

Setting	Parameters
Threshold for generating an alarm	Heartbeat Alarm Threshold specifies a number. If the number of monitored packets falls below this number, the MAX sends the SNMP alarm trap.

Multicast Client

The Multicast Client parameter enables the MAX to respond to multicast clients on the WAN link. Clients cannot be supported on the MBONE interface, so this means another WAN link or the local Ethernet supports a multicast router.

When you set Multicast Client to Yes, the MAX begins handling IGMP requests and responses on the interface. It does not begin forwarding multicast traffic until the rate limit is set. When you set Multicast Client to No, the MAX specifies that the MAX not respond to multicast clients on the interface. The default is No.

Multicast Rate Limit

The Multicast Rate Limit parameter specifies the rate at which the MAX accepts multicast packets from clients on this interface. It does not affect the MBONE interface.

Note: By default, the Rate Limit t parameter is set to 100, *which disables multicast forwarding on the interface.* The forwarder handles IGMP packets, but does not accept packets from clients or forward multicast packets from the MBONE router.

To begin forwarding multicast traffic on the interface, you must set the rate limit to a number less than 100. For example if you set it to 5, the MAX accepts a packet from multicast clients on the interface every 5 seconds. Any subsequent packets received in that 5-second window are discarded. You can specify a number lower than the default 100 to begin forwarding multicast traffic on the interface.

Implicit priority setting for dropping multicast packets

For high-bandwidth data, voice, and audio multicast applications, the MAX supports both multicast rate limiting (as described in “Client and Rate Limit” on page 12-2) and prioritized packet dropping. If the MAX is the receiving device under extremely high loads, it drops packets according to a priority ranking, which the following UDP port ranges determine:

- Traffic on ports 0–16384 (unclassified traffic) has the lowest priority (50).
- Traffic on ports 16385–32768 (Audio traffic) has the highest priority (70).
- Traffic on ports 32769–49152 (Whiteboard traffic) has medium priority (60).
- Traffic on ports 49153–65536 (Video traffic) has low priority (55).

Multicast interfaces

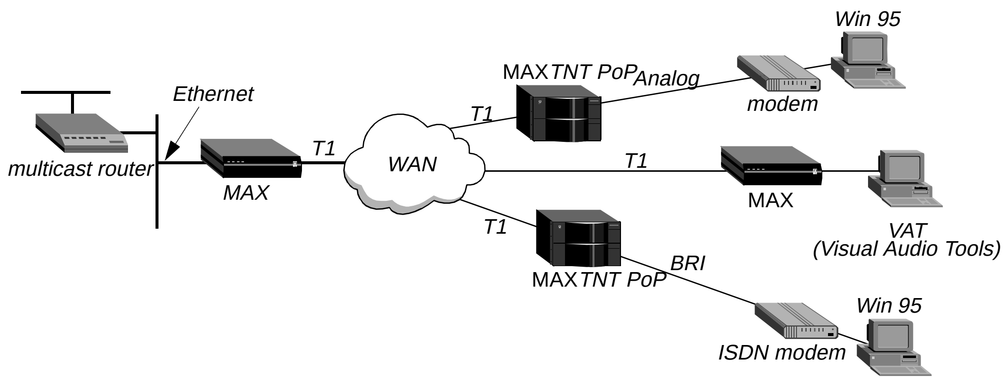
The MAX creates the following multicast interfaces at system startup:

Interface	Specified destination address
mcast	224.0.0.0/4 Multicast addresses, except for special addresses discussed in this section, are directed to this interface.
local	224.0.0.1/32 Multicast address for all systems on the local subnet. The MAX does not forward packets sent to this address.
local	224.0.0.2/32. Multicast address for all routers on the local subnet. The MAX does not forward packets sent to this address.
local	224.0.0.5/32. Multicast address for all OSPF routers on the network. The MAX does not forward packets sent to this address. If you disable OSPF routing, this route changes from local to a black-hole interface.
local	224.0.0.6/32. This local address is the multicast address for all OSPF designated routers on the network. The MAX does not forward packets sent to this address. If you disable OSPF routing, this route changes from local to a black-hole interface.

Forwarding from an MBONE router on Ethernet

Figure 12-1 shows a local multicast router on one of the MAX unit's Ethernet interfaces, and dial-in multicast clients.

Figure 12-1. MAX forwarding multicast traffic to dial-in multicast clients



Note: Heartbeat monitoring is an optional feature. You can operate multicast forwarding without it if you prefer.

As an example of this type of multicast configuration, the following procedure specifies the MBONE interface as the Ethernet port, and uses the heartbeat group address of 224.1.1.1:

1 Open Ethernet > Mod Config > Multicast.

2 Enable multicast forwarding, and leave the default values for the Mbone Profile, Client, and Rate Limit parameters:

```
Ethernet
   Mod Config
      Multicast...
         Forwarding=Yes
         Membership Timeout=60
         Mbone Profile=
         Client=No
         Rate Limit=5
```

3 Specify a heartbeat group address and UDP port for monitoring heartbeat packets. For example:

```
HeartBeat Addr=224.1.1.1
HeartBeat Udp Port=16387
```

4 Specify the time, count, and alarm threshold parameters. For example:

```
HeartBeat Slot Time=10
HeartBeat Slot Count=10
Alarm threshold=3
Source Addr=0.0.0.0
Source Mask=0.0.0.0
```

5 Close the Ethernet profile.

To enable multicasting on WAN interfaces:

1 Open the Connection profile for a multicast client site.

2 Open the IP Options subprofile and set Multicast Client to Yes. If appropriate, specify a rate limit other than the default of 5.

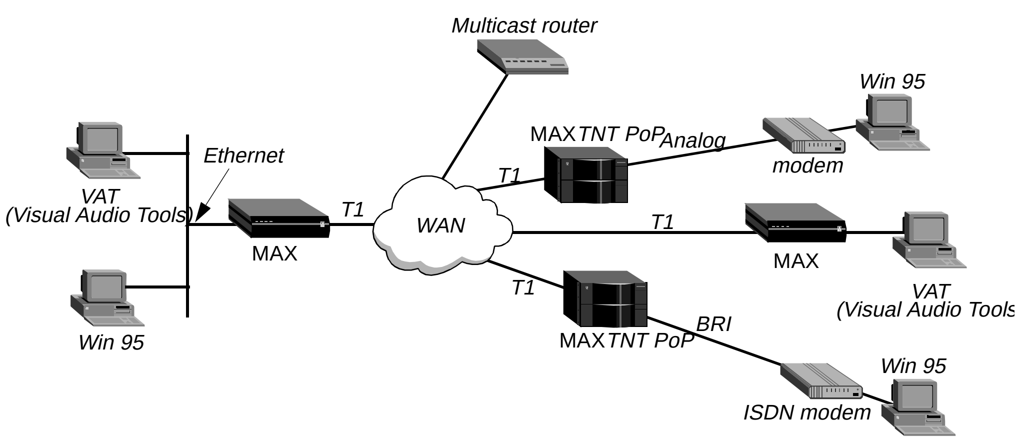
```
Ethernet
   Connections
     any Connection profile
        Ip options...
           Multicast Client=Yes
           Multicast Rate Limit=5
```

3 Close the Connection profile.

Forwarding from an MBONE router on a WAN link

Figure 12-2 shows a multicast router on the WAN with local and dial-in multicast clients.

Figure 12-2. MAX acting as a multicast forwarder on Ethernet and WAN interfaces



This section presents a sample configuration for the local MAX unit in Figure 12-2. The configuration specifies the MBONE interface as a WAN link accessed through a Connection profile #20.

Note: This example does not use heartbeat monitoring. If you want to configure the MAX for heartbeat monitoring, see the sample settings in "Forwarding from an MBONE router on Ethernet" on page 12-6.

Configuring the MAX to respond to multicast clients

To configure the MAX to respond to multicast clients on the Ethernet:

1 Open Ethernet > Mod Config > Multicast.

2 Enable multicast forwarding, specify the number of the Connection profile for the MBONE interface, and set Client to Yes:

```
Ethernet
   Mod Config
```

```
Multicast...
   Forwarding=Yes
   Membership Timeout=60
   Mbone Profile=20
   Client=Yes
```

3 In the same profile, set Multicast Rate Limit to a number lower than the default of 100:

```
Rate Limit=5
```

4 Close the Ethernet profile.

Configuring the MBONE interface

To configure the MBONE interface:

1 Open the Connection profile for an MBONE interface (in this example, profile #20).

2 Open the IP options subprofile and set Multicast Rate Limit to a number lower than the default of 100:

```
Ethernet
   Connections
      profile #20...
         Ip options...
            Multicast Client=No
            Multicast Rate Limit=5
```

3 Close the Connection profile.

Configuring multicasting on WAN interfaces

To enable multicasting on WAN interfaces:

1 Open the Connection profile for a multicast client site.

2 Open the IP options subprofile.

3 Set Multicast Client to Yes, and set Multicast Rate Limit to a number lower than the default of 100:

```
Ethernet
   Connections
     any Connection profile
        Ip options...
           Multicast Client=Yes
           Multicast Rate Limit=5
```

4 Close the Connection profile.

Setting Up Virtual Private Networks

13

Introduction to Virtual Private Networks

Virtual Private Networks (VPN) provide low-cost remote access to private LANs via the Internet. The tunnel to the private corporate network can be from an ISP, enabling Mobile Nodes to dial in to a corporate network, or it can provide a low-cost Internet connection between two corporate networks. Ascend currently supports these VPN schemes: Ascend Tunnel Management Protocol (ATMP), Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (L2TP).

An ATMP session can occur only between two Ascend units and must see UDP/IP. The MAX encapsulates all packets passing through the tunnel in standard Generic Routing Encapsulation as described in RFC 1701. ATMP creates and tears down a cross-Internet tunnel between the two Ascend units. In effect, the tunnel collapses the Internet cloud and provides what looks like direct access to a Home Network. The tunnels do not support bridging. All packets must be routed with IP or IPX.

The Microsoft Corporation developed Point-to-Point-Tunneling Protocol (PPTP) to enable Windows 95 and Windows NT Workstation users to dial into a local ISP to connect to a private corporate network across the Internet.

Version 8 of the Internet Engineering Task Force (IETF) draft titled *Layer Two Tunneling Protocol "L2TP,"* dated November, 1997, specifies the Layer 2 Tunneling Protocol (L2TP). L2TP enables you to connect to a private network by dialing into a local MAX, which creates and maintains an L2TP tunnel between itself and the private network.

Configuring ATMP tunnels

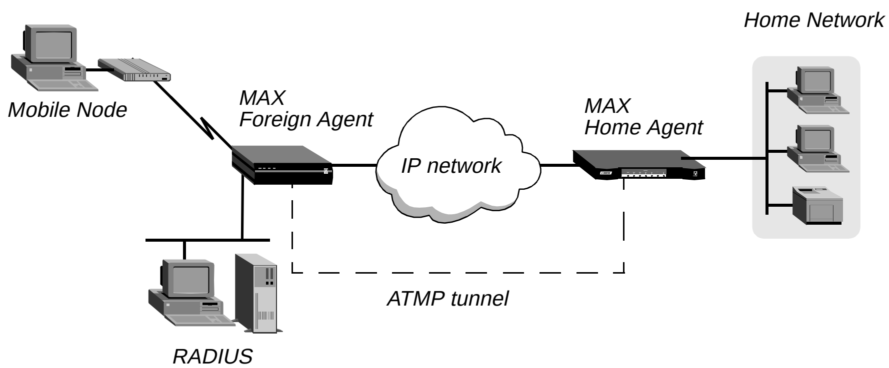
ATMP is a UDP/IP-based protocol for tunneling between two Ascend units across an IP network. Data is transported through the tunnel in Generic Routing Encapsulation (GRE), as described in RFC 1701. (For a complete description of ATMP, see RFC 2107, *Ascend Tunnel Management Protocol - ATMP.*)

This section describes how ATMP tunnels work between two MAX units. One of the units acts as a *Foreign Agent* (typically a local ISP) and one as a *Home Agent* (which can access the Home Network). A Mobile Node dials into the Foreign Agent, which establishes a cross-Internet IP connection to the Home Agent. The Foreign Agent then requests an ATMP tunnel on top of the IP connection. The Foreign Agent must use RADIUS to authenticate Mobile Nodes dial ins.

The Home Agent is the terminating part of the tunnel, and provides most of the ATMP intelligence. It must be able to communicate with the Home Network (the destination network for Mobile Nodes) through a direct connection, another router, or across a nailed connection.

For example, in Figure 13-1, the Mobile Node might be a sales person who logs into an ISP to access his or her Home Network. The ISP is the Foreign Agent. The Home Agent has access to the Home Network.

Figure 13-1. ATMP tunnel across the Internet



How the MAX creates ATMP tunnels

The MAX establishes an ATMP connection as follows:

1 A Mobile Node dials a connection to the Foreign Agent.

2 The Foreign Agent uses a RADIUS profile to authenticate the Mobile Node.

The MAX, configured as a Foreign Agent, requires RADIUS authentication of the Mobile Node, because only RADIUS supports the required attributes.

3 The Foreign Agent uses the Ascend-Home-Agent-IP-Addr attribute in the Mobile Node's RADIUS profile to locate a Connection profile (or RADIUS profile) for the Home Agent.

4 The Foreign Agent dials the Home Agent, and authenticates and establishes an IP connection in the usual way.

5 The Foreign Agent informs the Home Agent that the Mobile Node is connected, and requests a tunnel. The Foreign Agent sends up to 10 RegisterRequest messages at two-second intervals, timing out and logging a message if it receives no response to the requests.

6 The Home Agent requests a password before it creates the tunnel.

7 The Foreign Agent returns an encrypted version of the Ascend-Home-Agent-Password found in the Mobile Node's RADIUS profile. This password must match the Home Agent's Password parameter in the ATMP configuration in the Ethernet Profile.

8 The Home Agent returns a RegisterReply with a number that identifies the tunnel. If registration fails, the MAX logs a message and the Foreign Agent disconnects the Mobile Node. If registration succeeds, the MAX creates the tunnel between the Foreign Agent and the Home Agent.

9 When the Mobile Node disconnects from the Foreign Agent, the Foreign Agent sends a DeregisterRequest to the Home Agent to close the tunnel.

The Foreign Agent can send its request a maximum of ten times, or until it receives a DeregisterReply. If the Foreign Agent receives packets for a Mobile Node whose connection has been terminated, the Foreign Agent silently discards the packets.

Setting the UDP port

By default, ATMP agents use UDP port 5150 to exchange control information while establishing a tunnel. If the Home Agent ATMP profile specifies a different UDP port number, all tunnel requests to that Home Agent must specify the same UDP port.

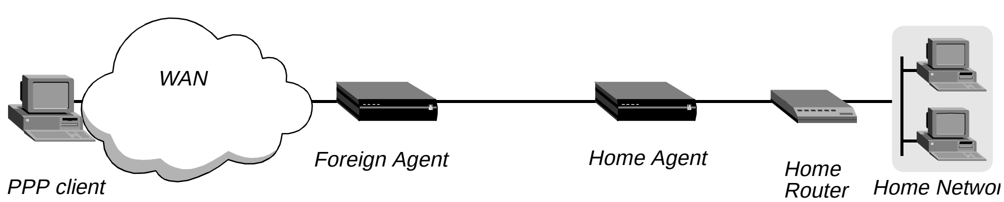
Note: A system reset is required for the ATMP subsystem to recognize the new UDP port number.

Setting an MTU limit

The type of link that connects a Foreign Agent and Home Agent determines the Maximum Transmission Unit (MTU). The link may be a dial-up connection, a Frame Relay connection, or an Ethernet link, and it may be a local network or routed through multiple hops. If the link between devices is multihop (if it traverses more than one network segment), the path MTU is the *minimum* MTU of the intervening segments.

Figure 13-2 shows an ATMP setup across an Ethernet segment, which limits the path MTU to 1500 bytes.

Figure 13-2. Path MTU on an Ethernet segment



If any segment of the link between the agents has an MTU smaller than 1528, some packet fragmentation and reassembly will occur. You can push fragmentation and reassembly tasks to connection end-points (a mobile client and a device on the home network) by setting an MTU limit. Client software then uses MTU discovery mechanisms to determine the maximum packet size, and then fragments packets before sending them.

How link compression affects the MTU

Compression affects which packets must be fragmented, because compressed packets are shorter than their original counterparts. If any kind of compression is on (such as VJ header or link compression), the connection can transfer larger packets without exceeding a link's Maximum Receive Unit (MRU). If compressing a packet makes it smaller than the MRU, it can be sent across the connection, whereas the same packet without compression could not.

How ATMP tunneling causes fragmentation

To transmit packets through an ATMP tunnel, the MAX adds an 8-byte GRE header and a 20-byte IP header to the frames it receives. The addition of these packet headers can make the packet larger than the MTU of the tunneled link, in which case the MAX must either fragment the packet after encapsulating it or reject the packet.

Fragmenting packets after encapsulating them has several disadvantages for the Foreign Agent and Home Agent. For example, it causes a performance degradation because both agents have extra overhead. It also means that the Home Agent device cannot be a GRF switch. (To maintain its very high aggregate throughput, a GRF switch does not perform reassembly.)

Pushing the fragmentation task to connection end-points

To avoid the extra overhead incurred when ATMP agents perform fragmentation, you can either set up a link between the two units that has an MTU greater than 1528 (which means it cannot include Ethernet segments), or you can set the Ethernet > Mod Config > ATMP > GRE MTU parameter to a value that is 28 bytes less than the path MTU.

If you set GRE MTU to zero (the default), the MAX might fragment encapsulated packets before transmission. The other ATMP agent must then reassemble the packets.

If you set GRE MTU to a nonzero value, the MAX reports that value to the client software as the path MTU, causing the client to send packets of the specified size. This pushes the task of fragmentation and reassembly out to the connection end-points, lowering the overhead on the ATMP agents.

For example, if the MAX is communicating with another ATMP agent across an Ethernet segment, you can set the GRE MTU parameter to a value 28 bytes smaller than 1500 bytes, as shown in the following example, to enable the unit to send full-size packets that include the 8-byte GRE header and a 20-byte IP header without fragmenting the packets first:

```
GRE MTU = 1472
```

With this setting, the connection end-point sends packets with a maximum size of 1472 bytes. When the MAX encapsulates them, adding 28 bytes to the size, the packets still do not violate the 1500-byte Ethernet MTU.

Forcing fragmentation for interoperation with outdated clients

To discover the path MTU, some clients normally send packets that are larger than the negotiated Maximum Receive Unit (MRU) and that have the Don't Fragment (DF) bit set. Such packets are returned to the client with an ICMP message informing the client that the host is unreachable without fragmentation. This standard, expected behavior improves end-to-end performance by enabling the connection end-points to perform any required fragmentation and reassembly.

However, some outdated client software does not handle this process correctly and continues to send packets that are larger than the specified GRE MTU. To enable the MAX to interoperate with these clients, you can configure the MAX to ignore the DF bit and perform the fragmentation that normally should be performed by the client software. This function in the MAX is sometimes referred to as *prefragmentation*.

When you set the GRE MTU parameter to a nonzero value, you can set the Force fragmentation parameter to Yes to enable the MAX to prefragment packets it receives that are larger than the negotiated MRU with the DF bit set. It prefragments those packets, and then adds the GRE and IP headers.

Note: Setting the Force fragmentation parameter to Yes causes the MAX to bypass the standard MTU discovery mechanism and fragment larger packets before encapsulating them in GRE. Because this changes expected behavior, it is not recommended except for ATMP interoperation with outdated client software that does not handle fragmentation properly.

Router and gateway mode

The Home Agent can communicate with the Home Network through a direct connection, through another router, or across a nailed connection. When the Home Agent relies on packet routing to reach the Home Network, it operates in router mode. When it has a nailed connection to the Home Network, it is in gateway mode.

Configuring the Foreign Agent

Following are the parameters (shown with sample settings) related to Foreign Agent configuration:

```
Ethernet
   Mod Config
      ATMP options...
         ATMP Mode=Foreign
         Type=N/A
         Password=N/A
         SAP Reply=N/A
         UDP Port=5150
         GRE MTU=1472
         Force fragmentation=No
         Idle limit=N/A
         ATMP SNMP Traps=No
```

Following are the parameters (shown with sample settings) for the IP routing connection to the Home Agent:

```
Ethernet
   Mod Config
      Ether options...
         IP Adrs=10.65.212.226/24

Ethernet
   Connections
    any Connection profile
      Station=name-of-home-agent
      Active=Yes
      Dial #=555-1212
      Route IP=Yes
      IP options...
         LAN Adrs=10.1.2.3/24
```

Following are the parameters (shown with sample settings) for using RADIUS authentication:

```
Ethernet
   Mod Config
      Auth...
         Auth=RADIUS
         Auth Host #1=10.23.45.11/24
         Auth Host #2=0.0.0.0/0
         Auth Host #3=0.0.0.0/0
         Auth Port=1645
         Auth Timeout=1
         Auth Key-=[]
         Auth Pool=No
         Auth Req=Yes
         Password Server=No
         Password Port=N/A
         Local Profile First=No
         Sess Timer=0
         Auth Src Port=0
         Auth Send Attr 6,7=Yes
```

Following are the parameters (shown with sample settings) for creating RADIUS user profiles for Mobile Nodes running TCP/IP:

```
node1 Password="top-secret"
   Ascend-Metric=2,
   Framed-Protocol=PPP,
   Ascend-IP-Route=Route-IP-Yes,
   Framed-Address=200.1.1.2,
   Framed-Netmask=255.255.255.0,
   Ascend-Primary-Home-Agent=10.1.2.3,
   Ascend-Home-Agent-Password="private"
   Ascend-Home-Agent-UDP-Port = 5150
```

Following are the parameters (shown with sample settings) for creating RADIUS user profiles for Mobile Nodes running NetWare:

```
node2 Password="ipx-unit"
   User-Service=Framed-User,
   Ascend-Route-IPX=Route-IPX-Yes,
   Framed-Protocol=PPP,
```

```
Ascend-IPX-Peer-Mode=IPX-Peer-Dialin,
Framed-IPX-Network=40000000,
Ascend-IPX-Node-Addr=123456789012,
Ascend-Primary-Home-Agent=10.1.2.3,
Ascend-Home-Agent-Password="private"
```

Understanding the Foreign Agent parameters and attributes

This section provides some background information about configuring a Foreign Agent to initiate an ATMP request to the Home Agent MAX. For detailed information about each parameter, see the *MAX Reference Guide*. For details about attributes and configuring external authentication, see the *MAX RADIUS Configuration Guide*.

Parameter(s)	**Usage**
ATMP Mode	For the Foreign Agent, the mode is Foreign which makes the Type, Password, and SAP Reply parameters not applicable.
UDP port	ATMP uses UDP port 5150 for ATMP messages between the foreign and Home Agents. If you specify a different UDP port number, make sure that the entire ATMP configuration agrees.
GRE MTU	Specifies the Maximum Transmission Unit (MTU) for the path between the Foreign and Home Agents as described in “Setting an MTU limit” on page 13-3.
ATMP SNMP Traps	Specifies that the MAX sends ATMP-related SNMP traps.
IP configuration and Connection profile parameters	The cross-Internet connection to the Home Agent is an IP routing connection that the MAX authenticates and establishes in the usual way. (For details, see Chapter 10, “Configuring IP Routing.”)
RADIUS authentication attributes	The Foreign Agent must use RADIUS to authenticate Mobile Nodes, and the RADIUS server must be running a version of the daemon that includes the ATMP attributes. (For details, see the *MAX RADIUS Configuration Guide*.)
RADIUS user-profile attributes	The RADIUS user profiles for Mobile Nodes must set ATMP attributes. The required attributes differ slightly, depending on whether the Mobile Node and Home Network run IP or IPX and whether the Home Agent MAX operates in router mode or gateway mode.

Table 13-1 lists the required attributes when the Mobile Node and Home Network are routing IP.

Table 13-1. Required RADIUS attributes to reach an IP Home Network

Home Agent in router mode	Home Agent in gateway mode
`Ascend-Primary-Home-Agent`	`Ascend-Primary-Home-Agent`
`Ascend-Home-Agent-Password`	`Ascend-Home-Agent-Password`
`Ascend-Home-Agent-UDP-Port`	`Ascend-Home-Agent-UDP-Port`
	`Ascend-Home-Network-Name`

Table 13-2 lists the required attributes when the Mobile Node and Home Network are routing IPX.

Table 13-2.Required RADIUS attributes to reach an IPX Home Network

Home Agent in router mode	Home Agent in gateway mode
`Ascend-IPX-Peer-Mode`	`Ascend-IPX-Peer-Mode`
`Framed-IPX-Network`	`Framed-IPX-Network`
`Ascend-IPX-Node-Addr`	`Ascend-IPX-Node-Addr`
`Ascend-Primary-Home-Agent`	`Ascend-Primary-Home-Agent`
`Ascend-Home-Agent-Password`	`Ascend-Home-Agent-Password`
`Ascend-Home-Agent-UDP-Port`	`Ascend-Home-Agent-UDP-Port`
	`Ascend-Home-Network-Name`

Following is a description of each Foreign Agent attribute:

Attribute	Description
`Ascend-Primary-Home-Agent`	IP address of the Home Agent, used to locate the Connection profile (or RADIUS profile) for the IP connection to the Home Agent.
`Ascend-Home-Agent-Password`	Used to authenticate the ATMP tunnel itself. Must match the password specified in the Home Agent’s Ethernet > Mod Config > ATMP Options subprofile. All Mobile Nodes use the *same* ATMP-Home-Agent-Password.
`Ascend-Home-Agent-UDP-Port`	Must match the UDP port configuration in Ethernet > Mod Config > ATMP Options. Required only for a port number other than the default 5150.

Attribute	Description
`Ascend-Home-Network-Name`	Name of the Home Agent's local Connection profile to the Home Network. Required only when the Home Agent is operating in gateway mode (when it has a nailed WAN link to the Home Network). For details, see "Configuring a Home Agent in gateway mode" on page 13-16.
`Ascend-IPX-Peer-Mode`	Dial-in NetWare clients must specify IPX-Peer-Dialin. This enables the Foreign Agent to handle RIP and SAP advertisements and assign the Mobile Node a virtual IPX network number.
`Framed-IPX-Network`	Virtual IPX network number. Assigned to dial-in NetWare clients (Mobile Nodes) to enable the Home Agent to route back to the Mobile Node. This IPX network number must be represented in decimal, not hexadecimal, and it must be unique in the IPX routing domain. (Note that you typically specify IPX network numbers in hexadecimal.) All Mobile Nodes logging into an IPX Home Network through the same Foreign Agent typically use the same virtual IPX network number.
`Ascend-IPX-Node-Addr`	Represents the Mobile Node on the virtual IPX network. Is represented as a 12-digit string that must be enclosed in double-quotes.

Example of configuring a Foreign Agent (IP)

To configure the Foreign Agent and create a Mobile Node profile to access a home IP network:

1 Open Ethernet > Mod Config > Ether Options and verify that the LAN interface has an IP address. For example:

```
Ethernet
   Mod Config
      Ether options...
         IP Adrs=10.65.212.226/24
```

2 Open the ATMP Options subprofile and set ATMP Mode to Foreign:

```
ATMP options...
   ATMP Mode=Foreign
   Type=N/A
   Password=N/A
   SAP Reply=N/A
   UDP Port=5150
```

3 Open the Auth subprofile and configure the Foreign Agent to authenticate through RADIUS. For example:

```
Auth...
   Auth=RADIUS
   Auth Host #1=10.23.45.11/24
   Auth Host #2=0.0.0.0/0
   Auth Host #3=0.0.0.0/0
   Auth Port=1645
```

```
Auth Timeout=1
Auth Key-=[]
Auth Pool=No
Auth Req=Yes
Password Server=No
Password Port=N/A
Local Profile First=No
Sess Timer=0
Auth Src Port=0
Auth Send Attr 6,7=Yes
```

For detailed information about each parameter, see the *MAX Reference Guide*.

4 Close the Ethernet profile.

5 Open a Connection profile and configure an IP routing connection to the Home Agent. For example:

```
Ethernet
   Connections
     any Connection profile
      Station=home-agent
      Active=Yes
      Encaps=MPP
      Dial #=555-1212
      Route IP=Yes

      Encaps options...
         Send Auth=CHAP
         Recv PW=home-pw
         Send PW=foreign-pw

      IP options...
         LAN Adrs=10.1.2.3/24
```

6 Close the Connection profile.

7 On the RADIUS server, open the RADIUS user profile and create an entry for a Mobile Node. For example:

```
node1 Password="top-secret"
   Ascend-Metric=2,
   Framed-Protocol=PPP,
   Ascend-IP-Route=Route-IP-Yes,
   Framed-Address=200.1.1.2,
   Framed-Netmask=255.255.255.0,
   Ascend-Primary-Home-Agent=10.1.2.3,
   Ascend-Home-Agent-Password="private"
   Ascend-Home-Agent-UDP-Port = 5150
```

8 Close the user profile.

When the Mobile Node logs into the Foreign Agent with the password *top secret*, the Foreign Agent uses RADIUS to authenticate the Mobile Node. It then looks for a profile with an IP address that matches the Ascend-Home-Agent-IP-Addr value, so that it can bring up an IP connection to the Home Agent.

Example of configuring a Foreign Agent (IPX)

The procedure for configuring a Foreign Agent to support IPX connections that use ATMP is very similar to one for IP. The only difference is in the Mobile Node's user profile as shown in the following example:

```
node2 Password="ipx-unit"
   User-Service=Framed-User,
   Ascend-Route-IPX=Route-IPX-Yes,
   Framed-Protocol=PPP,
   Ascend-IPX-Peer-Mode=IPX-Peer-Dialin,
   Framed-IPX-Network=40000000,
   Ascend-IPX-Node-Addr=123456789012,
   Ascend-Primary-Home-Agent=10.1.2.3,
   Ascend-Home-Agent-Password="private"
```

When the Mobile Node logs into the Foreign Agent with the password *ipx-uni*t, the Foreign Agent uses RADIUS to authenticate the Mobile Node. It then looks for a profile with an IP address that matches the Ascend-Home-Agent-IP-Addr value, so that it can bring up an IP connection to the Home Agent.

Configuring a Home agent

To configure an ATMP Home agent, you must set parameters in the ATMP profile, verify that the Home agent can communicate across an IP link with the Foreign agent, and configure the connection to the home network.

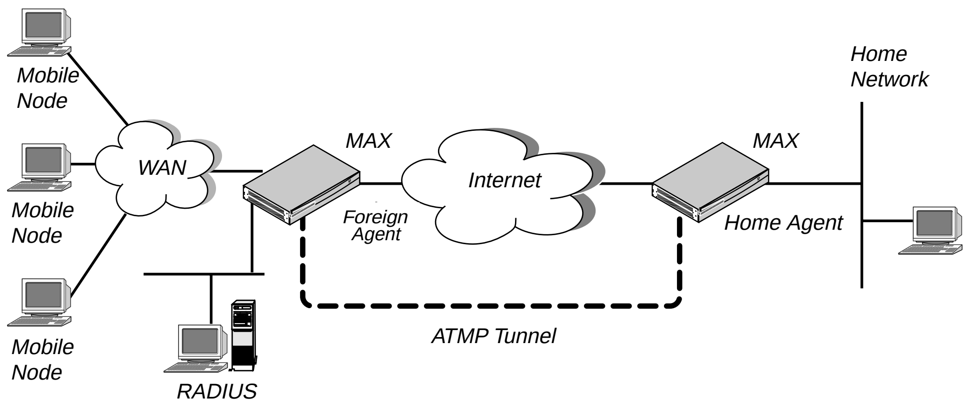
The link to the Foreign agent can be any kind of connection (dial-up, nailed, Frame Relay, etc.) or an Ethernet link, and it can be a local network or a remote network provided the two units communicate through an IP network.

Because the Home agent does not establish a connection on the basis of receiving tunneled data, the link to the home network cannot be a regular switched dial-up connection, but can be a nailed connection, a switched *incoming* connection from the home network, or a routed connection.

Configuring a Home Agent in router mode

When the ATMP tunnel has been established between the Home Agent and Foreign Agent, the Home Agent in router mode receives IP packets through the tunnel, removes the GRE encapsulation, and passes the packets to its bridge/router software. In its routing table, the Home Agent adds a host route to the Mobile Node.

Figure 13-3. Home Agent routing to the Home Network



The MAX requires the IPX routing parameters in the Ethernet profile only if the MAX is routing IPX. The following parameters (shown with sample settings) are used for configuring a Home Agent in router mode:

```
Ethernet
   Mod Config
      IPX Routing=Yes
      Ether options…
         IP Adrs=10.1.2.3/24
         IPX Frame=802.2
         IPX Enet #=00000000

      ATMP options...
         ATMP Mode=Home
         Type=Router
         Password=private
         SAP Reply=No
         UDP Port=5150
         GRE MTU=1472
         Force fragmentation=No
         Idle limit=0
         ATMP SNMP Traps=No
```

The IP routing connection to the Foreign Agent uses the following parameters (shown with sample settings):

```
Ethernet
   Connections
    any Connection profile
      Station=foreign-agent
      Active=Yes
      Encaps=MPP
      Dial #=555-1213
      Route IP=Yes

      Encaps options...
         Send Auth=CHAP
         Recv PW=foreign-pw
         Send PW=home-pw
```

```
IP options...
   LAN Adrs=10.65.212.226/24
```

Understanding the ATMP router mode parameters

This section provides some background information about configuring a Home Agent in router mode. For detailed information about each parameter, see the *MAX Reference Guide*.

.

Parameter	Usage
ATMP Mode	For the Home Agent, the mode is Home.
Type	When you set the ATMP Type to Router, the Home Agent relies on routing (not a WAN connection) to pass packets received through the tunnel to the Home Network.
Password	Used This is the password used to authenticate the ATMP tunnel itself. Must match the password specified in the Ascend-Home-Agent-Password attribute of each Mobile Node's RADIUS profile. (All Mobile Nodes use the same password for that attribute.)
SAP Reply	Enables a Home Agent to reply to the Mobile Node's IPX Nearest Server Query if it knows about a server on the Home Network. If the parameter is set to No, the Home Agent simply tunnels the Mobile Node's request to the Home Network.
UDP port	ATMP uses UDP port 5150 for ATMP messages between the foreign and Home Agents. If you specify a different UDP port number, make sure that the entire ATMP configuration agrees.
Idle limit	Specifies the number of minutes the Home Agent maintains an idle tunnel before disconnecting it.
GRE MTU	Specifies the Maximum Transmission Unit (MTU) for the path between the Foreign and Home Agents as described in "Setting an MTU limit" on page 13-3.
Force fragmentation	Enables/disables prefragmentation of packets that have the DF bit set, as described in "Forcing fragmentation for interoperation with outdated clients" on page 13-5.
IP configuration and Connection profile parameters	The cross-Internet connection to the Foreign Agent is an IP routing connection that the MAX authenticates and establishes in the usual way. (For details, see Chapter 10, "Configuring IP Routing.")

Routing to the Mobile Node

When the Home Agent receives IP packets through the ATMP tunnel, it adds a host route for the Mobile Node to its IP routing table. It then handles routing in the usual way. When the Home Agent receives IPX packets through the tunnel, it adds a route to the Mobile Node on the basis of the virtual IPX network number assigned in the RADIUS user profile.

For IP routes, you can enable RIP on the Home Agent's Ethernet to enable other hosts and networks to route to the Mobile Node. Enabling RIP is particularly useful if the Home Network is one or more hops away from the Home Agent's Ethernet. If you turn RIP off, other routers require static routes that specify the Home Agent as the route to the Mobile Node.

Note: If the Home Agent's Ethernet is the Home Network (a direct connection), you should turn on proxy ARP in the Home Agent so that local hosts can use ARP to find the Mobile Node.

For details on IP routes, see Chapter 10, "Configuring IP Routing.". For information about IPX routes, see "Configuring IPX Routing" on page 9-1.

Example of configuring a Home Agent in router mode (IP)

To configure the Home Agent in router mode to reach an IP Home Network:

1 Open Ethernet > Mod Config > Ether Options and verify that the LAN interface has an IP address. You can also set routing options. For example:

```
Ethernet
   Mod Config
      Ether options...
         IP Adrs=10.1.2.3/24
         RIP=On
```

2 Open the ATMP Options subprofile, set ATMP Mode to Home, and set Type to Router.

3 Specify the password used to authenticate the tunnel (Ascend-Home-Agent-Password). For example:

```
      ATMP options...
         ATMP Mode=Home
         Type=Router
         Password=private
         SAP Reply=No
         UDP Port=5150
         GRE MTU=1472
         Force fragmentation=No
         Idle limit=0
         ATMP SNMP Traps=No
```

4 Close the Ethernet profile.

5 Open a Connection profile and configure an IP routing connection to the Foreign Agent. For example:

```
Ethernet
   Connections
    any Connection profile
      Station=foreign-agent
      Active=Yes
      Encaps=MPP
      Dial #=555-1213
      Route IP=Yes

      Encaps options...
         Send Auth=CHAP
         Recv PW=foreign-pw
         Send PW=home-pw
```

```
      IP options...
         LAN Adrs=10.65.212.226/24
```

6 Close the Connection profile.

Example of configuring a Home Agent in router mode (IPX)

To configure the Home Agent in router mode to reach an IPX network:

1 Open Ethernet > Mod Config > Ether Options and verify that the LAN interface has an IP address (needed for communication with the Foreign Agent) and can route IPX.

```
Ethernet
   Mod Config
      IPX Routing=Yes
      Ether options…
         IP Adrs=10.1.2.3/24
         IPX Frame=802.2
         IPX Enet #=00000000
```

For details, see "Configuring IPX Routing" on page 9-1

2 Open the ATMP Options subprofile, set ATMP Mode to Home, and set Type to Router.

```
      ATMP options...
         ATMP Mode=Home
         Type=Router
```

3 Specify the password used to authenticate the tunnel (Ascend-Home-Agent-Password).

4 Set SAP Reply to Yes, and leave the default for UDP port:

```
         Password=private
         SAP Reply=Yes
         UDP Port=5150
```

5 Close the Ethernet profile.

6 Open a Connection profile and configure an IP routing connection to the Foreign Agent. For example:

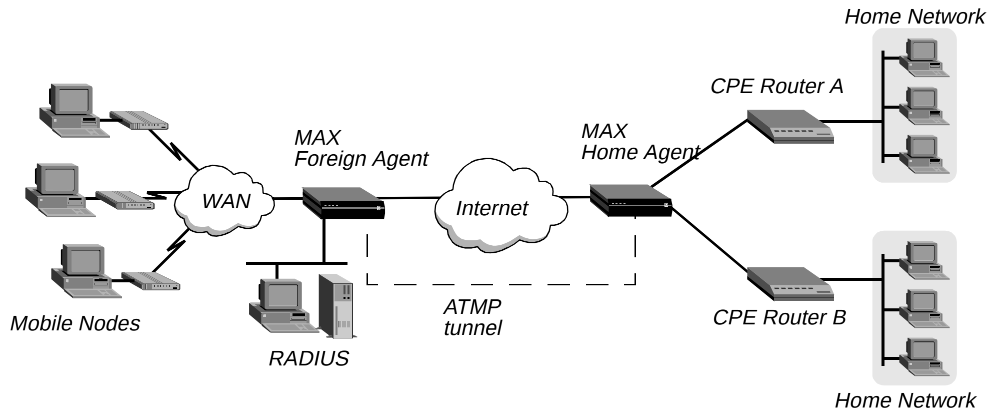
```
Ethernet
   Connections
    any Connection profile
      Station=foreign-agent
      Active=Yes
      Encaps=MPP
      Dial #=555-1213
     Route IP=Yes

      Encaps options...
         Send Auth=CHAP
         Recv PW=foreign-pw
        Send PW=home-pw

      IP options...
         LAN Adrs=10.65.212.226/24
```

7 Close the Connection profile.

Configuring a Home Agent in gateway mode

When you configure the Home Agent in gateway mode, it receives GRE-encapsulated IP packets from the Foreign Agent, strips off the encapsulation, and passes the packets across a nailed WAN connection to the Home Network.

Figure 13-4. Home Agent in gateway mode



Note: To enable hosts and routers on the Home Network to reach the Mobile Node, you must configure a static route in the Customer Premise Equipment (CPE) router on the Home Network (not in the Home Agent). The static route must specify the Home Agent as the route to the Mobile Node. That is, the route's destination address specifies the Framed-Address of the Mobile Node, and its gateway address specifies the IP address of the Home Agent.

Limiting the maximum number of tunnels

If you decide to limit the maximum number of tunnels a gateway will support, you should consider the expected traffic per mobile client connection, the bandwidth of the connection to the home network, and the availability of alternative Home Agents (if any). For example, the lower the amount of traffic generated by each mobile client connection, the more tunnels a a gateway connection will be able to handle.

Enabling RIP on the interface to the home router

The router at the far end of the gateway profile must be able to route back to mobile clients. The easiest way to accomplish this is by setting the ATMP RIP parameter to Send-v2. With this setting, the Gateway Home Agent constructs a RIP-v2 Response(2) packet at every RIP interval and sends it to the home network from all tunnels using the gateway profile. For each tunnel, the Response packet contains the mobile client IP address, the subnet mask, the next hop = 0.0.0.0, metric = 1. RIP-v2 authentication and route tags are not supported.

Note: The home network router should not send RIP updates, because the Home Agent does not inspect them. The RIP updates would be forwarded to the mobile clients instead.

If you set ATMP RIP to Off, the administrator of the home network must configure a static route to each mobile client. A static route to a mobile client can be specific to the client, where the route's destination is the mobile client IP address and the next-hop router is the Home Agent address. For example, in the following route the mobile client is a router (this is not a host route), and the Home Agent address is 2.2.2.2:

```
Dest=110.1.1.10/29
Gateway=2.2.2.2
```

Or, if the mobile clients have addresses allocated from the same address block (including router mobile client addresses with subnet masks less than 32 bits) and no addresses from that block are assigned to other hosts, the home network administrator can specify a single static route that encompass all mobile clients that use the same Home Agent. For example, in the following route all mobile clients are allocated addresses from the 10.4.*n.n* block (and no other hosts are allocated addresses from that block), and the Home Agent address is 2.2.2.2:

```
Dest=10.4.0.0/16
Gateway = 2.2.2.2
```

Configuring a Home Agent in gateway mode involves the following parameters (shown with sample settings):

```
Ethernet
   Mod Config
      IPX Routing=Yes
      Ether options…
         IP Adrs=10.1.2.3/24
         IPX Frame=802.2
         IPX Enet #=00000000

      ATMP options...
         ATMP Mode=Home
         Type=Gateway
         Password=private
         SAP Reply=No
         UDP Port=5150
         GRE MTU=1472
         Force fragmentation=No
         Idle limit=0
         ATMP SNMP Traps=No
```

The IP routing connection to the Foreign Agent uses the following parameters (shown with sample settings):

```
Ethernet
   Connections
    any Connection profile
      Station=foreign-agent
      Active=Yes
      Encaps=MPP
      Dial #=555-1213
      Route IP=Yes

      Encaps options...
         Send Auth=CHAP
         Recv PW=foreign-pw
         Send PW=home-pw
```

```
IP options...
   LAN Adrs=10.65.212.226/24
```

The nailed connection to the Home Network uses the following parameters (shown with sample settings):

```
Ethernet
   Connections
      Station=homenet
      Active=Yes
      Encaps=MPP
      Dial #=N/A
      Calling #=N/A
      Route IP=Yes
     Route IPX=Yes
      IP options...
         LAN Adrs=5.9.8.2/24
      Telco options...
         Call Type=Nailed
         Group=1,2
      Session options...
         ATMP Gateway=Yes
         MAX ATMP Tunnels=0
         ATMP RIP=Send-v2
```

The IPX routing parameters are required only if the MAX is routing IPX.

Understanding the ATMP gateway mode parameters

This section provides some background information about configuring a Home Agent in gateway mode. For detailed information about each parameter, see the *MAX Reference Guide*.

Set the following parameters in the Mod Config profile's ATMP Options subprofile:

Parameter	Usage
ATMP Mode	For the Home Agent, the mode is Home.
Type	When you set Type to Gateway, the Home Agent forwards packets received through the tunnel to the Home Network across a nailed WAN connection.
Password	Used to authenticate the ATMP tunnel itself. Must match the password specified in the Ascend-Home-Agent-Password attribute of each Mobile Node's RADIUS profile. (All Mobile Nodes use the same password for that attribute.)
SAP Reply	Enables a Home Agent to reply to the Mobile Node's IPX Nearest Server Query if it knows about a server on the Home Network. If the parameter is set to No, the Home Agent simply tunnels the Mobile Node's request to the Home Network.
UDP Port	ATMP uses UDP port 5150 for ATMP messages between the foreign and Home Agents. If you specify a different UDP port number, make sure that the entire ATMP configuration agrees.

Parameter	Usage
Idle limit	Specifies the number of minutes the Home Agent maintains an idle tunnel before disconnecting it.
GRE MTU	Specifies the Maximum Transmission Unit (MTU) for the path between the Foreign and Home Agents as described in "Setting an MTU limit" on page 13-3.
Force fragmentation	Enables/disables prefragmentation of packets that have the DF bit set, as described in "Forcing fragmentation for interoperation with outdated clients" on page 13-5.

IP configuration and Connection profile

The cross-Internet connection to the Foreign Agent is an IP routing connection that the MAX authenticates and establishes in the usual way. For details, see Chapter 10, "Configuring IP Routing."

Connection profile to the Home Network

The Connection profile to the Home Network must be a local profile. It cannot be specified in RADIUS. The name of this Connection profile must match the name specified by the Ascend-Home-Network-Name attribute in the Mobile Node's RADIUS profile. In addition, the Connection profile for connection to the Home Network must specify the following values:

- Nailed call type. The Home Agent must have a nailed connection to the Home Network, because it dials the WAN connection on the basis of packets received through the tunnel.
- ATMP Gateway session option enabled. The ATMP Gateway parameter must be set to Yes. This parameter instructs the Home Agent to send to the mobile node the data that it receives back from the Home Network on this connection.
- ATMP tunnel limit. The MAX ATMP Tunnels parameter specifies the number of ATMP tunnels that the MAX as a Home Agent gateway can establish to a Home Network. The maximum number of ATMP tunnels can be specified individually for each Home Network.

Also, you can specify that the MAX include mobile-client routes in RIP-v2 responses to the home router. The ATMP RIP parameter specifies whether or not the MAX includes mobile-client routes in RIP-v2 responses to the home router.

Example of configuring a Home Agent in gateway mode (IP)

To configure the Home Agent in gateway mode to reach an IP Home Network:

1 Open Ethernet > Mod Config > Ether Options and verify that the LAN interface has an IP address. For example:

```
Ethernet
   Mod Config
      Ether options...
         IP Adrs=10.1.2.3/24
```

2 Open the ATMP Options subprofile, set ATMP Mode to Home, and set Type to Gateway.

3 Specify the password used to authenticate the tunnel. It must match the Ascend-Home-Agent-Password attribute of each Mobile Node's RADIUS profile. For example:

```
ATMP options...
   ATMP Mode=Home
   Type=Gateway
   Password=private
   SAP Reply=No
   UDP Port=5150
   GRE MTU=1472
   Force fragmentation=No
   Idle limit=0
   ATMP SNMP Traps=No
```

4 Close the Ethernet profile.

5 Open a Connection profile and configure an IP routing connection to the Foreign Agent. For example:

```
Ethernet
   Connections
     any Connection profile
      Station=foreign-agent
      Active=Yes
      Encaps=MPP
      Dial #=555-1213
      Route IP=Yes

      Encaps options...
         Send Auth=CHAP
         Recv PW=foreign-pw
         Send PW=home-pw

      IP options...
         LAN Adrs=10.65.212.226/24
```

6 Open a Connection profile and configure a nailed WAN link to the Home Network. For example:

```
Ethernet
   Connections
     any Connection profile
      Station=homenet
      Active=Yes
      Encaps=MPP
      Dial #=N/A
      Calling #=N/A
      Route IP=Yes

      IP options...
         LAN Adrs=5.9.8.2/24

      Telco options...
         Call Type=Nailed
         Group=1,2

      Session options...
         ATMP Gateway=Yes
         MAX ATMP Tunnels=0
         ATMP RIP=Send-v2
```

7 Close the Connection profile.

Example of configuring a Home Agent in gateway mode (IPX)

To configure the Home Agent in gateway mode to reach an IPX Home Network:

1 Open Ethernet > Mod Config > Ether Options and verify that the LAN interface has an IP address (required for communication with the Foreign Agent) and can route IPX. For example:

```
Ethernet
   Mod Config
      IPX Routing=Yes
      Ether options…
         IP Adrs=10.1.2.3/24
         IPX Frame=802.2
         IPX Enet #=00000000
```

For details, see Chapter 10, "Configuring IP Routing."

2 Open the ATMP Options subprofile, set ATMP Mode to Home, and set Type to Gateway.

3 Specify the password used to authenticate the tunnel. It must match the Ascend-Home-Agent-Password attribute of each Mobile Node's RADIUS profile .

4 Set SAP Reply to Yes. The profile now has the following settings:

```
      ATMP options...
         ATMP Mode=Home
         Type=Gateway
         Password=private
         SAP Reply=Yes
         UDP Port=5150
         GRE MTU=1472
         Force fragmentation=No
         Idle limit=0
         ATMP SNMP Traps=No
```

5 Close the Ethernet profile.

6 Open a Connection profile and configure an IP routing connection to the Foreign Agent. For example:

```
Ethernet
   Connections
    any Connection profile
      Station=foreign-agent
      Active=Yes
      Encaps=MPP
      Dial #=555-1213
      Route IP=Yes

      Encaps options...
         Send Auth=CHAP
         Recv PW=foreign-pw
         Send PW=home-pw

      IP options...
         LAN Adrs=10.65.212.226/24
```

7 Open a Connection profile and configure a nailed WAN link that routes IPX to the Home Network. For example:

```
Ethernet
   Connections
    any Connection profile
         Station=homenet
         Active=Yes
         Encaps=MPP
         PRI # Type=National   (for ISDN PRI lines only)
         Dial #=555-1212
         Route IPX=Yes

         Encaps options...
            Send Auth=CHAP
            Recv PW=homenet-pw
            Send PW=my-pw

         IPX options...
            IPX RIP=None
            IPX SAP=Both
            NetWare t/o=30

         Telco options...
            Call Type=Nailed
            Group=1,2

         Session options...
            ATMP Gateway=Yes
            MAX ATMP Tunnels=0
            ATMP RIP=Send-v2
```

8 Close the Connection profile.

Specifying the tunnel password

The Home Agent typically requests a password before establishing a tunnel. The Foreign Agent returns an encrypted version of the password found in the mobile client profile.

If the password sent by the Foreign Agent matches the Password value specified in the ATMP profile, the Home Agent returns a RegisterReply with a number that identifies the tunnel, and the mobile client's tunnel is established. If the password does not match, the Home Agent rejects the tunnel, and the Foreign Agent logs a message and disconnects the mobile client.

Setting an idle timer for unused tunnels

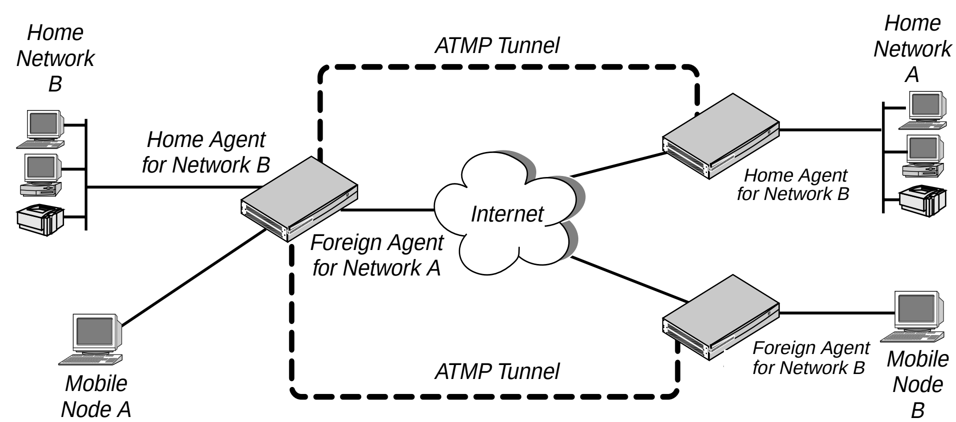
When a mobile client disconnects normally, the Foreign Agent sends a request to the Home Agent to close down the tunnel. However, when a Foreign Agent restarts, tunnels that were established to a Home Agent are not normally cleared, because the Home Agent is not informed that the mobile clients are no longer connected. The unused tunnels continue to hold memory on the Home Agent. To enable the Home Agent to reclaim the memory held by unused tunnels, set an inactivity timer on a Home Agent by changing the Idle limit parameter to a non-zero value.

The inactivity timer runs only on the Home Agent side and specifies the number of minutes (1 to 65535) that the Home Agent maintains an idle tunnel before disconnecting it. A value of 0 disables the timer, which means that idle tunnels remain connected forever. The setting affects only tunnels created after the timer was set. Tunnels that existed before the timer was set are not affected by it.

Configuring the MAX as an ATMP multimode agent

You can configure the MAX to act as both a Home Agent and Foreign Agent on a tunnel-by-tunnel basis. Figure 13-5 shows a sample network topology that has a MAX acting as a Home Agent for Network B and a Foreign Agent for Network A.

Figure 13-5. MAX acting as both Home Agent and Foreign Agent



To configure the MAX as a multimode agent, set ATMP Mode to Both and complete both the foreign and Home Agent specifications. Setting ATMP Mode to Both indicates that the MAX will function as both a Home Agent and Foreign Agent on a tunnel-by-tunnel basis.

For example, to configure the MAX to operate as both a Home Agent and Foreign Agent, first check the interface and set the ATMP options:

1 Open Ethernet > Mod Config > Ether Options and verify that the LAN interface has an IP address. For example:

```
Ethernet
   Mod Config
      Ether options...
         IP Adrs=10.65.212.226/24
```

2 Open the ATMP Options subprofile and set ATMP Mode to Both.

3 Configure the other home-agent settings as appropriate. For example, to use Gateway mode and a password of *private*:

```
ATMP options...
   ATMP Mode=Both
   Type=Gateway
   Password=private
   SAP Reply=No
   UDP Port=5150
   GRE MTU=1472
   Force fragmentation=No
   Idle limit=0
   ATMP SNMP Traps=No
```

Then set the Foreign Agent aspect of the multimode configuration:

1 Open the Auth subprofile and configure RADIUS authentication. For example:

```
Auth...
   Auth=RADIUS
   Auth Host #1=10.23.45.11/24
   Auth Host #2=0.0.0.0/0
   Auth Host #3=0.0.0.0/0
   Auth Port=1645
   Auth Timeout=1
   Auth Key-=[]
   Auth Pool=No
   Auth Req=Yes
   Password Server=No
   Password Port=N/A
   Local Profile First=No
   Sess Timer=0
   Auth Src Port=0
   Auth Send Attr 6,7=Yes
```

For detailed information about each parameter, see the *MAX Reference Guide*.

2 Close the Ethernet profile.

3 On the RADIUS server, open the RADIUS user profile and create an entry for a Mobile Node. For example:

```
node1 Password="top-secret"
   Ascend-Metric=2,
   Framed-Protocol=PPP,
   Ascend-IP-Route=Route-IP-Yes,
   Framed-Address=200.1.1.2,
   Framed-Netmask=255.255.255.0,
   Ascend-Primary-Home-Agent=10.1.2.3,
   Ascend-Home-Agent-Password="private"
   Ascend-Home-Agent-UDP-Port = 5150
   Ascend-Home-Network-Name=home-agent
```

4 Close the user profile.

5 Open a Connection profile and configure an IP routing connection to the Network A Home Agent. For example:

```
Ethernet
   Connections
     any Connection profile
      Station=home-agent
      Active=Yes
      Encaps=MPP
      Dial #=555-1212
      Route IP=Yes

      Encaps options...
         Send Auth=CHAP
         Recv PW=home-pw
         Send PW=foreign-pw

      IP options...
         LAN Adrs=10.1.2.3/24
```

6 Close the Connection profile.

Finally, set the Home Agent aspect of the multimode configuration:

1 Open a Connection profile and configure an IP routing connection to the Network B Foreign Agent. For example:

```
Ethernet
   Connections
    any Connection profile
      Station=foreign-agent
      Active=Yes
      Encaps=MPP
      Dial #=555-1213
      Route IP=Yes

      Encaps options...
         Send Auth=CHAP
         Recv PW=foreign-pw
         Send PW=home-pw

      IP options...
         LAN Adrs=10.65.212.226/24
```

2 Open a Connection profile and configure a nailed WAN link to the Network B Home Network. For example:

```
Ethernet
   Connections
    any Connection profile
      Station=homenet
      Active=Yes
      Encaps=MPP
      Dial #=N/A
      Calling #=N/A
      Route IP=Yes

      IP options...
         LAN Adrs=5.9.8.2/24

      Telco options...
         Call Type=Nailed
         Group=1,2

      Session options...
         ATMP Gateway=Yes
         MAX ATMP Tunnels=0
         ATMP RIP=Send-v2
```

3 Close the Connection profile.

Supporting Mobile Node routers (IP only)

To enable an IP router to connect as a Mobile Node, the Foreign Agent's RADIUS entry for the Mobile Node must specify *the same subnet as the one that identifies the Home Network*. For example, to connect to a Home Network whose router has the following address:

```
10.1.2.3/28
```

The Foreign Agent's RADIUS entry for the remote router would contain lines such as the following:

```
node1 Password="top-secret"
   Ascend-Metric=2,
   Framed-Protocol=PPP,
   Ascend-IP-Route=Route-IP-Yes,
   Framed-Address=10.168.6.21,
   Framed-Netmask=255.255.255.240,
   Ascend-Primary-Home-Agent=10.1.2.3,
   Ascend-Home-Agent-Password="private"
```

With these Framed-Address and Framed-Netmask settings (equivalent to 10.168.6.21/28) for the Mobile Node router, the connecting LAN can support up to 14 hosts. The network address (or base address) for this subnet is 10.168.6.16. This address represents the network itself, because the host portion of the IP address is all zeros.

The broadcast address (all ones in host portion of address) for this subnet is 10.168.6.31. Therefore, the valid host address range is 10.168.6.17—10.168.6.30, which includes 14 host addresses.

The MAX handles routes to and from the Mobile Node's LAN differently, depending on whether the Home Agent is configured in router mode or gateway mode.

Home Agent in router mode

If the Home Agent connects directly to the Home Network, set Proxy ARP=Always, which enables the Home Agent to respond to ARP requests on behalf of the Mobile Node.

If the Home Agent does not directly connect to the Home Network, the situation is the same as for any remote network: Routes to the Mobile Node's LAN must either be learned dynamically from a routing protocol or configured statically.

The Mobile Node always requires static routes to the Home Agent as well as to other networks reached through the Home Agent. (It cannot learn routes from the Home Agent.)

Home Agent in gateway mode

If the Home Agent forwards packets from the Mobile Node across a nailed WAN link to the home IP network, the answering unit on the Home Network must have a static route to the Mobile Node's LAN.

In addition, because no routing information passes through the connection between the Mobile Node and the Home Agent, the Mobile Node's LAN can only support local subnets that fall within the network specified in the RADIUS entry.

For example, using the previous sample RADIUS entry, the Mobile Node could support two subnets with a mask of 255.255.255.248: one on the 10.168.6.16 subnet and the other on the 10.168.6.24 subnet. The answering unit on the Home Network would have only one route to the router itself (10.168.6.21/28).

ATMP connections that bypass a Foreign Agent

If a Home Agent MAX has the appropriate RADIUS entry for a Mobile Node, the Mobile Node connects directly to the Home Agent. An ATMP-based RADIUS entry that is local to the Home Agent enables the Mobile Node to bypass a Foreign Agent connection, but it does not preclude a Foreign Agent. If both the Home Agent and the Foreign Agent have local RADIUS entries for the Mobile Node, the node can choose a direct connection or a tunneled connection through the Foreign Agent.

For example, the following RADIUS entry authenticates a mobile NetWare client that connects directly to the Home Agent. In this example, the Home Agent is in the gateway mode (it forwards packets from the Mobile Node across a nailed WAN link to the home IPX network):

```
mobile-ipx Password = "unit"
   User-Service = Framed-User,
   Ascend-Route-IPX = Route-IPX-Yes,
   Framed-Protocol = PPP,
   Ascend-IPX-Peer-Mode = IPX-Peer-Dialin,
   Framed-IPX-Network = 40000000,
   Ascend-IPX-Node-Addr = 12345678,
   Ascend-Home-Agent-IP-Addr = 192.168.6.18,
   Ascend-Home-Network-Name = "homenet",
   Ascend-Home-Agent-Password = "pipeline"
```

Note: If you configure the Home Agent in router mode (which forwards packets from the Mobile Node to its internal routing module), the Ascend-Home-Network-Name line is not included in the user entry. The Ascend-Home-Network-Name attribute specifies the name of the answering unit across the WAN on the home IPX network.

Configuring PPTP tunnels for dial-in clients

Point to Point Tunneling Protocol (PPTP) enables Windows 95 and Windows NT Workstation users to dial into a local ISP to connect to a private corporate network across the Internet. To the user dialing the call, the connection looks like a regular login to an NT server that supports TCP/IP, IPX, or other protocols.

The MAX acts as a PPTP Access Controller (PAC) which functions as a front-end processor to offload the overhead of communications processing. At the other end of the tunnel, the NT server acts as a PPTP Network Server (PNS). All authentication is negotiated between the Windows 95 or NT client and the PNS. The NT server's account information remains the same as if the client dialed in directly. No changes are needed.

How the MAX works as a PAC

Currently, PPTP supports call routing and routing to the NT server by PPP-authenticated connection on a per-line basis, or on the basis of the called number or calling number. The following section describes how to dedicate an entire WAN access line for each destination PNS address. For details about configuring WAN lines and assigning phone numbers, see Chapter 2, "Configuring the MAX for WAN Access." For details about routing PPTP calls on the basis of called or calling number, see the *MAX RADIUS Configuration Guide*.

In the PPTP configuration, you specify the destination IP address of the PNS (the NT server), to which all calls that come in on the PPTP-routed line will be forwarded. When the MAX receives a call on that line, it passes the call directly to the specified IP address end-point, creating the PPTP tunnel to that address if one is not already up. The PNS destination IP address must be accessible by IP routing.

Note: The MAX handles PPTP calls differently than it does regular calls. No Connection profiles are used for these calls, and the Answer profile is not consulted. The calls are routed through the PPTP tunnel solely on the basis of the phone number dialed.

Following are the PPTP PAC configuration parameters (shown with sample settings):

```
Ethernet
   Mod Config
      L2 Tunneling Options...
         PPTP Enabled=Yes
         Line 1 tunnel type=PPTP
         Route line 1=10.65.212.11
         Line 2 tunnel type=None
         Route line 2=0.0.0.0
         Line 3 tunnel type=None
         Route line 3=0.0.0.0
         Line 4 tunnel type=None
         Route line 4=0.0.0.0
```

Understanding the PPTP PAC parameters

This section provides some background information about configuring PPTP. For detailed information about each parameter, see the *MAX Reference Guide*.

Enabling PPTP

When you enable PPTP, the MAX can bring up a PPTP tunnel with a PNS and respond to a request for a PPTP tunnel from a PNS. You must specify the IP address of the PNS in one or more of the Route Line parameters.

Specifying a PRI line for PPTP calls and the PNS IP address

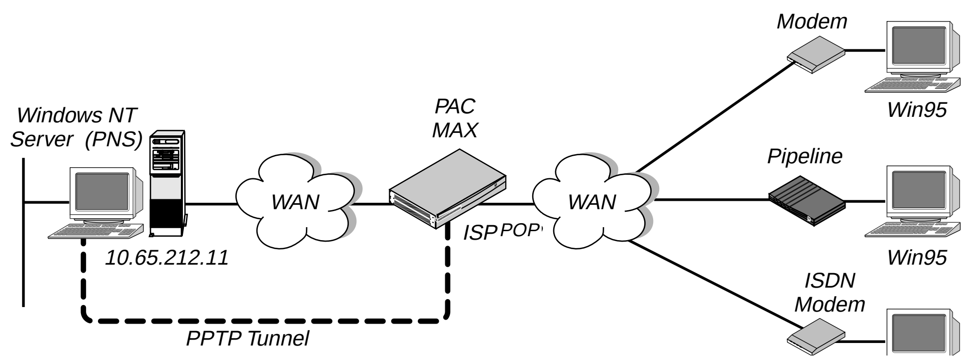
The PPTP parameters include four Route Line parameters, one for each of the MAX unit's WAN lines. If you specify the IP address of a PNS in one of these parameters, that WAN line is dedicated to receiving PPTP connections and forwarding them to that destination address.

The IP address you specify must be accessible via IP, but there are no other restrictions on it. It can be across the WAN or on the local network. If you leave the default null address, that WAN line handles calls normally.

Example of a PAC configuration

Figure 13-6 shows an ISP POP MAX unit communicating across the WAN with an NT Server at a customer premise. Windows 95 or NT clients dial into the local ISP and are routed directly across the Internet to the corporate server. In this example, the MAX unit's fourth WAN line is dedicated to PPTP connections to that server.

Figure 13-6. PPTP tunnel



To configure this MAX for PPTP:

1 Open Ethernet > Mod Config > PPTP Options.

2 Turn on PPTP, and set Route Line 4 to the PNS IP address.

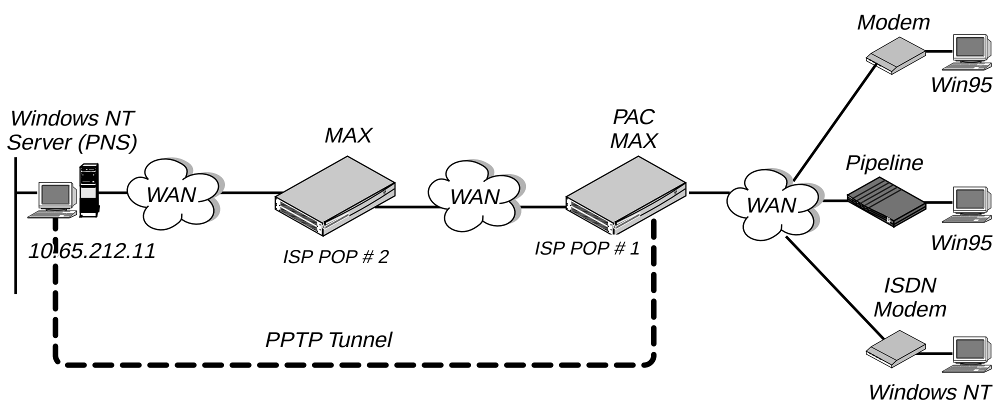
```
Ethernet
   Mod Config
      L2 Tunneling Options...
         PPTP Enabled=Yes
         Line 1 tunnel type=None
         Route line 1=0.0.0.0
         Line 2 tunnel type=None
         Route line 2=0.0.0.0
         Line 3 tunnel type=None
         Route line 3=0.0.0.0
         Line 4 tunnel type=PPTP
         Route line 4=10.65.212.11
```

3 Close the Ethernet Profile.

Example of a PPTP tunnel across multiple POPs

Figure 13-7 shows an ISP POP MAX communicating through an intervening router to the PNS that is the end-point of its PPTP tunnel. The MAX routes the packets in the usual way to reach the end-point IP address.

Figure 13-7. PPTP tunnel across multiple POPs



In this example, the MAX at ISP POP #1 dedicates its second WAN line to PPTP connections to the PNS at 10.65.212.11. To configure this MAX as a PAC:

1 Open Ethernet > Mod Config > PPTP Options.

2 Turn on PPTP, and specify the PNS IP address for Route Line 2.

```
Ethernet
   Mod Config
      L2 Tunneling Options...
         PPTP Enabled=Yes
         Line 1 tunnel type=None
         Route line 1=0.0.0.0
         Line 2 tunnel type=PPTP
         Route line 2=10.65.212.11
         Line 3 tunnel type=None
         Route line 3=0.0.0.0
         Line 4 tunnel type=None
         Route line 4=0.0.0.0
```

3 Close the Ethernet Profile.

The PAC must have a route to the destination address, in this case a route through the ISP POP #2. It does not have to be a static route. It can be learned dynamically by means of routing protocols. The remaining steps of this procedure configure a static route to ISP POP #2:

4 Open an unused IP Route profile and activate it. For example:

```
Ethernet
   Static Rtes
      Name=pop2
      Active=Yes
```

5 Specify the PNS destination address:

```
      Dest=10.65.212.11
```

6 Specify the address of the next-hop router (ISP POP #2). For example:

```
Gateway=10.1.2.4
```

7 Specify a metric for this route, the route's preference, and whether the route is private. For example:

```
Metric=1
Preference=100
Private=Yes
```

8 Close the IP Route profile.

Routing a terminal-server session to a PPTP server

You can initiate a PPTP session in which the terminal-server interface routes the session to a PPTP server. The PPTP command gives you two options for selecting the tunnel the MAX creates. You can specify either the IP address or host name of the PPTP server. Normal PPTP authentication proceeds once the MAX creates the tunnel.

Enter the command, at the terminal-server prompt as follows:

`pptp` *pptp_server*

where `pptp_server` is the IP address or hostname of the PPTP server. When you enter the command, the system displays the following text:

```
PPTP: Starting session
```

```
PPTP Server pptp_server
```

Configuring L2TP tunnels for dial-in clients

L2TP enables you to dial into a local ISP and connect to a private corporate network across the Internet. You dial into a local MAX, configured as an L2TP Access Concentrator (LAC), and establish a PPP connection. Attributes in your RADIUS user profile specify that the MAX, acting as an LAC, establishes an L2TP tunnel. The LAC contacts the L2TP Network Server (LNS) that connects to the private network. The LAC and the LNS establish an L2TP tunnel (via UDP), and any traffic your client sends is tunneled to the private network. Once the MAX units establish the tunnel, the client connection has a PPP connection with the LNS, and appears to be directly connected to the private network.

You can configure the MAX to act as either an LAC, an LNS, or both. The LAC performs the following functions:

- Establishes PPP connections with dial-in clients.
- Sends requests to LNS units, requesting creation of tunnels.
- Encapsulates and forwards all traffic from clients to the LNS via the tunnel.
- De-encapsulates traffic received from an established tunnel, and forwards it to the client.
- Sends tunnel-disconnect requests to LNS units when clients disconnect.

The LNS performs the following functions:

- Responds to requests by LAC units for creation of tunnels.
- Encapsulates and forwards all traffic from the private network to clients via the tunnel.

- De-encapsulates traffic received from an established tunnel, and forwards it to the private network.
- Disconnects tunnels on the basis of requests from the LAC.
- Disconnects tunnels when the value you set for a user profile's MAX-Connect-Time attribute expires. You can also manually disconnect tunnels from the LNS by using SNMP, the terminal-server Kill command, or the DO Hangup command (which you access by pressing <Ctrl- D).

Note: With this release, a MAX acting as an LNS cannot send Incoming Call Requests to an LAC. Only an LAC can make requests for the creation of L2TP tunnels.

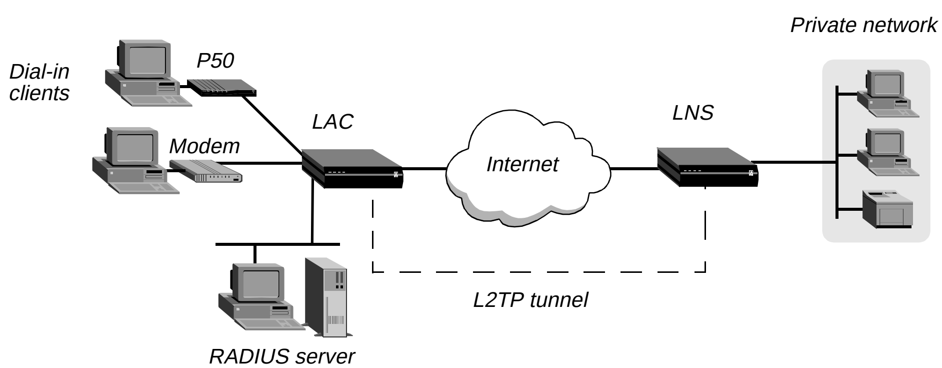
Elements of L2TP tunneling

This section describes how L2TP tunnels work between an LAC and an LNS. A client dials into an LAC, from either a modem or ISDN device, and the LAC establishes a cross-Internet IP connection to the LNS. The LAC then requests an L2TP tunnel via the IP connection.

The LNS is the terminating part of the tunnel, where most of the L2TP processing occurs. It communicates with the private network (the destination network for the dial-in clients) through a direct connection.

Figure 13-8 shows an ISP POP MAX, acting as an LAC, communicating across the WAN with a private network. Clients dial into the ISP POP and are forwarded across the Internet to the private network.

Figure 13-8. L2TP tunnel across the Internet



How the MAX creates L2TP tunnels

The dial-in client, the LAC, and the LNS establish, use, and terminate an L2TP-tunnel connection as follows:

1. A client dials, over either a modem or ISDN connection, into the LAC.
2. On the basis of dialed number or after authentication (depending on the LAC configuration), the LAC communicates with the LNS to establish an IP connection.
3. Over the IP connection, the LAC and LNS establish a control channel.
4. The LAC sends an Inbound Call Request to the LNS.
5. Depending on the LNS configuration, the client might need to authenticate itself a second time.

6. After successful authentication, the tunnel is established, and data traffic flows.
7. When the client disconnects from the LAC, the LAC sends a Call Disconnect Notify message to the LNS. The LAC and LNS disconnect the tunnel.

LAC and LNS mode

The MAX can function as an LAC, an LNS, or both. When configured as both, the MAX functions as an LAC when so specified by the dial-in client configuration, and as an LNS in response to an Inbound Call Request from an LAC.

Note: The MAX can support several simultaneous connections, some in which it acts as an LAC, and some in which it acts as an LNS. For any single connection, however, the MAX can operate as either an LAC or LNS, but not both.

Tunnel authentication

You can configure the LNS to authenticate a tunnel during tunnel creation. You must enable tunnel authentication on both the LAC and LNS.

On the LNS, you must create a Names/Passwords profile where:

- The value in the Ethernet > Names/Passwords > Name parameter matches the value of the System > Sys Config > Name parameter on the LAC.
- The value of the Ethernet > Names/Passwords > Recv PW parameter matches the password configured on the LAC.

On the LAC, you can specify the password with the Tunnel-Password attribute in the RADIUS user profile for the connection initiating the session, or you can configure the password in a Names/Passwords profile. If you create a Names/Passwords profile, the value of the Ethernet > Names/Passwords > Name parameter must match the the value of the System > Sys Config > Name parameter on the LNS.

Conversely, you can configure the LAC and LNS to not require tunnel authentication.

Client authentication

Either the LAC, the LNS, or both, can perform PAP or CHAP authentication of clients for which they create tunnels. If you configure the MAX to create tunnels on a per-line basis, only the LNS can perform authentication, because the MAX automatically builds a tunnel to the LNS for any call it receives on that line.

If you use RADIUS to configure L2TP on a per-user basis, and you specify the Client-Port-DNIS attribute, the LAC does not perform PAP or CHAP authentication. If you specify Client-Port-DNIS, the tunnel is created as soon as the LAC receives a DNIS number that matches a Client-Port-DNIS for any user profile. You can configure the LNS to perform PAP or CHAP authentication after the LAC and LNS establish the tunnel.

If you use RADIUS to configure L2TP, but do not specify the Client-Port-DNIS attribute, the LAC performs PAP or CHAP authentication before the tunnel is established. Once the tunnel is up, the LNS can perform authentication again on the client. Each client sends the same username and password during the authentication phase, so for each client, make sure you configure the LAC and LNS to look for the same usernames and passwords.

You can also direct the MAX to create an L2TP tunnel, from the terminal server, by using the L2TP command. You can configure authentication on the LNS, requiring users to authenticate themselves when they manually initiate L2TP tunnels from the terminal server.

Flow control

The LAC and LNS automatically use a flow control mechanism that is designed to reduce network congestion. You do not need to configure the mechanism.

You can, however, configure the maximum number of unacknowledged packets that the LAC or LNS receives before it requests that the sending device stop sending data. You can configure the LAC or LNS to receive up to 63 unacknowledged packets before refusing new data, or you can disable flow control completely.

Configuration of the MAX as an LAC

The LAC is responsible for requesting L2TP tunnels to the LNS. You configure the LAC to determine when a dial-in connection should be tunneled, and you can specify the LNS used for the connection.

Understanding the L2TP LAC parameters

This section provides some background information about parameters used in configuring the MAX as an LAC:

Parameter	**How it's used**
L2TP Mode	Enables the MAX unit's LAC functionality if you set L2TP Mode to LAC or Both.
L2TP Auth Enabled	You must either enable tunnel authentication for both the LAC and LNS or enable it for neither. You configure a tunnel password in a Names/Passwords profile.
L2TP RX Window	Specifies the number of unacknowledged packets the MAX receives (when configured as an LAC or a LNS) before requesting that the sending device stop transmitting data.
Line *N* Tunnel Type	Specifies whether the MAX should dedicate an entire WAN line to either L2TP or PPTP. If you want the MAX to establish tunnels on a connection-by-connection basis, set Line *N* Tunnel Type to None on all lines.
Route Line *N*	Specifies the IP address of the LNS. This parameter applies *only* if you dedicate an entire WAN line to tunneling with the Line *N* Tunnel Type parameter. If you want the MAX to establish tunnels on a connection-by-connection basis, leave Route Line *N* blank for all lines.

Configuring the MAX

To configure the MAX as an L2TP LAC, you must first enable L2TP LAC on the MAX, then specify how the MAX determines which connections are tunneled.

Configuring systemwide L2TP LAC parameters

To configure systemwide L2TP LAC parameters on the MAX:

1 Open the Ethernet > Mod Config > L2 Tunneling Options menu.

2 Set L2TP Mode to LAC or to Both.

3 If you require tunnel authentication, set L2TP Auth Enabled to Yes.

You must configure both the LAC and LNS identically, to either require or not require authentication.

4 Set L2TP RX Window to the number of packets that the MAX should receive before it requests that the sending device stop transmitting packets.

The default is seven. Set the parameter to 0 (zero) to disable flow control in the receiving direction. The MAX continues to perform flow control for the sending direction regardless of the value of L2TP RX Window.

Enabling L2TP tunneling for an entire WAN line

If you want the LAC to create L2TP tunnels for every call received on a specific WAN line:

1 Open the Ethernet > Mod Config > L2 Tunneling Options menu.

2 For the line for which you are configuring LAC functionality (Line *N*) , set Line *N* Tunnel Type to L2TP. For example, if you want to tunnel all calls received on the first WAN port (labeled WAN 1 on the MAX back panel), set Line 1 Tunnel Type to L2TP.

3 Set Route line *n* to the IP address of the LNS.

Enabling L2TP tunneling on a per-user basis

You can configure RADIUS to direct the MAX to create L2TP tunnels for specific users. To do so, you use three standard RADIUS attributes: Tunnel-Type, Tunnel-Medium-Type, and Tunnel-Server-Endpoint. Table 13-3 describes them.

Table 13-3.RADIUS attributes for specifying L2TP tunnels

Attribute	Description	Possible values
Tunnel-Type (64)	Specifies which tunneling protocol to use for this connection.	PPTP or L2TP. You must set this attribute to L2TP to direct the MAX to create an L2TP tunnel.
Tunnel-Medium-Type (65)	Specifies the protocol type, or medium, used for this connection. Currently, the MAX supports IP only. Future software releases will support additional medium types.	Currently, the only supported value is IP. You must set this attribute to IP.

Table 13-3.RADIUS attributes for specifying L2TP tunnels

Attribute	Description	Possible values
Tunnel-Server-Endpoint (67)	Specifies the IP address or fully qualified host name of the LNS, if you set Tunnel-Type to L2TP, or PPTP Network Server (PNS), if you set Tunnel-Type to PPTP.	If a DNS server is available, you can specify the fully qualified host name of the LNS. Otherwise, specify the IP address of the LNS in dotted decimal notation (*n.n.n.n*, where *n* is a number from 0 to 255.) You must set this attribute to an accessible IP host name or address.

Configuration of the MAX as an LNS

When the MAX acts as an LNS, it responds to requests by LAC units to establish tunnels. The LNS does not initiate outgoing requests for tunnels, so configuration of the MAX is simple. Proceed as follows:

1. Open the Ethernet > Mod Config > L2 Tunneling Options menu.
2. Set L2TP Mode to either LNS or Both.
3. If you require tunnel authentication, set L2TP Auth Enabled to Yes.

   You must configure both the LAC and LNS identically, to either require or not require authentication.
4. Set L2TP RX Window to the number of packets that the MAX should receive before it requests that the sending device stop transmitting packets.

   The default is 7. Set the parameter to 0 (zero) to disable flow control in the receiving direction. The MAX continues to perform flow control for the sending direction regardless of the value of L2TP RX Window.

Index

Symbols

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

Z