MAX 6000 Series ISP and Telecommuting Configuration Guide

Ascend Communications, Inc.
Part Number: 7820-0579-002
For software version 6.0.0

MAX is a trademark of Ascend Communications, Inc. Other trademarks and trade names mentioned in this publication belong to their respective owners.

Copyright © 1998, Ascend Communications, Inc. All Rights Reserved.

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

Ascend Customer Service

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

Obtaining Technical Assistance

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

Information you will need

Before contacting Ascend Customer Service, gather the following information:

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

How to contact Ascend Customer Service

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

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

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

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

Ascend Communications
1701 Harbor Bay Parkway
Alameda, CA 94502

Need information about new features and products?

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

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

  `http://www.ascend.com`

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

  `ftp.ascend.com`

Important safety instructions

The following safety instructions apply to the MAX:

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

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

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

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

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

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

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

8 Models with AC power inputs are intended to be used with a three-wire grounding type plug - a plug which has a grounding pin. This is a safety feature. Equipment grounding is

vital to ensure safe operation. Do not defeat the purpose of the grounding type plug by modifying the plug or using an adapter.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Contents

Figures

Tables

About This Guide

How to use this guide

This guide explains how to configure and use the MAX as an Internet Service Provider (ISP) or telecommuting hub. This guide contains:

- 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 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 setting up these networks through ATMP and PPTP protocols.
- Chapter 14, “MAX System Administration,” explains how to administer and manage the MAX.
- Appendix A, “Troubleshooting,” helps you correct problems that can occur during or after configuration.
- Appendix B, “Upgrading System Software,” explains how to upgrade the MAX system software.

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

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

Convention	Meaning
`Monospace text`	Represents text that appears on your computer's screen, or that could appear on your computer's screen.
`Boldface 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. The parameter that follows the angle bracket is one of the options that appears when you select the parameter that precedes the angle bracket.
Key1-Key2	Represents a combination keystroke. To enter a combination keystroke, press the first key and hold it down while you press one or more other keys. Release all the keys at the same time. (For example, Ctrl-H means hold down the Control key and press the H key.)
Press Enter	Means press the Enter, or Return, key or its equivalent on your computer.
Note:	Introduces important additional information.
 **Caution:**	Warns that a failure to follow the recommended procedure could result in loss of data or damage to equipment.
 **Warning:**	Warns that a failure to take appropriate safety precautions could result in physical injury.

Manual set

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

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

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

This chapter covers these topics:

Using the MAX as an ISP or telecommuting hub

The MAX is a high-performance WAN router that can be used to concentrate many incoming switched connections to a corporate backbone or to another network, such as the Internet or a Frame Relay 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. Of course, the MAX also supports leased connections for those users whose connection times justify a permanent virtual connection to the backbone network.

The most common uses of the MAX are as an ISP (Internet Service Provider) hub, to manage many switched IP connections to the Internet, and as a telecommuting hub, to provide high-speed connections between a corporate backbone and remote locations. Its 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.

Note: If you have a MAX running Multiband Simulation, bridging and routing are disabled. Also, the following terminal server commands do not apply: close, ipxping, open, resume, rlogin, telnet.

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 using an analog modem, an ISDN V.120 terminal adapter (such as a BitSurfer), or an ISDN router such as an Ascend Pipeline. When used as an ISP hub, the MAX is configured as an IP router that establishes the dial-in WAN connection with subscribers and routes their data stream 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, with another Internet router (such as a Cisco router) on that LAN.

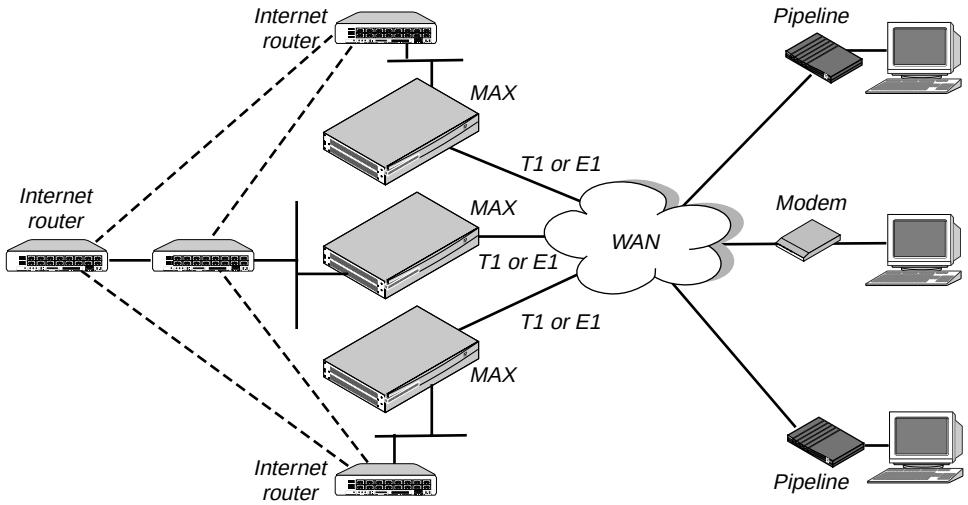


Figure 1-1. Using the MAX as an ISP hub

Typically, the MAX has T1 or E1 lines using 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 it could also use serial WAN, nailed T1, nailed E1, or Frame Relay.

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 users at branch offices, at home, at customer sites, at vendor sites, and on the road. The MAX enables these remote users to access the corporate backbone just as though they were connected locally. The backbone may be a NetWare LAN, an IP network, or a multi-protocol network. Figure 1-2 shows an example where home users, remote offices, and customer sites access the backbone network.

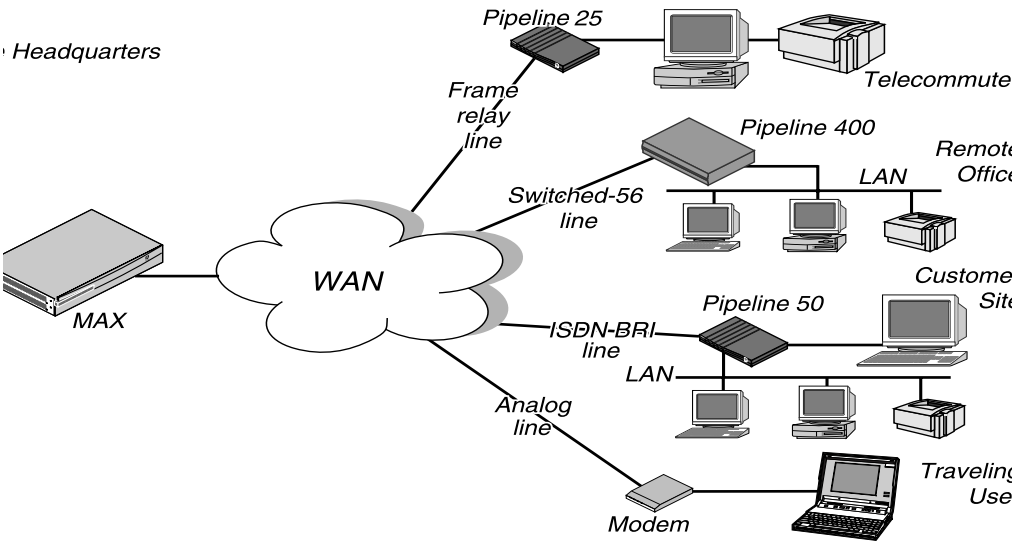


Figure 1-2. Using the MAX as a telecommuting hub

In this example network, a telecommuter in a home office logs into the corporate LAN using a Pipeline 25 and Frame Relay. 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 using 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. One user may access the MAX by using the switched services on an ISDN BRI or Switched-56 line, while another user might require a nailed 56K Frame Relay circuit.

Overview of MAX configuration

This section provides an overview of configuring the MAX. This section contains:

- 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 this introductory material, 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 you troubleshoot problems later.

Configuring lines, slots, and ports for WAN access

The MAX has four built-in T1 or E1 lines and a V.35 serial port (8 Mbps). Each T1 and E1 line has a wide variety of configuration options, including whether or not ISDN signaling is used, type of physical-layer framing, cable length, and telco options. The way you configure each 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.

The serial WAN port is typically used for a leased high-speed connection to a Frame Relay switch or to another WAN router. The port itself requires little configuration. Most of the required information is specified in a Frame Relay or Connection profile.

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 have enabled the lines, slots, and ports for WAN access, you need to configure the manner in which calls will be routed to them (for dial-out access to the WAN) and 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. Authentication and authorization are both described fully in the *MAX Security Supplement.* Following are some of the connection security features supported in the MAX:

- Authentication protocols

  For PPP connections, the MAX supports both PAP (Password Authentication Protocol) and CHAP (Challenge-Handshake Authentication Protocol). CHAP is more secure than PAP, and is preferred if both sides of the connection support it.

- Callback security

  You can specify that the MAX call back any user dialing into it, which ensures 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.

- 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 security

  After a dial-in user has passed the initial connection security, another password can be required for access to the MAX terminal services. Within the terminal server, you can restrict which commands are accessible to users, or prevent them from executing any command other than Telnet.

- Filters and firewalls

  Filters and firewalls provide a packet-level security mechanism that 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 an NNI (network-to-network interface) switch, a DCE (data communications equipment) unit responding to users, or as a DTE (data terminal equipment) 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 may have one physical connection to an X.25 DCE using 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 basis 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 real-time because multicasting is a much cheaper and faster way to communicate the same information to multiple hosts.

OSPF routing

OSPF (Open Shortest Path First) 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, an Ascend-proprietary tunneling mechanism, and PPTP (Point-to-Point Tunneling Protocol).

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 what looks like 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 may 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 now be placed and received.

Overview of management features

This section describes management functions that use features built into the MAX. This section contains:

- Using the terminal server command line
- Using status windows to track WAN or Ethernet activity
- Managing the MAX using SNMP
- Using remote management to configure far-end Ascend units
- Updating software in the MAX unit's flash RAM
- Using Call Detail Reporting

The MAX provides up to nine security levels to control which management and configuration functions are accessible to users. These security profiles are described in detail in the *MAX Security Supplement*.

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.

Using status windows to track WAN or Ethernet activity

Eight status windows display on the right side of the screen in the MAX 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 may want to use CDR 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 which 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.

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 you 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.”

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

To do this:	Go to this chapter or document:
Set up virtual private networks	Chapter 13, “Setting Up Virtual Private Networks.”
Set up SNMP access and traps	Chapter 14, “MAX System Administration.”
Manage the system	Chapter 14, “MAX System Administration.”
Work with status windows	*MAX Reference Guide*
Write configuration scripts	*MAX MIF Supplement*
Set up security	*MAX Security Supplement*
Set up RADIUS	*MAX RADIUS Configuration Guide*

Configuring the MAX for WAN Access 2

This chapter covers these topics:

Introduction to WAN configuration

The MAX has four built-in T1 or E1 lines and a V.35 serial port for WAN access. It also has eight expansion slots which can support additional bandwidth (BRI lines), AIM ports modules to support videoconferencing, or digital modems to support analog modem connections over digital lines.

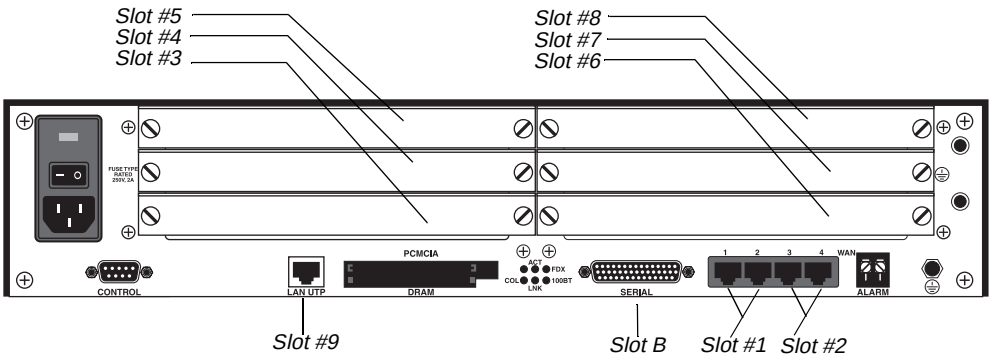


Figure 2-1. Slot and port numbering in the MAX 6000

How the vt100 menus relate to slots and ports

The numbers in the vt100 menus relate to slot numbers in the MAX unit, which may be an actual expansion slot or a *virtual* slot on the unit's motherboard.

- The system itself is slot number 0 (menu 00-000).

  The System menu contains these profiles and submenus, which are all 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
  ```

- The built-in T1 or E1 lines are slot 1 and slot 2 (menus 10-000 and 20-000).

  Each of these slots contain two T1 or E1 lines. The organization of the menus for configuring and testing the lines is:

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

  20-000 Net/T1 (or Net/E1)
     20-100 Line Config
     20-200 Line Diag
  ```

- The six expansion slots are slots 3 through 8 (menus 30-000 through 80-000), with the numbering shown in Figure 2-1.
- The Ethernet is slot 9 (menu 90-000). The Ethernet menu contains submenus and profiles related to the local network, routing and bridging, and WAN connections.
- EtherData is slot A (menu A0-000). For the MAX with built-in Ethernet, this menu is not applicable.
- The serial WAN port is slot B (menu B0-000).

Phone number assignments

The MAX receives calls on phone numbers assigned to its T1 or E1 and (if applicable) Net BRI channels. This section describes important issues related to assigning those phone numbers.

In the MAX configuration, there is a limit of 24 characters, which can include the following characters: 1234567890()[]!z-*#|

Add-on numbers

You build multichannel calls (MP, MP+, AIM, 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 it can dial to connect those channels, and stores the add-on numbers it receives from the answering unit. The calling unit must integrate the add-on numbers with the phone number it dialed initially to add channels to the call. 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 rightmost digits identifying each phone number, excluding the digit(s) that are in common, as in the following example:

- If the add-on number in the called unit is shorter than the phone number dialed by the calling unit, only the rightmost digits are replaced.
  - For example, suppose you dial 777-3300 to reach channel 1of line 1 and 777-3331, 777-3332, through 777-3348, reaches other channels and other lines. In this case, set Ch1#=30 and the other channels and lines 31, 32, and so forth.
- If the add-on number is longer than the phone number dialed, the extra digits are discarded. For example:
  - Ch1# = 510-655-1212
  - Dial# = 555-1213
  - derived number for channel 1 = 655-1212
- If there is no add-on number, the derived number equals the dialed number.
  - 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 ChN 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. A SPID is derived from a telephone number and should be supplied by your carrier.

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 these formats:

`01`*`nnnnnnn`*`0`

`01`*`nnnnnnn`*`00`

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

`aaannnnnnnSS`

`aaannnnnnnSS``00`

In the Northern Telecom SPID formats, *aaannnnnn* 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 may 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 "Call routing" on page 2-48

Configuring T1 lines

Each 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 may be available for user data, or 23 channels may be available for data with the 24th channel reserved for signaling. These are the T1 line configuration parameters:

```
Net/T1
   Line Config
      Name=mytelco
      1st Line=Trunk
      2nd Line=Trunk
      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=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 N=Switched
         Ch N #=12
         Ch N Slot=3
         Ch N Prt/Grp=1
         Ch N TrnkGrp=5
```

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

At the top level, you can assign a name to this line configuration. You can configure several profiles and activate a profile when it is needed.

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 will be transparently passed over to line 2. A device (such as a PBX) connected to line 2 assumes it is connected to the WAN switch and is not aware that the channels actually passed through the MAX before going to the WAN.

Understanding the line interface parameters

This section provides background information on the T1 line interface parameters.

T1 signaling mode

A T1 line's signaling mode (Sig Mode) may 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 to provide 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 using the Call Control mechanism.

Assigning an interface ID to NFAS lines

The NFAS ID num 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 number they specify.

Inband, robbed-bit call control mechanism

Rob Ctl is the call control mechanism for robbed-bit signaling. When 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 when it seizes a trunk.

Carrier switch type

The Switch Type is the network switch providing ISDN service on a T1 PRI line. The ISDN carrier supplies the information; for example, if your carrier is AT&T, the switch type is AT&T.

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

T1 line framing and encoding

The Framing Mode used by the physical layer of the T1 line may be D4 or ESF. D4 format, also known as the superframe format. This format consists of 12 consecutive frames, separated by framing bits. The line cannot be using ISDN signaling with D4 framing; otherwise, false framing and Yellow Alarm emulation can result. ESF specifies the extended superframe format. This format consists 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 that the encoding is Bipolar with 8-Zero Substitution. None is identical to AMI, but without density enforcement.

FDL for monitoring line quality

The telephone company uses a FDL (facilities data link) 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 to use (AT&T, ANSI, or Sprint).

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 a FDL protocol.

Cable length and the amount of attenuation required

The Length parameter is the length of the physical T1 line in feet from the external CSU (channel service unit) to the MAX. If the T1 transceiver in the MAX does not have an internal CSU, it can connect to a T1 line no longer than 655 feet. Anything of greater length requires an internal CSU. The value should reflect the longest line length you expect (up to a maximum of 655 feet).

The Buildout parameter is the amount of attenuation to apply to the T1 transceiver's internal CSU (channel service unit) to match the cable length from the MAX to the next repeater. Valid values are 0 db (decibels) through 22.5 db.

Attenuation is a measure of the power lost on a transmission line or on a portion of that line. When you specify a value for Buildout, the MAX applies attenuation to the T1 line, causing the line to lose power when the received signal is too strong. Repeaters boost the signal on a T1 line. If the MAX is too close to a repeater, you may need to add some attenuation. Check with your carrier to determine the correct value.

Clock source for synchronous transmission

This 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.

You may need to disable this parameter on one unit if two Ascend units connect to each other by a crossover cable (with optional T1 repeaters) between their network ports.

Supporting a PBX

The PBX Type is the signaling to use with the PBX on line 2. When set to Voice, the PBX that connects to line 2 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 2 to dial 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). It 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). See "Call routing" on page 2-48.

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 will be routed to the PBX, without exception.

Input Sample Count lets you specify two rather than the default one sample for standard tone durations and other PBXs that use a non-standard 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 Two is recommended.

Call-by-Call signaling values

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

Understanding the channel configuration parameters

This section provides background information on the T1 channel configuration parameters.

Specifying how the channel will be used

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

- Switched (the default). A switched channel supports switched connections. It may 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). This is assigned automatically to channel number 24 when ISDN signaling is in use.
- NFAS-Prime (the primary D channel for two T1 lines that support NFAS signaling). This will be used as the D channel for both lines, unless it becomes unavailable.
- NFAS-Second (the secondary D channel for two T1 lines that support NFAS signaling). This will be used as the secondary (backup) D channel.

- Drop-and-Insert (pass 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
- Ch N # is the add-on number associated with each switched channel. See "Add-on numbers" on page 2-3.

Associating the channel with a slot/port in the MAX

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 placing calls. In effect, it reserves the channel for calls to and from the specified slot or port. For details, see "Call routing" on page 2-48.

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

Assigning the channel to a trunk group

Trunk group numbers 4 through 9 can be assigned to channels to make them available for outbound calls. See "Routing outbound calls" on page 2-54 for details.

Example T1 configurations

This section provides some example configurations for T1 lines.

Configuring a line for ISDN PRI service

When configuring ISDN PRI service for your MAX units, you must configure ISDN signaling for the line, and optionally, you can 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 uses switched channels and ISDN signaling. To configure Line 1 of this T1 module:

1 Open Net/T1 > Line Config and set the 1st Line to Trunk.

```
Net/T1
   Line Config
      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 allows users calling into a MAX to get better clarification of call disconnects during the initial set-up 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 instance a lot of local Ethernet traffic slowing down RADIUS requests or DNS lookups, then you might want your users to get a different disconnect indication 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 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 > Line menu.

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

This 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.

Configuring robbed-bit signaling

This 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 and set the 2nd Line to Trunk (for example).

```
Net/T1
   Line Config
      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 and set both lines to Trunk service.

```
Net/T1
   Line Config
      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 Leave 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 Leave 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)

Use 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 example 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 more information on each parameter mentioned below, 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 (DNIS —Dialed Number Identification Service or called-party information element).

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

1 Open Net/T1 > Line Config for the second pair of T1 lines on the MAX 6000 (that is, slot 2, or the 20-100 menu).

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

Note: The MAX 2000 has only one pair of T1 lines. These steps apply to the Line 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 Line 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 which 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.

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

7 Set the T1-PRI:PRI # Type parameter as allowed by your PRI lines provider and appropriate to the calls placed by your PBX places.

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

8 Set the T1-PRI:NumPlandID parameter as required by your PRI lines provider.

```
Line 2...
   T1-PRI:NumPlandID=
```

9 The PBX Type parameters tell 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 value Data does not supply call progress tones or information messages to the user.

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

10 The following two parameters tell the MAX whether or not to convert a call incoming on the PRI line(s) to robbed-bit T1 signaling or to answer the call and perform normal incoming call routing.

Set the Ans Service parameter (Most installations select Voice.)

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

Note: If you set Ans Svc=Voice, incoming voice service calls on PRI line(s) are converted to T1 signaling on the line outgoing to the PBX. Data service calls are routed according to the MAX unit's normal incoming call routing, 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 all incoming voice service calls are switched to the PBX and none ever reach the digital modems.

11 Set the Ans # parameter. Most installations leave this parameter blank.

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

12 The following parameters convert the phone number dialed at the PBX to an ISDN PRI format.

Set the Delete Digit parameter.

```
Line 2...
   Delete Digit=
```

13 Set the Add Number parameter.

```
Line 2...
   Add Number=
```

14 The Call-by-Call parameter adds the appropriate ISDN PRI call setup request for calls dialed out from the PBX.

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

15 Close the Line 2 subprofile.

16 Close the T1 profile.

17 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 Use Trunk Grps System profile 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 may 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 > Line 1 (for example).

```
Net/T1
   Line Config
      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 more information on 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 may be available for user data, or 31 channels may be available for data with the 32nd channel reserved for signaling. These are the E1 line configuration parameters:

```
Net/E1
   Line Config
      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 N=Switched
         Ch N #=1212
         Ch N Slot=3
         Ch N Prt/Grp=1
         Ch N TrnkGrp=5
```

Note: The Ch N parameters are repeated for each channel in the line (31 channels if PRI signaling is used, and 32 channels for robbed-bit.)

At the top level, you can assign a name to this line configuration. You can configure several profiles and activate a profile when it is needed.

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: As a workaround to having the carrier manually disable lines, you can set Ethernet > Answer > ID Auth to Required. Provided you have not configured any CLID profiles, the MAX 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 perform a test connection to another DPNSS unit without using an intervening switch by setting Back-to-Back to Yes.

For more information on each parameter, see the *MAX Reference Guide*.

Understanding the line interface parameters

This section provides background information on the E1 line interface parameters.

E1 signaling mode

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

- ISDN signaling using the D channel. The 32nd channel of the E1 line must be designated as the D channel.
- DPNSS indicates that the interface supports DPNSS or DASS 2 signaling.
- R2 indicates R2 signaling.
- Metered indicates metered R2 signaling protocol, for use in Brazil and South Africa.
- Chinese indicates a version of the R2 signaling protocol, for use in China.

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 which should use 56 kbps over R2 lines.

Carrier switch type

The Switch Type is the type of network switch providing ISDN service on an E1 PRI line.

- 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 (This conforms to the Danish E1-TB91020, July 1991 specification and 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).

E1 framing

The physical layer of the E1 line uses framing G.703, which is the standard Framing Mode used by most E1 ISDN providers and by DASS 2, or 2DS, a variant of G.703 required by most E1 DPNSS providers in the U.K.

Specifying digits received on an incoming R2 call

Number Complete specifies how many digits complete number on 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

Group B signaling and Group II signaling specify the group signal to send prior to answering a call.

Required settings when you configure the switch for DASS 2 or DPNSS

L3 and L2 End specify CCITT Layer 2 and CCITT Layer 3. They must be set to their default values when the line connects to a switch configured for DASS 2 or DPNSS.

NL value must be set to 64, its default value, when the line connects to a switch configured for DASS 2 or DPNSS.

Loop avoidance must be set to 7, its default value, when the line connects to a switch configured for DASS 2 or DPNSS.

Contact the carrier for more details. For ISDN, these settings are not applicable.

Clock source for synchronous transmission

This 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 on the E1 channel configuration parameters.

Specifying how to use the channel

Each of the 32 channels of an E1 line may be configured for one of the following uses:

- Switched (the default). A switched channel supports switched connections. It may be robbed-bit or a B channel, depending on how the line's signal mode.
- Nailed (a clear-channel 64k circuit).
- D channel (the channel used for ISDN D channel signaling). This is assigned automatically to channel number 16 when ISDN signaling is in use.
- Unused (unavailable for use).

Phone number assignments

Ch N # is the add-on number associated with each switched channel. See "Add-on numbers" on page 2-3.

Associating the channel with a slot/port in the MAX

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 placing calls. In effect, it reserves the channel for calls to and from the specified slot or port. For details, see “Call routing” on page 2-48.

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

Assigning the channel to a trunk group

Trunk group numbers 4 through 9 can be assigned to channels to make them available for outbound calls. See “Routing outbound calls” on page 2-54 for details.

Example E1 configurations

This section provides some example configurations for E1 lines.

Using ISDN signaling

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

1 Open Net/E1 > Line Config > Line 1 and specify ISDN signaling.

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

2 Set the Switch Type parameter to Net5 (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
```

4 Close the E1 profile.

Using DPNSS signaling

To configure the E1 line for DPNSS signaling:

1 Open Net/E1 > Line Config > Line 1.

2 Set the DPNSS signaling mode and compatible switch type. For example:

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

Mercury is a variant of DPNSS.

3 Set the framing mode. For example:

```
         Framing Mode=2DS
```

2DS gives a variant of G.703 required by most E1 DPNSS providers in the U.K.

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; for example, if there are 5 nailed channels at the local end, there must be 5 nailed channels at the remote end. However, channel assignments do not have to match; for example Channel 1 may 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 assigned in the channels' Prt/Grp parameter. A total of 64 nailed connections can be defined over nailed channels.

1 Open Net/E1 > Line Config > Line 1 (for example).

```
Net/E1
   Line Config
      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 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 more information on each command, 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 using 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 the German 1TR6 switch or the Japan NTT switch, these switches send 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. eventCallCharge 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 is typically used to connect to a Frame Relay switch. The clock speed received from the link determines the serial WAN data rate. The maximum acceptable clock is 8 Mbit/s. The clock speed at the serial WAN port has no effect on the bandwidth of other WAN interfaces in the MAX.

These are the serial WAN configuration parameters:

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

For more information on each parameter, see the *MAX Reference Guide*.

Understanding the serial WAN parameters

This section provides some background on the serial WAN configuration.

Assigning a group number to the serial WAN bandwidth

The Nailed Grp parameter assigns a number that can be referenced as the Group in a Connection profile or the Nailed Grp in a Frame Relay profile. If it is specified in a Connection

profile, the MAX bridges or routes packets to another unit across that nailed connection. If it is used in a Frame Relay profile, 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.

Signals to control the serial WAN data flow

The Activation parameter tells the MAX which signals control the data flow through the serial WAN port. The DCE to which the serial WAN port is connected (such as a Frame Relay switch) determines how to set its value. The CTS (Clear To Send) 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.
3. Set the Activation parameter to Static.

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

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 PCM (Pulse Coded Modulation) encoded digital stream, which 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 and sends it across the WAN to an analog modem.

For example, these are the digital modem configuration parameters for a V.34 modem slot card installed with 8 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 more information on each parameter, see the *MAX Reference Guide*.

56k Modem Numbering

K56Flex modem cards are not numbered sequentially. This 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 8 in a MAX 6000, the `Show Modems` command in the Terminal Server displays the following output:

```
ascend% show modems

slot:item   modem  status
8:0         1      idle
8:1         2      idle
8:2         3      idle
8:3         4      idle
8:6         5      idle
8:7         6      idle
8:10        7      idle
8:11        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 an 12-MOD K56Flex modem card in slot 8 in a MAX 6000, the `Show Modems` command in the Terminal Server displays the following output:

```
ascend% show modems

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

Understanding the digital modem parameters

To process 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. See "Call routing" on page 2-48.

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

See terminal server information in Chapter 3, "Configuring WAN Links."

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. See "Configuring V.110 modems" on page 2-24 for information about processing V.110 calls.

Example configuration

To configure digital modems:

1. Open V.34 Modem > Mod Config (or V.42 Modem > Mod Config).
2. Specify the rightmost 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*. Active calls are not torn down. When an active call drops, 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 the quiesced modem, a delay of up to 20 seconds may occur before the modem becomes available for service.

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

For details, see the *MAX Reference Guide*.

Configuring V.110 modems

A V.110 card provides eight V.110 modems, each of which enables the MAX to communicate with an asynchronous device over synchronous digital lines. An 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). See terminal server information in Chapter 3, “Configuring WAN Links.”

These are the V.110 configuration parameters:

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

For more information on each parameter, see the *MAX Reference Guide*.

Understanding the V.110 modem parameters

To process asynchronous data calls that use V.110 encapsulation requires 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. See “Call routing” on page 2-48.

After the V.110 modem processes the call, the call passes to the MAX unit’s terminal server software. If it does not contain PPP encapsulation, it is handled as a login call, which may 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 are asynchronous calls with CCITT V.110 encapsulation. These calls require V.110 modem processing.

Example 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 is a mobile phone service currently offered in Japan only. In addition to voice communication, PHS offers data communication at bandwidth up to 32 Kilobits per second. You can use this service for phone calls as well as Internet access.

This feature is available through the addition of a slot card, allowing 16 concurrent PHS users. You can install up to six 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; if you do not have this installed, the System Options menu displays PHS Not Installed.

When the MAX is booted with a PHS card in slot 4 and the software enabled, the following is displayed:

```
Main Edit Menu
   00-000 System
   10-000 Net/T1
   20-000 Net/T1
   30-000 Empty
   40-000 PIAFS-16
   50-000 Empty
   60-000 Empty
   70-000 Empty
   80-000 Empty
   90-000 Ethernet
   A0-000 Ether Data
   B0-000 Serial WAN
```

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 BRI (Basic Rate Interface) network interface card has eight BRI lines. These lines provide lower-cost connections to some sites that do not require or have access to the higher-bandwidth T1 or E1 lines. These are the relevant BRI network configuration parameters.

```
Net/BRI
   Line Config
      Name=bri-net
      Switch Type=AT&T
      BRI Analog Encode=Mu-Law
      Line N...
         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 more information on each parameter, see the MAX *Reference Guide.*

Note: After you have configured the line, you may need to configure the card for outbound calls. See “Configuring the Net BRI line for outbound calls” on page 2-28.

Understanding the Net BRI parameters

This section provides some background information on the Net BRI parameters.

Assigning a profile name

You can configure several profiles and activate a profile when it is needed. The name should indicate usage.

Carrier switch type and how it operates

The Switch Type is the central network switch that provides ISDN service to the MAX. For details on supported switch types, see the *MAX Reference Guide*.

BRI Analog Encode

If you are going to receive modem calls, this parameter allows you to select the encoding type. For more information on this parameter, see the *MAX Reference Guide*.

Link Type

This 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 SPIDs (Service profile Identifiers). In multipoint mode, the MAX requires two phone numbers and two SPIDs. All international switch types except DBP Telecom and all domestic (U.S.A.) 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

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 “Call routing” on page 2-48.

Note: You cannot control whether an incoming call will ring 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.

Assigning the channel to a trunk group

Trunk group numbers 4 through 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. See “Routing outbound calls” on page 2-54 for details.

Phone number and SPID (Service Profile Identifier) assignments

Pri Num 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, it is not applicable.

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

Example Net BRI configurations

This section provides some example configurations for Net BRI lines.

Configuring incoming switched connections

In this example configuration, 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.
2. Assign a name to the profile and specify the carrier's switch type.

```
Net/BRI
   Line Config
      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=P_T_P
```

4. Configure the B channels for switched usage, and for routing to the local network.

```
         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.

```
         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 this example Net BRI configuration, the MAX has two T1 or E1 lines and has a Net BRI card installed in slot 5. To enable local users to initiate outbound connections using the BRI lines, the MAX must be configured for trunk groups. 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.
3. Open Net/BRI > Line Config > Line 1.

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

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 initiating from the MAX unit's bridge/router use trunk groups:

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

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

8 Close the Ethernet profile.

To specify that a connection uses a BRI line:

9 Open the Connection profile.

10 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 places the call using the channels in that trunk group.

11 Close the Connection profile.

Note: See "Routing outbound calls" on page 2-54 for a way to use Destination profiles to specify lines as backup channels if all WAN channels are busy. Instead of explicitly entering the dial number in the Connection profile, you can reference a Destination profile, which 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 by invoking the terminal server command line and using 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. Devices terminating these local ISDN BRI lines may 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. To the terminating equipment, 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.

These are the Host BRI configuration parameters.

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

For more information on each parameter, see the *MAX Reference Guide*.

Understanding the Host BRI parameters

This section provides some background information about the Host BRI configuration parameters.

Assigning a profile name

You can configure several profiles and activate a profile when it is needed. The name should indicate usage.

Enabling the line

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

Specifying how the terminating equipment sends and receives calls

Dial Plan specifies how the device terminating a Host BRI line can send and receive calls: by using the extended dial plan or Trunk Groups. For details on dial plans, see "Routing outbound calls" on page 2-54.

Routing calls to the terminating equipment on the Host BRI line

Ans 1# and Ans 2# are two of the MAX unit's add-on numbers assigned to a WAN line (a line that may receive inbound calls from the WAN). See "Call routing" on page 2-48.

Example Host BRI configurations

This section provides some example configurations for Host BRI lines.

Routing inbound calls to the terminating device

In this example configuration, 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 caller dials 555-1212 and connects to the terminating equipment that terminates the BRI line 1.

1 Open Host/BRI > Line Config and assign a name to it.

```
Host/BRI
   Line Config
      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 example 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 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.

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. For example,

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

Note: See "Routing outbound calls" on page 2-54 for details.

6 Close the Dial Plan profile.

To configure the Host BRI module for outbound calls using this Dial Plan:

7 Open Host/BRI > Line Config > Line 1.

8 Set Dial Plan to Extended

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

9 Close the Host BRI profile.

Configuring a local BRI-to-BRI call

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

```
345
```

This number references a Dial Plan profile, using a special 3-digit format. 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 a local BRI-to-BRI call that is never seen by the telephone company:

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

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

2 Close the Host BRI profile.

Configuring BRI/LT lines

These are the BRI/LT configuration parameters.

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

For more information on each parameter, see the *MAX Reference Guide.*

Understanding the BRI/LT parameters

This section provides some background information on the Net BRI parameters.

Assigning a profile name

You can configure several profiles and activate a profile when it is needed. The name should indicate usage.

Enabling the line

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

Specifying how the terminating equipment sends and receives calls

Dial Plan specifies how the device terminating a BRI/LT line can send and receive calls: by using the extended dial plan or Trunk Groups. For details on dial plans, see “Routing outbound calls” on page 2-54.

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

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 “Call routing” on page 2-48.

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.

Assigning the channel to a trunk group

Trunk group numbers 4 through 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. See “Routing outbound calls” on page 2-54 for details.

Phone number and SPID (Service Profile Identifier) assignments

Pri Num 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, it is not applicable.

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

Routing calls to the terminating equipment on the BRI/LT line

Ans 1# and Ans 2# are two of the MAX unit’s add-on numbers assigned to a WAN line (a line that may receive inbound calls from the WAN). See “Call routing” on page 2-48.

Example BRI/LT configuration

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

1 Open BRI/LT > Line Config and assign a name to it.

```
Host/BRI
   Line Config
      Name=idsl
```

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 more information on each parameter, 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 TE (Terminal Equipment) must send digits to the MAX using 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 attached ISDN TE and routes voice calls to the PSTN (Public Switched Telephone Network) over a T1 line or ISDN PRI line. The MAX receives incoming voice calls and routes them to TEs connected to IDSL cards based on DNIS (Dialed Number Identification Service).

Configuring the MAX IDSL card for outgoing voice calls

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

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 > 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 will use 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 will terminate at the MAX and not be forwarded to the PSTN.
3. Exit and save Line profile.

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

Configuring the MAX IDSL card for incoming voice calls

To configure the MAX to accept voice calls from the PSTN network and route them to TEs connected to the IDSL slot cards, select one of the following methods

The following instructs the MAX to route calls to the IDSL card on the basis of the called number:

1. Open the BRI/LT > Line Config > 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 since the MAX matches the DNIS number of the incoming call to configured numbers in Ans *n*#.

The following instructs the MAX to route calls to the IDSL card on the basis of the T1 channel on which the calls are received:

1. Open the Net/T1 > Line Config > 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 7.

Configuring a MAX for outgoing voice calls over IDSL

Use the following steps to configure a MAX to support outgoing voice calls when connected to a MAX IDSL slot card for routing to PSTN network:

Note: If you use a TE other than a Pipeline, it must support en-bloc dialing.

1. Open Ethernet > Answer > PPP Options menu
2. Set Encaps to MPP.
   MPP supports data call preemption. See note below.
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 MAX 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 are required to prepend the phone number you dial with an additional digit to get an outside line.

For example, if the MAX is configured 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) that are configured with a Trunk Group set to 9.

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

Note: This feature also supports data call preemption. If you use two channels for a single MPP data call, and dial your analog phone, one channel will be reallocated to the voice call, leaving one channel for the data call. When you hang up, the channel will be reallocated 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 TA or Pipeline, or from the IDSL card to any intermediate repeater (see Figure 2-2).

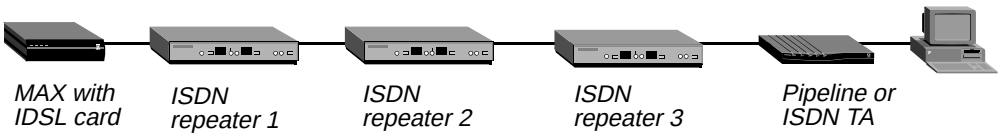


Figure 2-2. IDSL connection with repeaters

In Figure 2-2, 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 ISDN at the end of the connection. This allows you to isolate trouble over the entire connection.

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

1. Select BRI/LT > Line Diag > 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.
   - 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 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

When you enable the Loop Sealing Current, the following message appears in the Edit window:

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

When you disable the Loop Sealing Current, 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 a MAX 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-multiplex mode uses these calls 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, a device can send a signal to another party, indicating that it has data to send; in this case, the control-line state is RTS (Request to Send). The other device can send a signal to indicate that it is ready to receive data; in this case, 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. This means you must specify call routing for calls to reach the local Ethernet. See “Call routing” on page 2-48.

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 Port profile contains these parameters:

```
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
```

For more information on each parameter, see the *MAX Reference Guide*.

Understanding the Port profile parameters

This section provides some background information about the AIM port configuration.

Specifying the dial plan

The Dial Plan parameter specifies how to place calls from this port, by using trunk groups or the extended dial plan. See “Routing outbound calls” on page 2-54.

Routing inbound calls to the codec

Answer numbers specify add-on numbers assigned to a WAN line. This is one way of routing inbound calls received on those numbers to the AIM port. See “Call routing” on page 2-48.

What happens when you turn on the power

Idle specifies the action the port takes when you turn on the power, or if 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).

How the codec dials out

Dial specifies how the codec dials an outbound call:

- 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 but using 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 using different message protocols).
- X.21 ext1-P (same as X.21 ext1, but used for a PictureTel X.21 dialer).

How the codec answers calls

Answer specifies how the codec answers a call:

- 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).

Clearing calls on this port

Clear specifies whether the control-line state determines when the MAX clears a call.

Host session authentication

The receiving unit uses Port Password to compare the Call Password the caller sends upon initial connection of the first channel of an AIM or BONDING call. If the 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 may have sent a password.

Note that the MAX only authenticates AIM and BONDING calls; the MAX does not authenticate dual-port calls. See “Understanding the Call profile parameters” on page 2-43.

Clocking data from the codec

Terminal Timing is 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.

Setting an escape character for RS-366 dialing

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

Preventing timeouts while waiting for a carrier detect signal

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.

Controlling port usage

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 takes any existing calls offline. The DS0 Min Rst parameter resets accumulated DS0 minutes to zero after a specified time, or disables the timer.

Example 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.

Performing 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 more information on each parameter, 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 reflects back to the originator. The WAN interface is the port on the MAX 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. These are the related host interface parameters:

```
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
```

For more information on each parameter, see the *MAX Reference Guide*.

Understanding the host interface parameters

This section provides some background information about configuring the interface to the codec.

Pairing ports for dual-port calls

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

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 any call type. Pairing ports does not disable RS-366 dialing at the secondary port.

Restricting access to the AIM port from the Palmtop Controller

You can prevent Palmtop operators from accessing the port, or restrict their level of access.

Enabling dual-port calls

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

1. Open Host/6 > Mod Config.
2. Assign a name (optional).
3. Use 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.

See “Configuring a two-channel dual-port call” on page 2-47.

Configuring WAN connections between serial hosts

A Call profile defines a WAN connection on the AIM port. These are the Call profile parameters:

```
Host/6 (or Host/Dual)
   PortN 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 N...
   Activ=N/A
   Beg Time=N/A
   Min Ch Cnt=2
   MAX Ch Cnt=12
   Target Util=N/A
```

For more information on each parameter, see the *MAX Reference Guide*.

Understanding the Call profile parameters

This section provides some background information on Call profile parameters.

Dialing out to the remote codec

The dial number 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. See “Routing outbound calls” on page 2-54 for details about specifying the method of placing the call.

Note: The V.25bis protocol implementation in the MAX includes extensions that enable specification of a phone number using the V.25bis CRS command. You can specify a BONDING or other profile in the CRS command, followed by a phone number, which is stored in this parameter. For this usage, the phone number has a limit of 20 characters.

Defining the type of connection and how to manage bandwidth.

Call type specifies the type of connection between the local and remote codecs.

- 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 using 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 (Call Mgm). 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. The Inc Ch Count and Dec Ch Count specify the number of channels it can add and subtract at one time, respectively.

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

What the MAX does when it cannot establish a base channels of a connection

Fail Action 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).

Supporting configuration for certain call types or management methods

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

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

The MAX connects to the remote end over a single channel and then dials multiple channels to the same destination based on 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.

- Dyn Alg specifies which algorithm to use for calculating ALU during the time period specified by the Sec History parameter.
- Sec History specifies a number of seconds to be used as the basis for calculating average line utilization (ALU), which is compared to a target percentage threshold (Target Util). When the ALU exceeds the threshold for a specified time period, 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 number of seconds the ALU must exceed the Target Util before the MAX adds bandwidth.
- Sub Pers specifies the number of seconds the ALU must fall below the Target Util before the MAX subtracts bandwidth.
- Time period N

  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.

Host session authentication

The calling unit sends the Call Password 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 indicates that the call failed authentication with the message *Password Mismatch.*

See “Understanding the Port profile parameters” on page 2-39.

Example AIM call configuration

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

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

2 Specify the dial number to reach the remote device and set the call type to AIM.

```
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.

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

5 Specify the DBA parameters.

```
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

FT1 calls contain nailed channels, while 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 switch 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 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.

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

8 Specify how the switched channels will connect. For example:

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

This setting must be the same in the devices at both ends of the link. The setting shown above connects 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 configures 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 Host/6 > Port 3 Menu > Directory.

2 Set the Dial # parameter using a special 3-digit format

```
Host/6
   Port 3 Menu
      Directory
         Name=terminal-adaptors
         Dial #=241
```

See “Routing outbound calls” on page 2-54.

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 a dual-port call to the serial host; these ports are the primary port and the secondary port. The MAX places the two calls in tandem and clears the calls in tandem, so it considers them a single call. These 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. See “Enabling dual-port calls” on page 2-42. 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.

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

3 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 separated by an exclamation mark. For example

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

4 Set Call Type to 2 Chnl

```
         Call Type=2 Chnl
```

5 Close the Call profile.

Call routing

This section describes how you set up the MAX to configure incoming and outgoing call routing. If you have a mixed incoming calls, such as mixed modem and digital, this section answers questions on 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 this 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. When a call routes to the Ethernet port, the bridge/router software forwards it to a host or hosts according to packet addresses.

These are the topics related to routing inbound switched calls:

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.

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 using bearer service information if it finds no explicit call-routing information.

Setting up ISDN subaddressing

These are the parameters for setting up ISDN subaddressing:

```
System
   Sys Config
      Sub-Adr=Routing
      Serial=1
      LAN=2
      DM=3
      V.110=4
```

A single-digit number is assigned 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. For example, with the configuration shown above, 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. In effect, these settings say "route all calls received on this number to me." 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. These are the related parameters:

```
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 AIM slot card, you can assign channels to a port on the card. This channel 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.

Configure slot and port routing only when answer number and ISDN subaddress routing are not specified. These are the related parameters:

```
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 matching answer number is found, it evaluates the slot and port specifications and routes the call to the specified destination. In the MAX 6000 model, these are the valid slot specifications:

- 0 (Zero, the default). Zero means this parameter is not used to route incoming calls.
- 1 and 2 are invalid settings, because they represent the built-in slots containing T1 or E1 lines.
- 3 through 8 represent expansion slots. When looking at the back panel of the MAX unit, slot 3 is the bottom slot in the left bank of slots, followed by 4 and 5 in ascending order. slot 6 is the bottom right slot, followed by 7 and 8 in ascending order.
- 9 represents the LAN. Calls are routed 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

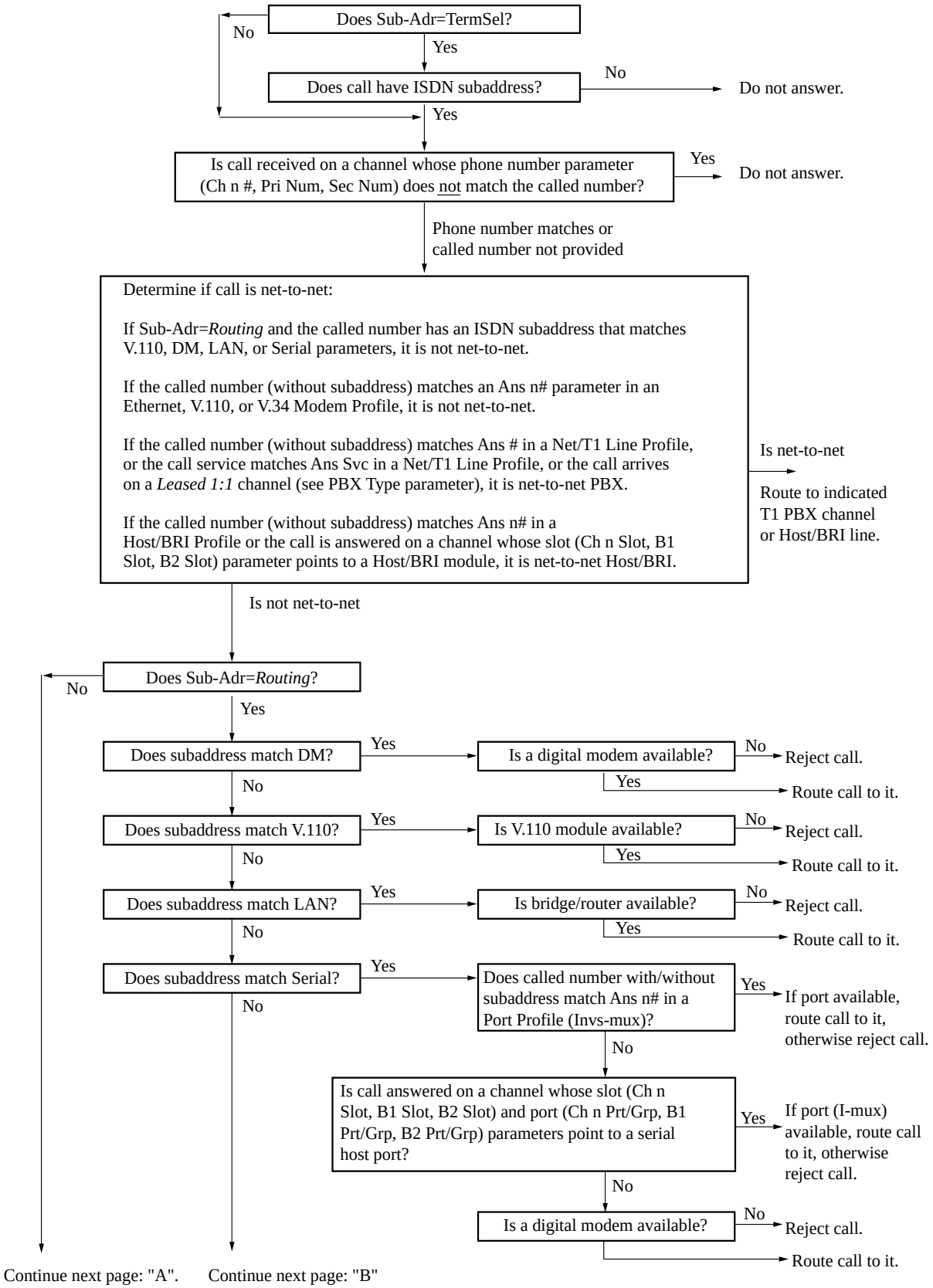
If you set Excl Routing to No (which it is by default), the MAX routes the call based on bearer service. Voice calls are routed to a digital modem, V.110 calls are routed to a V.110 module, and data calls are routed to an AIM port, or if no AIM ports are available, to the bridge/router. If you set Excl Routing to Yes and none of the previous call-routing comparisons were successful, the MAX drops the call. This is the parameter for turning on exclusive port routing:

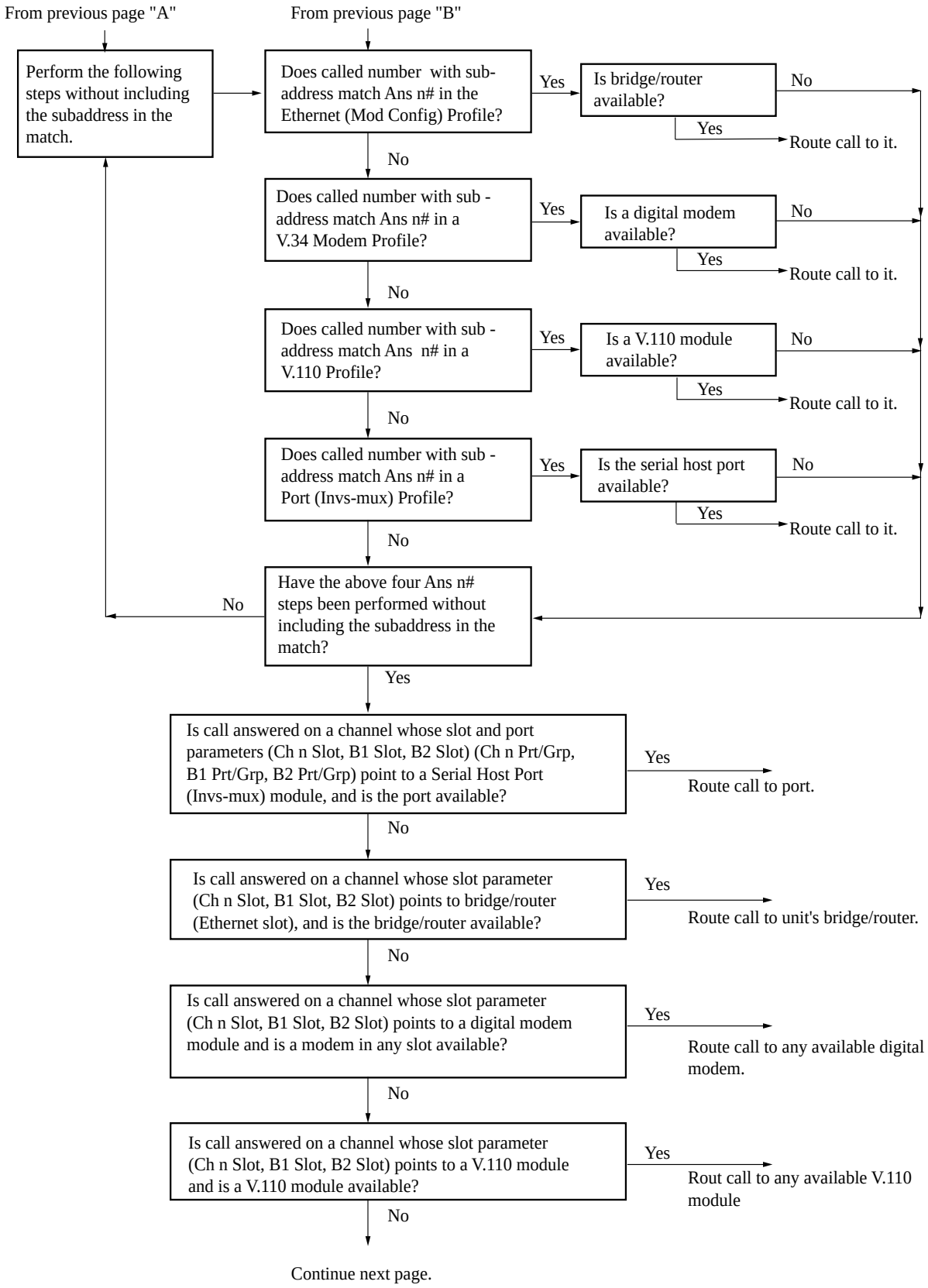
```
System
   Sys Config
   Excl Routing=No
```

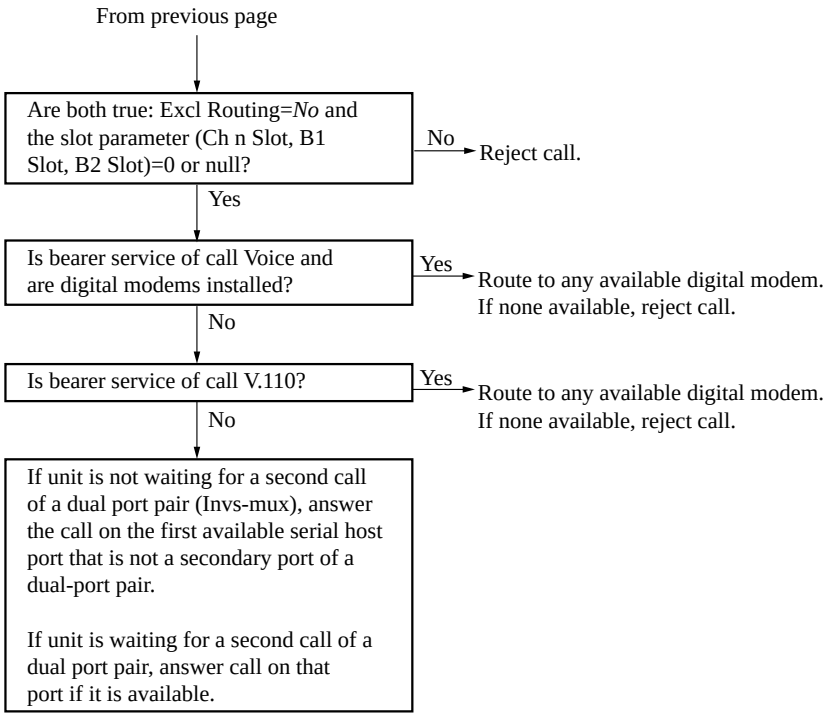
Exclusive port routing prevents the MAX from accepting calls for which it has no explicit routing destination.

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, it is not net-to-net.
If the called number (without subaddress) matches an Ans n# parameter in an Ethernet, V.110, or V.34 Modem Profile, it 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 Profile or the call is answered on a channel whose slot (Ch n Slot, B1 Slot, B2 Slot) parameter points to a Host/BRI module, it is net-to-net Host/BRI.
Is net-to-net
Route to indicated T1 PBX channel or Host/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 available?
No
Reject call.
Yes
Route call to it.
No
Does subaddress match Serial?
Yes
Does called number with/without subaddress match Ans n# in a Port Profile (Invs-mux)?
Yes
If port available, route call to it, otherwise reject call.
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 digital modem available?
No
Reject call.
Route call to it.
Continue next page: "A".
Continue next page: "B"


From previous page "A"
From previous page "B"
Perform the following steps without including the subaddress in the match.
Does called number with sub-address match Ans n# in the Ethernet (Mod Config) Profile?
Yes
Is bridge/router available?
No
Yes
Route call to it.
No
Does called number with sub - address match Ans n# in a V.34 Modem Profile?
Yes
Is a digital modem available?
No
Yes
Route call to it.
No
Does called number with sub - address 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 sub - address 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 available?
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 (Ethernet slot), 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
Rout 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 first looks for channels associated with the trunk group specified in the Dial # (if any) and the port that originated the call, based on the channel configuration parameters. 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.

These are the topics related to routing outbound calls:

Enabling trunk groups

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

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

Trunk group 2 is used 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.

Dialing using trunk group 3 (Destination profiles)

Trunk group 3 is the first digit in a 3-digit dialing prefix in which the next 2 digits are interpreted as the number of a Destination profile.

Dialing using trunk groups 4 through 9

Trunk groups 4 through 9 reference specific groups of WAN channels to use for placing the call. If that group has no available channels, the call is not placed.

Dialing using 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 3-digit dialing prefix in which the next 2 digits are interpreted as the number of a Dial Plan profile.

Matching slot and port specifications (reserved channels)

Whether or not trunk groups are enabled, the MAX relies on slot/port specifications to place outbound calls, if any slot/port numbers are specified. 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 will not find the channel available.

Enabling trunk groups

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 to be available for outbound calls. This is the related parameter:

```
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 through 9 are available for assignment to channels.

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

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. These are the related parameters:

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

With the dial number 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 (zero) or any number between 3 and 8. If it is zero, the call goes to any available AIM port (the third digit is ignored in this case). If it is between 3 and 8, it represents an expansion slot number and the third digit is the host port on that card.

Dialing using trunk group 3 (Destination profiles)

When 3 is the first digit in a three-digit dialing prefix, the MAX interprets the next two digits as the number of a Destination profile. These are the related parameters:

```
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 the dial number 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 4 may contain channels serviced by Spring and trunk group 5 may be serviced by AT&T.

Dialing using trunk groups 4 through 9

Trunk group numbers 4 through 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. Trunk group assignments are also used to group the channels from different types of lines; for example, when the MAX lines are serviced by more than one carrier, you might assign trunk group 4 to a line serviced by one carrier and trunk group 5 to a line serviced by another.

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

These are the related parameters:

```
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 between 4 and 9, the MAX places the call using channels in that trunk group.

Dialing using the extended dial plan

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 using PRI channels. However, it can also be used to set up the PRI parameters for other outbound calls. These are the related parameters:

```
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. The call will be placed using channels in trunk group 8 and the PRI settings in that Dial Plan profile.

Slot and port specifications (reserved channels)

Specifying a slot and port number in a channel configuration reserves the channel for calls to and from the specified slot or port. These are the related parameters:

```
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 9.

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 determining which channels are available for placing the call.

- If the slot and port specifications for a channel are set to zero (the default), the channel is available for all outbound calls that specify the right trunk group.
- If the slot is non-zero and the port is zero, the channel is available to outbound calls originating on that slot.
- If both the slot and port numbers are non-zero, the channel is available only to outbound calls originating on that port.

Configuring WAN Links

3

This chapter covers these topics:

Introduction to WAN links

This chapter describes how to configure various types of links across the WAN. It focuses on the encapsulation issues for these types of connections:

- PPP (Point-to-Point Protocol)

  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.

- EU-UI and EU-RAW

  Two 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, and when these address fields are absent, the MAX uses EU-RAW. EU connections can be dial-in or dial-out.

  EU encapsulation does not support an authentication protocol. CLID authentication is used to match incoming calls to the proper Connection profile when, for example, special filters are applied to certain callers, or some callers route IP and others bridge.

- ARA (AppleTalk Remote Access)

  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. Those calls may be logged into the terminal server interface or, if they contain PPP, passed to the router.

Note: Frame Relay, X.25, IP or IPX routing, and bridging all require both connection-specific and more general system configuration. Those topics appear in their own chapters later in this guide.

This chapter does not describe RADIUS user profiles, which 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 an incoming call is answered or dropped. If the call does not comply with the Answer profile, the MAX drops the call before answering it.

Most administrators set up the Answer profile to reject calls for which no configured profile is found. When a call has a configured profile, the related encapsulation and session options in the Answer profile are not used—the MAX relies on the connection-specific settings instead. However, if the configured profile is a Name-password profile, the MAX may use the settings in the Answer profile to build the session. The Answer profile contains these 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 more information about each parameter, see the *MAX Reference Guide*.

Use Answer profile settings as the defaults for externally authenticated calls

Use Answer as Default indicates whether the Answer Profile should override the factory defaults when the MAX validates an incoming call using RADIUS or TACACS.

Forcing 56k data service

Force 56 tells the MAX to use only the 56-kbps portion of a channel, even when all 64 kbps appear to be available. It is useful for answering calls from European or Pacific Rim countries from within North America, 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: Since the default bandwidth for data calls across R2 lines is 64 kbps, set Force 56 to Yes in any Connection profile which should use 56 kbps over R2 lines.

Requiring a configured profile to answer a call

If you do not require a configured profile for all callers, the MAX builds a temporary profile for unknown callers. Many sites consider this a security breach. Note that setting Profile Reqd to Yes disables Guest access for ARA connections.

Called number and caller-ID authentication

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

Enabling types of encapsulation

The Encaps subprofile contains settings for each type of link encapsulation that may be supported. 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 validates an incoming call using RADIUS or TACACS and Use Answer as Default is enabled.

Setting encapsulation-specific options

See the sections on configuring connections later in this chapter for details on the PPP, Combinet, and other encapsulation options. 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. Full technical specifications for X.75 can be found in the CCITT Blue Book Recommendation X series 1988.

Session options

In the Answer profile, session options set default filters and timers to build connections that use RADIUS (if Use Answer as Defaults is enabled) or Names/Passwords profiles. The Framed Only option can limit terminal server access per user.

DHCP options

In the Answer profile, DHCP options enable the MAX to act as a DHCP server for a local Pipeline unit for connections that use RADIUS (if Use Answer as Defaults is enabled) or Names/Passwords profiles.

Example Answer profile configuration

To set up a basic Answer profile:

1. Open the Answer profile and set Profile Reqd to Yes.
2. Set up CLID (Calling Line ID) 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.

Connection profiles contain these parameters:

```
Ethernet
   Connections
      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...
         depends on 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 more information about each parameter, see the MAX *Reference Guide*.

Understanding Connection profile parameters

This section provides some background information on Connection profile parameters.

The remote device's station name

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

ISDN call information

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).

The dial number

Dial # is the phone number you use to dial out this connection. It can contain up to 24 characters, which may include 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."

The called number

Called # (typically the number dialed by the far end) appears in an ISDN message as part of the call when DNIS (Dial Number Information Service) is in use. In some cases, the phone company may 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. See the *MAX Security Supplement* for details.

The calling number

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

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

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.

Routing configurations

Each connection may be configured for IP routing, IPX routing, OSPF routing (which requires IP routing), or AppleTalk routing. Each of these routing setups has a separate subprofile within a Connection profile. See the appropriate chapters later in this guide.

Bridging

Link-level bridging forwards packets to and from remote networks based on the hardware-level address, not a logical network address. Bridge and Dial Brdcast are related parameters. See the chapter on packet bridging later in this guide.

Connection profile Session options

These are the Session Options parameters in a Connection profile:

```
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 details, see the later chapters in this guide and the *MAX Reference Guide*.

Applying data or call filters to a session

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. See Chapter 7, "Defining Static Filters."

Timing inactive sessions

The Idle timer specifies how long the connection may remain idle before the MAX drops it. TS Idle Mode parameter specifies whether the MAX uses the terminal server idle timer and, if so, whether it monitors traffic in one or both directions to determine when the session is idle. TS Idle specifies how long the terminal server session can remain idle before the MAX logs out the user and terminates the connection.

Setting a maximum call duration

This 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 may be slightly longer than the number of minutes you set.

Allowing bandwidth to be preempted

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.

Specifying a backup connection when a nailed connection fails

Backup 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, a backup switched connection to corporate net #2 may be used. You cannot use this parameter to provide alternative lines to a single destination.

IP direct connections

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

Frame Relay redirect connections

A Frame Relay redirect connection channels all inbound packets out to a Frame Relay switch. See Chapter 4, “Configuring Frame Relay.”

Call blocking

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

Connection profile telco options

These are the Telco Options parameters in a Connection profile:

```
Ethernet
   Connections
      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
```

For more complete information on each parameter, see the *MAX Reference Guide*. This section provides a brief overview.

Enabling both dial-in and dial-out on this connection

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

Setting callback security

When you set Callback 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 are in use).

Nailed, switched, and other call types

The Call Type=switched is the default. The other options are nailed, nailed-MPP, 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/MPP connection combines nailed and switched channels. When you choose this Call Type, you need to specify which side of the link can add switched channels by using the FT1 Caller parameter. See "Example MP connection without BACP" on page 3-22 for details about the Nailed/Mpp call type.

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, which is similar to the way a nailed connection is maintained. A permanent switch connection conserves connection attempts but causes a long connection time, which may be cost effective for some customers. See the *MAX Reference Guide* for details.

Data service

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

Billing numbers

Bill # can specify 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 may require its own billing number. The billing number can contain up to 24 characters.

Dialout OK

This specifies whether the Connection profile may be used for dialing out on one of the MAX unit's digital modems. Only if you set Dialout OK to Yes will the local user be allowed access to the immediate modem feature.

Connection profile accounting options

These are the accounting parameters in a Connection profile:

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

Accounting type

You can 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.

Accounting host and port

These specify the IP address of a connection-specific accounting server to use for information related to this link, and the UDP port number to use in accounting requests.

Accounting timeout and key

The accounting key is a shared secret (a password shared with the accounting server). The Acct Timeout parameter specifies how long to wait for a response to a RADIUS accounting request. TACACS+ has its own timeout method.

Accounting ID base

This specifies the numeric base (base 10 or base 16) for the session ID.

Connection profile DHCP options

The DHCP parameters in a Connection profile are:

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

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

Reply Enabled

This specifies whether the MAX processes DHCP packets and acts as a DHCP server on this connection. If you set this 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, it 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

This 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

This 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. It is not applicable if you set Reply Enabled to No.

Name-Password profiles

Name-password profiles provide simple name/password authentication for incoming calls. They are used only if authentication is required in the Answer profile (Recv Auth). 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.

Note: If Recv Auth is set to None in the Answer profile, Name-password profiles are not used.

Name-password profiles contain these parameters:

```
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 on Name-password profiles.

Name

The name must exactly match the name specified by a dial-in user, including case changes. We recommend that you do not 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.

Password

The password must exactly match the password specified by a 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 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 may 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 then activate the profile.

```
Ethernet
   Names / Passwords
      Name=Brian
      Active=Yes
      Recv PW=brianpw
      Template Connection #=0
```

3. Leave the Template Connection # set to 0 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 will also need to set the AppleTalk options parameter Peer=Dialin. See the AppleTalk routing chapter in this guide for more information.

Configuring PPP connections

This section describes how to configure PPP-encapsulated connections. A PPP connection may be one of the following types:

- PPP—a single-channel connection to any remote device running PPP software.
- MP (Multilink PPP)—a multilink connection to an MP-compliant device from any vendor.
- MP with BACP (MP with Bandwidth Allocation Control Protocol)—an MP call that uses BACP to increase or decrease bandwidth on demand.
- MP+ (Multilink PPP with Ascend extensions)—a multilink connection to another Ascend unit, which uses Ascend dynamic bandwidth allocation to increase or decrease bandwidth on demand.

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 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. See "Spanning multilink or MP+ calls across multiple MAX units" on page 3-28.

Note: If a connection configured for multilink PPP fails to establish multiple channels, it falls back to a single-channel PPP session. In each case, the PPP parameters are used as part of the

connection negotiation. MP, BACP, and MP+ settings are used *in addition to* the single-channel PPP settings.

Configuring single-channel PPP connections

This section describes how to the parameter used for PPP negotiation to establish a single-channel PPP call and to establish the base channel of multilink PPP calls. These are the related parameters:

```
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

Ethernet
   Connections
      Encaps=PPP
      Encaps options...
         Send Auth=None
         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
```

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

Understanding the PPP parameters

This section provides some background information about the PPP parameters.

Enabling routing and bridging in the Answer profile

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. See the appropriate chapter on routing or bridging later in this guide for more information.

Authentication method used for passwords received from the far end

The Recv Auth parameter specifies which 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), or Either, which includes PAP, CHAP and MS-CHAP (Microsoft Challenge Handshake Authentication Protocol format supported by Windows NT systems). The far end must also support the specified protocol.

Authentication method used for passwords sent to the far end

The Send Auth parameter specifies which protocol to use for the password sent to the far end during PPP negotiation.

Passwords to send to and receive from the far end

The Send PW 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.

Maximum receive units (MRU)

MRU specifies the maximum number of bytes the MAX can receive in a single packet on a PPP link. Usually the default 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.

Link and 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., which 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.

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

This parameter in the Answer profile specifies how the MAX responds to caller requests to support CBCP. 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.

CBCP Mode

This parameter specifies what method of callback the MAX offers the incoming caller.

CBCP Trunk Group

This 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.

Note: For more information about CBCP, see the *MAX 6000 Series Reference Guide* and the *MAX 6000 Series Security Supplement*.

Example 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.

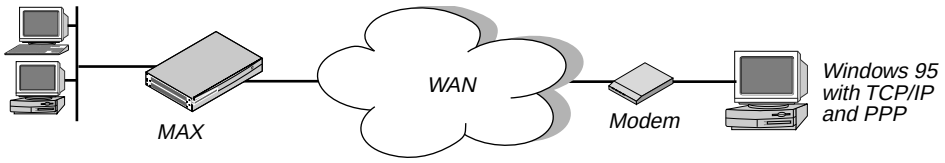


Figure 3-1. A PPP connection

To configure this PPP connection:

1 Make sure the Answer profile enables PPP encapsulation and sets the appropriate routing, bridging, and authentication values. 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 outdial for v.110 modems

The MAX can make outgoing calls to a client on the other side of a v.110 terminal adapter using the PPP protocol. This feature also supports the callback feature via v.110 for the MAX Link Client software product.

See “Configuring dialout options” on page 3-61 for information about enabling dialout using the MAX unit’s digital modems.

To enable PPP outdial 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.

The Data Svc settings that begin with “v110” enable for V.110 outdial. These settings include the v110 indicator (which tells the MAX to communicate with a V.110 terminal adapter), the bit rate for the connection, and the data service to use. For example:

```
v110 19.2 56k
```

uses a bit rate of 19.2 (“19.2”) over a line using the Switched-56 data service. If the MAX cannot sync up with the remote TA using the specified bit rate, it attempts to use one of the other bit rates. See the *MAX Reference Guide* for more details on this Data Svc setting.

Configuring MP and BACP connections

Multilink PPP (MP) uses the encapsulation defined in RFC 1717. MP enables the MAX to interact with MP-compliant equipment from other vendors to use multiple channels for a call. Both sides of the connection must support MP. In addition to the PPP parameters described in "Understanding the PPP parameters" on page 3-16, these are the parameters related to MP connections without BACP:

```
Ethernet
   Answer
      Encaps...
         MP=Yes
         PPP=Yes

      PPP options...
         Min Ch Count=1
         Max Ch Count=1

Ethernet
   Connections
      Encaps=MP
      Encaps options...
         Base Ch Count=1
```

If the Bandwidth Allocation Control Protocol (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, these are the parameters for MP connections with BACP:

```
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
      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
```

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

Understanding the MP and BACP parameters

This section provides some background information on MP and BACP configuration.

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.

Enabling BACP for MP connections

You can enable BACP to use that protocol to increase or decrease bandwidth on demand for MP connections. Both sides of the connection must support BACP.

Specifying channel counts

The base channel count specifies the number of channels to use to establish the call. After the base channel or channels have been established, another link must be dialed to add channels. Inc Ch Count and Dec Ch Count specify the number of channels it 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. See also Parallel Dial in the System profile.

Dynamic algorithm for calculating bandwidth requirements

Dyn Alg specifies an algorithm for calculating average line utilization (ALU) over a certain number of seconds (Sec History). Figure 3-2 shows how the algorithms weight usage samples.

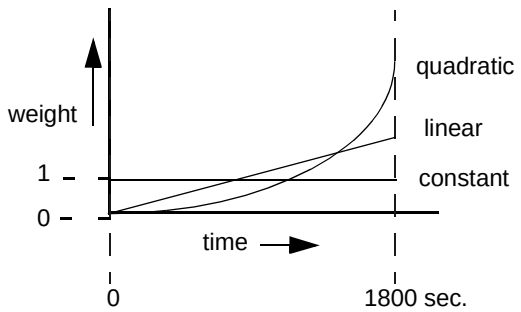


Figure 3-2. Algorithms for weighing bandwidth usage samples

- Quadratic (the default) gives more weight to recent samples of bandwidth usage than to older samples taken over the specified number of seconds. The weighting grows at a quadratic rate.

- Linear gives more weight to recent samples of bandwidth usage than to older samples taken over the specified number of seconds. The weighting grows at a linear rate.
- Constant gives equal weight to all samples taken over the specified number of seconds.

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).

Comparing the average utilization to a 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.

How long the condition should persist before adding or dropping links

Add Pers specifies a number of seconds for which the ALU must persist beyond the Target Util threshold before the MAX adds bandwidth. Sub Pers specifies a number of seconds for which 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 these 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.
- Once the MAX adds bandwidth, there is typically a minimum usage charge; thereafter, billing is time sensitive. The Sub Pers value should be at least equal to the minimum duration charge plus one or two billing time increments. Typically, billing is done to the next multiple of six seconds, with a minimum charge for the first thirty seconds. Your carrier representative can help you understand the billing structure of their switched tariffs.
- You can add channels one at a time or in multiples (see the Parallel Dial parameter).
- Avoid adding or subtracting channels too quickly (less than 10-20 seconds apart).

  Adding or subtracting channels very quickly leads to many short duration calls, each of which incur the carrier's minimum charge. In addition, adding or subtracting channels too quickly can affect link efficiency, since the devices on either end have to retransmit data when the link speed changes.

Example 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.

```
      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 using 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 based on 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 on packets transmitted on this connection, and configure the Ascend criteria for bandwidth management.

```
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

MP+ (Multilink PPP Plus) uses PPP encapsulation with Ascend extensions. MP+ enables the MAX to connect to another Ascend unit using multiple channels. 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, these are the parameters for MP+ connections:

```
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
         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
```

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

Understanding the MP+ parameters

This section provides some background information on MP+ connections.

Channel counts and bandwidth allocation parameters

BACP and MP+ use the same criteria for increasing or decreasing bandwidth for a connection. For details on the bandwidth allocation parameters, see “Understanding the MP and BACP parameters” on page 3-21 and “Guidelines for configuring bandwidth criteria” on page 3-22.

Sending an auxiliary password for added channels

The Aux Send PW parameter can specify another password for authenticating subsequent links as they are dialed. See the *MAX Security Supplement* for details.

Monitoring traffic in one or both directions

DBA Monitor 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, which causes the MAX to ignore bandwidth utilization when determining whether to clear a call and use the Idle timer instead.

Example MP+ configuration

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

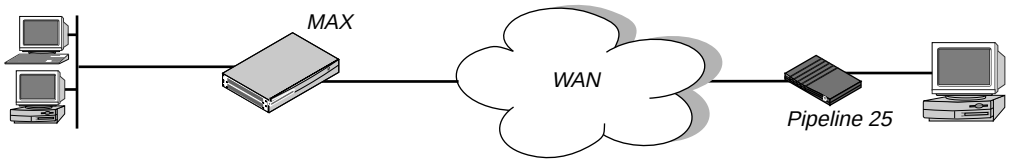


Figure 3-3. An MP+ connection

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 MPP 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/MPP connection is a nailed connection that can add switched channels for increased bandwidth. When you connect nailed or switched channels end-to-end, you establish a nailed/MPP connection. The MAX dials switched channels when the MAX 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/MPP 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/MPP connection is either the Max Ch Count 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/MPP 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/MPP 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/Mpp 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.

Spanning multilink or MP+ calls across multiple MAX units

You can configure multiple MAX units to form a stack, or group of MAX units, that allows a Multilink PPP (MP) or MP+ call to span the MAX units in the stack.

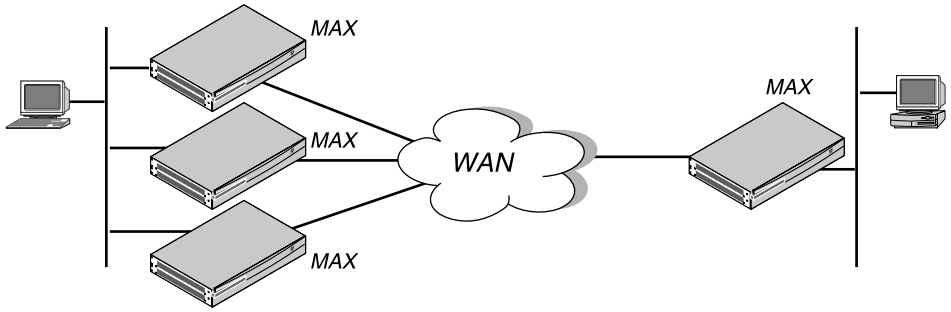


Figure 3-4. A MAX stack for spanning multilink PPP calls (MP) or MP+

Call spanning using 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 will answer 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 an Ethernet multicast packet to locate each other.

Multicast 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 MP/MP+ bundle 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 non-local 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 of 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. See Figure 3-5.

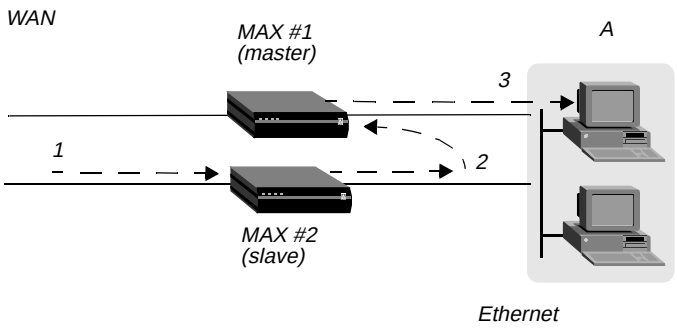


Figure 3-5. Packet flow from the slave channel to the Ethernet

Note: This graphic 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. See 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.

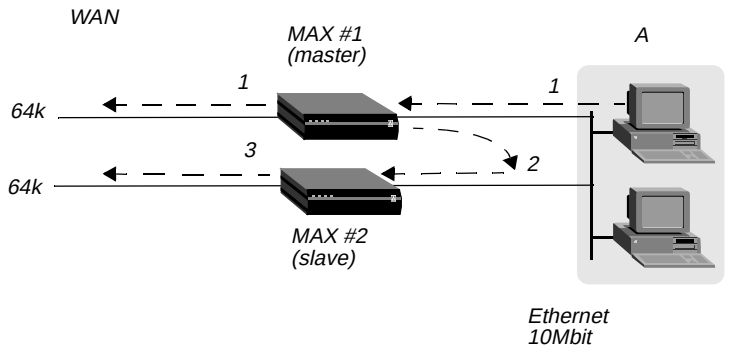


Figure 3-6. Packet flow from the Ethernet

Connection profiles not shared within a stack

A stack does not support sharing of local Connection profiles between the MAX units in the stack. Every MAX in the stack 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 a 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 200 Plus supports up to three stacked channels. A MAX can handle *n* real channels and *n*/3 *stacked* channels.

There is no theoretical limit to the number of MAX units in a stack, other than performance considerations. Since 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 will 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 will be 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. Since 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, utilizes 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 allows each MAX to utilize up to a full 10Mb Ethernet and the entire stack combined can generate up to full 100Mb of Ethernet data. Once again assuming that the 100Mpbs is saturated at 50% usage, we can now use up to 51200Kbps of bandwidth, or 10 times more than in the example above. 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 have MAX units in a stack, 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+ 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 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.

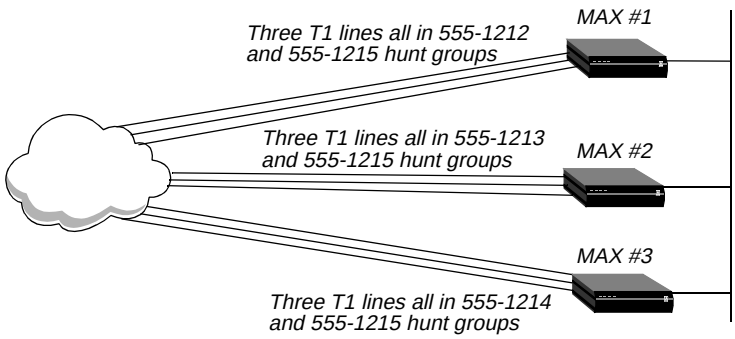


Figure 3-7. Hunt groups for a MAX stack handling both MP and MP+ calls

Viewing Figure 3-7, 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. This means 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 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.

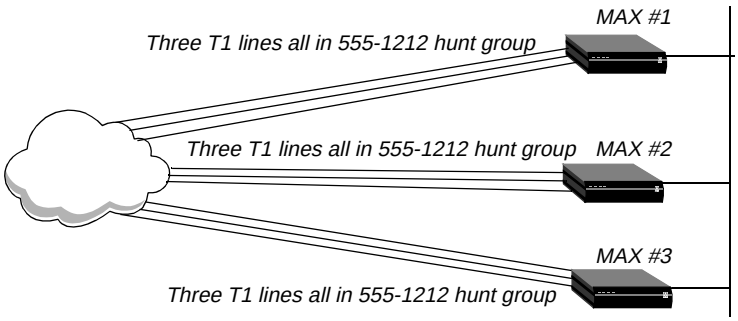


Figure 3-8. Hunt groups for a MAX stack handling only MP-without-BACP calls

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+ 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 continues to MAX #2, and so on.

Both MP+ and MP callers dial the global hunt group number to connect to the stack. The sections "MP-without-BACP calls," and "MP+ calls and MP calls with or without BACP" 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."

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.

Stacking Enabled

This 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

This 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 an Ethernet multicast packet on the specified UDP port. Since these multicast 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 more 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 on 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 is 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. Since 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. See Chapter 8, "Configuring Packet Bridging." Figure 3-9 shows a Combinet connection.

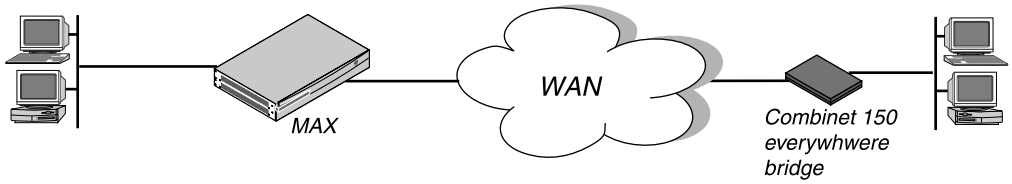


Figure 3-9. A Combinet connection

These are the parameters related to Combinet configuration:

```
Ethernet
   Mod Config
      Bridging=Yes

Ethernet
   Answer
      Encaps...
         COMB=Yes

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

Ethernet
   Connections
      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 more information about each parameter, see the *MAX Reference Guide*.

Understanding Combinet bridging parameters

This section provides some background information on a Combinet configuration.

Specifying the hardware address of the remote Combinet bridge

The Station parameter must specify the MAC (Media Access Control) 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. See 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 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.

Configuring line-integrity monitoring

Interval 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 Base Ch Count parameter specifies the base number of channels to use when setting up the call. It can be set to 1 (64 kbps) or 2 (128 kbps).

Compression

This parameter enables or disables STACKER LZS compression/decompression. Both sides of the link must enable compression or it is not used.

Example 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.

```
Ethernet
   Connections
      Station=000145CFCF01
      Active=Yes
```

3 Configuring bridging options.

```
      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.)

```
   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*.

These are the parameters related to EU configuration:

```
Ethernet
   Answer
      Id Auth=Called Reqd
      Encaps...
         EU-UI=Yes
         EU-RAW=Yes

Ethernet
   Connections
      Calling #=555-7878
      Called #=555-1212
      Encaps=EU-RAW
      Encaps options...
         MRU=1524

Ethernet
   Connections
      Calling #=555-7878
      Called #=555-1212
      Encaps=EU-UI
      Encaps options...
         MRU=1524
         DCE Addr=1
         DTE Addr=3
```

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

Understanding the EU parameters

This section provides some background information on EU parameters.

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.

MRU (Maximum Receive Units)

The MRU parameter 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.

DCE (data communications equipment) address

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 their unit accordingly.

DTE (data terminal equipment) address

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 EU configurations

Figure 3-10 shows three Connection profiles using EU encapsulation with ID authentication.

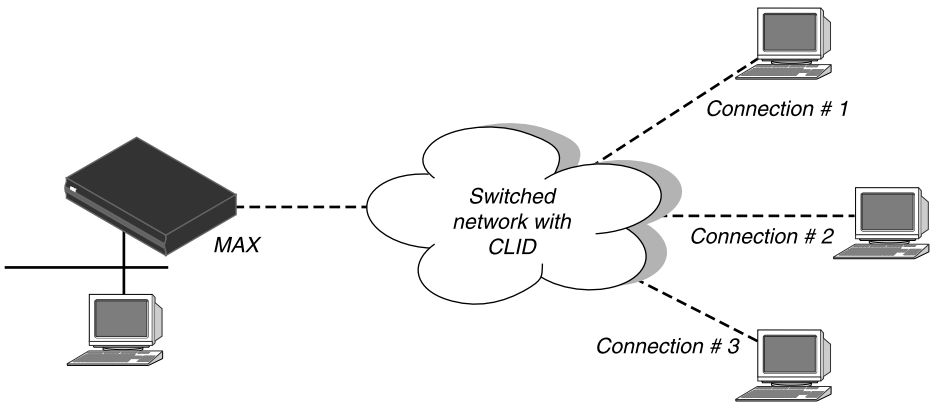


Figure 3-10. EU connection

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.

```
Calling #=555-1212
```

7 Select the EU-RAW encapsulation type and, if necessary, configure the MRU in the Encaps Options subprofile.

```
Encaps=EU-RAW
Encaps options...
   MRU=1524
```

8 Close the Connection profile.

Example 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.

```
Ethernet
   Connections
      Station=remote-device
      Active=Yes
```

5 Specify the calling line number.

```
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.

```
Encaps options...
   MRU=1524
   DCE Addr=1
   DTE Addr=3
```

8 Close the Connection profile.

Configuring an ARA connection

ARA (AppleTalk Remote Access) uses V42 Alternate Procedure as its data link, so it can be used only over asynchronous modem connections.

The parameters related to ARA connections are:

```
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=
```

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

Understanding the ARA parameters

This section provides some background information on ARA parameters.

AppleTalk and zone name

The AppleTalk parameter in the Ethernet profile enables the AppleTalk stack in the MAX. If the local Ethernet supports an AppleTalk router with configured zones, the Zone Name parameter should specify the zone in which the MAX unit resides.

Turning off ARA Guest access

When Profile Reqd=Yes in the Answer profile, ARA Guest access is disabled.

A password required from ARA clients

The Password parameter specifies the password sent to the MAX from the ARA client.

Setting the maximum number of minutes for an ARA session

Max Time specifies the maximum number of minutes an ARA session can remain connected. If it is set to 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 ARA configuration that allows IP access

This section shows an example ARA configuration that enables a Macintosh with an internal modem dialing into the MAX 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. The sample network looks like this:

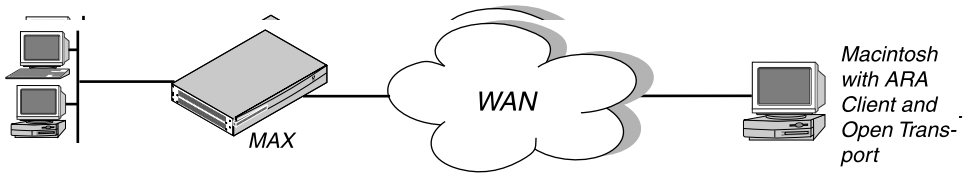


Figure 3-11. An ARA connection enabling IP access

Note: If IP access is not required, 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.

The Macintosh ARA Client software must be configured 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 right dial-in number in the ARA Client software.

The Macintosh TCP/IP software must be configured as follows:

- 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, via DHCP, or via RARP. 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 BOOTP.

- 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.* That option is not supported in the MAX.

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 (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.

```
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.

```
Ethernet
   Connections
      Station=mac
      Active=Yes
```

5 Select ARA encapsulation and configure the ARA options.

```
      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.

Dial-in PPP support 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.

Configuring dial-in PPP for AppleTalk

You can set up a MAX to allow an AppleTalk client to dial in using PPP in two ways:

- using a Connection profile
- using a Name/Password profile

Configuring an AppleTalk PPP connection using a Connection profile

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. 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 will need to configure the other fields in the AppleTalk options menu by continuing with through step 11

   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.

7. Configure the AppleTalk zone name for the Ascend unit in the AppleTalk options sub-menu 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.

8. Specify whether the Ascend unit is a seed or non-seed router. The default value for AppleTalk Router is Off.
   - You assign the network range and zone name configuration for a seed router. There must be at least one seed router on a routed AppleTalk network. Select AppleTalk Router=Seed for this option.
   - A non-seed 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 #*x* are N/A.

If you are configuring a non-seed router and are using Names/Passwords, go to "Configuring an AppleTalk PPP connection using a Name/Password profile" on page 3-44.

9 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.

10 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.

11 Specify the zone names that the platform can seed.

The Pipeline can seed up to 5 zones, and the MAX can seed up to 32. Enter up to 33 alphanumeric characters in zone name fields.

Configuring an AppleTalk PPP connection using a Name/Password profile

1 Open the Ethernet > Mod Config menu.

2 Set Appletalk=Yes.

3 Open the PPP Options menu of the Answer profile.

4 Set Route Appletalk=Yes.

5 Open the Appletalk options submenu of the PPP options menu.

```
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. 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 will need to configure the other fields in the AppleTalk options menu by continuing with Step 7 through Step 11 in "Configuring an AppleTalk PPP connection using a Name/Password profile" on page 3-44.

Note: Step 7 through Step 11 are given here for convenience, and duplicate the steps for setting up AppleTalk routing in the AppleTalk chapter of this guide.

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 more 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, they are handled like regular PPP sessions. (See “Configuring PPP connections” on page 3-15.)

Figure 3-12 shows a user dialing in via analog modem using dial-up software that does not include PPP. This type of call must be routed first to a digital modem, after which it is forwarded automatically to the terminal server.

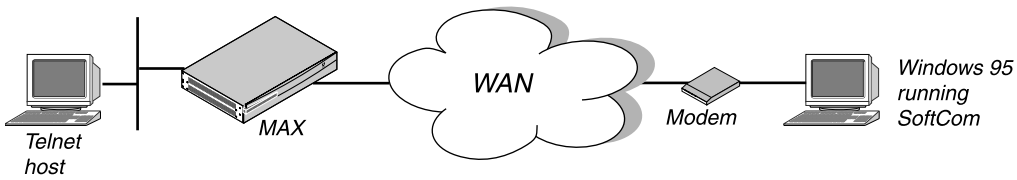


Figure 3-12. Terminal server connection to a local Telnet host

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. See “Introduction to WAN links” on page 3-1 for information about the telco options in a Connection profile, which apply equally to PPP or terminal server calls.

Connection authentication issues

When the terminal server receives a forwarded call, the terminal server waits briefly to receive a PPP packet. If it times out waiting for PPP, it sends its Login prompt. When it receives a name and password, it authenticates 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 connection is then established 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 profile for a single user. For more details on 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 *RADIUS Reference Guide*.

These are some recommended settings for callers with modems and terminal adapters:

- Analog modems and async PPP connections

  If the Connection profile specifies PAP or CHAP authentication, 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, it 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 the 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, this 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 details on these parameters, see “Understanding the PPP parameters” on page 3-16.

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
```

See “Connection profile Session options” on page 3-9 and “Configuring single-channel PPP connections” on page 3-16.

V.120 terminal adapter connections

V.120 terminal adapters (also known as ISDN modems) are asynchronous devices that use CCITT V.120 encapsulation. These are the values that appear to work best for V.120 operation:

- 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. See "Connection authentication issues" on page 3-46.

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. Refer to the V.120 manual for information on entering these settings.

- 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 this:

```
Ethernet
   Connections
      Station=tommy
      Active=Yes
      Encaps=PPP
      Encaps options...
         Recv PW=localpw
      Session options...
         TS Idle Mode=Input
         TS Idle=60
```

See "Connection profile Session options" on page 3-9 and "Configuring single-channel PPP connections" on page 3-16.

TCP-clear 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.

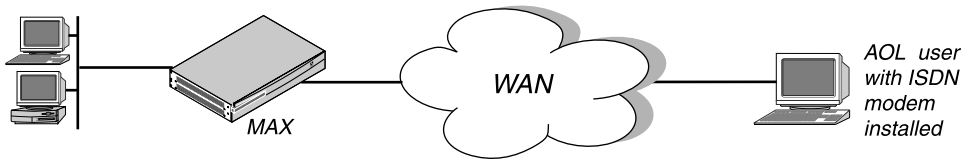


Figure 3-13. A TCP-clear connection

Note: A TCP-clear connection is host-to-host: as soon as the MAX authenticates the connection, a TCP connection is established to the host 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:

```
Ethernet
   Connections
      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*.

See also "Connection profile Session options" on page 3-9 and "TCP Modem connections (DNIS Login)" on page 3-49.

TCP Modem connections (DNIS Login)

This feature allows you to enable or disable TCP modem access to the MAX as well as configure the default port for TCP modem access.

The MAX treats a TCP-encapsulated call between two MAX units over an asynchronous line as if it were a modem. This is referred to as TCP modem. Previously, the MAX would always allow such calls. Now, you can disable TCP modem connections to the MAX. In addition, you can change the TCP port used for these connections. Previously the default port for TCP modem access was 150. It is now 6150.

Figure 3-14 illustrates an example TCP modem setup. A user dialing into an ISP first connects to telephone switch, which then establishes a connection to a MAX. This local MAX 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; the local MAX merely passes the data through. The ISP MAX typically authenticates remote users.

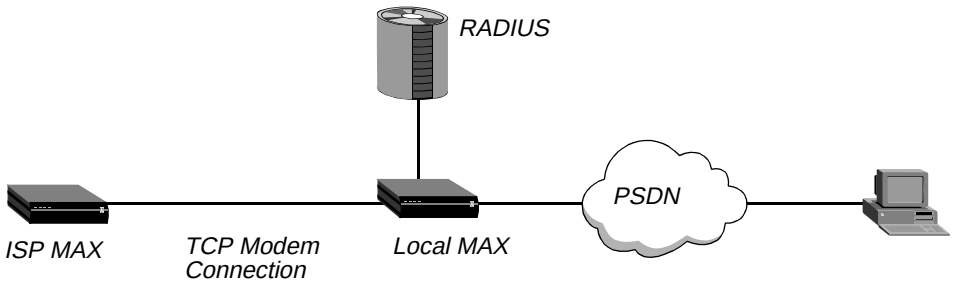


Figure 3-14. Sample TCP modem connection

For more information about TCP modem connections, refer to the *RADIUS Guide*.

Enabling terminal server calls and setting security

The terminal server can provide a command-line interface or a menu of Telnet hosts that dial-in users can log into. 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

  Users who have access to the command-line can see information about your network by using administrative terminal server commands. You can also allow them to initiate their own Telnet, Rlogin, or TCP connections to hosts.

- 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 with a choice. The login and password entered by the user will be those required by the host, not by the terminal server.

- 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)
```

To configure the terminal server mode:

1. Open Ethernet > Mod Config > TServ Options.
2. Enable incoming terminal server calls.

```
Ethernet
   Mod Config
      TServ options...
         TS Enabled=Yes
```

3. Password-protect terminal mode.

```
         Passwd=tspassword
         Security=Partial
```

4. Close the Ethernet profile.

The terminal server security mode 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.

- If you set security mode to none, users are not prompted for a login name and password.
- If you set security mode to partial, users are prompted for a name and password only when entering terminal mode, not for menu mode.
- If you set security mode to full, users are prompted 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 by the terminal server software.

To affect how the modem negotiation and data packetizing occurs, you can set the following parameters:

```
Ethernet
   Mod Config
      TServ options...
         V42/MNP=Will
         Max Baud=33600
         MDM Trn Level=-13
         Cell First=No
         Cell Level=-18
         7-Even=No
         Packet Wait Time=2
         Packet characters=0
```

This section provides background information on the modem configuration parameters.

Digital modem error control

The digital modems negotiate LAPM/MNP error control with the analog modem at the other end of the connection according to how this parameter is set. It 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.

Setting a maximum baud rate

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.

Specifying the default modem transmit level

When a modem calls the MAX, the unit attempts to connect at the transmit attenuate level you specify. This is the amount of attenuation in decibels the MAX should apply to the line, causing the line to lose power when the received signal is too strong. Generally, you do not need to change the transmit level. However, when the carrier is aware of line problems or irregularities, you may need to alter the modem's transmit level.

Rockwell modem code has been modified to make the transmit level programmable, so users can change the default setting for their specific connection. Transmitting at higher level helps certain modems with near-end-echo problems.

Attempting cellular connections first

The MAX supports cellular modem calls. The user can also 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-bit even parity

The MAX does not use 7-bit even parity on outbound data unless you set this parameter to Yes. Most applications do not use 7-bit even parameter.

Support for specialized applications on modem connections

Packet Wait time 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 modem configuration

To sets 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 a host in immediate mode), the MAX establishes a session between the remote user's PC and the terminal server. To affect how the MAX establishes a session and what commands are available to the user, you can set these parameters:

```
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.

Controlling how the screen appears to users while the connection is set up

Silent determines whether status messages appear or not while the connection is being established. Clr Scrn can be set to clear the screen when the MAX establishes a connection.

Setting the terminal mode password

Passwd specifies a password up to 15 characters. This is the password terminal server users will be prompted for when establishing a connection to the terminal server itself.

Setting the login banner and prompts

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, by default:

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 multi-line prompt, set Prompt Format to Yes and use "\n" to represent a carriage return/line feed and "\t" to represent a tab.

Specifying the command-line prompt

Prompt specifies the command-line prompt, which by default is:

ascend%

Be sure to include a trailing space if desired.

Another login prompt for RADIUS-authenticated logins

The 3rd Prompt is 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 the third prompt and that it appears last in the login sequence. This is the default setting.

Some ISPs use a terminal server that follows a login sequence different from that used by Ascend, for example, that includes a menu selection prior to login. Administrators at those sites can configure 3rd prompt to appear first to mimic that terminal server and retain compatibility with client software in use by subscribers. See the *MAX Reference Guide* for more details.

Affecting 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.

Clear Call specifies whether when the user terminates a Telnet or Rlogin session, the connection terminates as well.

Buffer Chars determines whether the terminal server buffers input characters for 100 milliseconds before forwarding them to the host, or sends the characters as received.

Telnet Mode specifies whether binary, ascii, or transparent mode is the default for Telnet sessions. Def Telnet instructs the terminal server to interpret unknown command strings as the name of a host for a Telnet session. Local Echo sets a global default for echoing characters locally, which can be changed for an individual session within Telnet.

Displaying a message when informing users of their address

The terminal server displays “Your IP address is...” (followed by the assigned address). You can change that default message.

Specifying a 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. This means that the timer begins when the login prompt appears on the terminal server screen, and continues (is not reset) when the user makes unsuccessful login attempts.

Example terminal mode configuration

This example configures the password and makes the Rlogin option available to dial-in users. Note that you enable the Telnet option by default.

1. Open Ethernet > Mod Config > TServ Options.
2. Specify the terminal server password.
3. Configure a multi-line login prompt.

```
Ethernet
   Mod Config
      TServ options...
         Login Prompt=Welcome to Ascend Remote Server\nEnter your
name:
         Prompt Format=Yes
```

4. Enable the use of the Rlogin command in terminal mode.

```
         Passwd=tspasswd
         Rlogin=Yes
```

5. 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. To affect how the MAX establishes a session, you can set these parameters:

```
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 on the immediate mode configuration parameters.

Specifying the type of immediate service

Immed Service 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 on 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.

The host and the port on which the connection is made

Specify the hostname or address to which users will be connected in terminal server immediate mode. You can also specify a TCP port number to use for the connections.

Example immediate mode configuration

This example configures immediate Telnet service that relies 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.

```
Ethernet
   Mod Config
      TServ options...
         Immed Service=Telnet
         Immed Host=host1.abc.com
         Immed Port=23
         Telnet Host Auth=Yes
```

6. Close the Ethernet profile.

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 these parameters:

```
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 on the menu mode configuration parameters.

Specifying menu mode as the initial interface

Initial Scrn determines whether the terminal server brings up a menu interface first for interactive users initiating connections. Depending on the Toggle Scrn setting, users may be able to switch to the command-line interface from menu mode by pressing the zero key. The Security setting determines whether a login and password will be required when entering the menu interface.

Obtaining the menu from RADIUS

Remote Conf specifies that the terminal server menu and list of hosts will be obtained from a RADIUS server.

Specifying the hostnames and addresses of up to four Telnet hosts

The Host and Text parameters expect an IP address and hostname, respectively, for up to four Telnet hosts.

Example menu mode configuration

This example allows the menu to appear at login and specifies four hosts; this example also cannot enter the command-line.

1 Open Ethernet > Mod Config > TServ Options.

2 Specify that 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 appearing in the menu.

```
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
```

See “Enabling terminal server calls and setting security” on page 3-50 for an example menu. Dial-in users will be able to Telnet to these hosts by selecting the hostname or IP address.

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, initiating 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 entering the terminal server interface. These parameters 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 on the PPP mode configuration parameters.

Enabling PPP mode

You can prevent users from initiating PPP sessions by setting PPP to No.

PPP delay

PPP Delay specifies the number of seconds the terminal server waits before transitioning to packet-mode processing.

PPP direct

PPP Direct 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.)

The message informing users they are in PPP mode

You can specify that no message appear, or choose between *PPP Mode* and *PPP Session*.

Example PPP configuration

This example enables PPP direct mode:

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 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 these parameters.

```
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 on the SLIP mode configuration parameters.

Enabling SLIP (Serial Line IP) sessions

You can disable or enable SLIP sessions by using the SLIP parameter.

Allowing users to obtain an IP address from a BOOTP server

SLIP BOOTP enables the terminal server to respond to BOOTP within SLIP sessions. If it is enabled, a user who initiates a SLIP session can get an IP address from the designated IP address pool via BOOTP. If it is disabled, 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

This parameter enables you to specify text 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

This 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

- 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 that the gateway is the MAX unit's IP address.

Example SLIP configuration

This example enables SLIP sessions and specifies that the terminal server will respond to BOOTP in SLIP sessions:

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: Slip Bootp=Yes.

```
Ethernet
   Mod Config
      TServ options...
         SLIP=Yes
         SLIP BOOTP=Yes
```

4. Close the Ethernet profile.

Configuring dialout options

The terminal server has access to the MAX digital modems, and can be used to enable users on the local network to dialout using those modems. You can enable local dialout using these parameters:

```
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 on the dialout configuration parameters.

Enabling dialout

If you enable Modem dialout, 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.

Enabling direct access dialout

If you enable Immediate Modem service, users telnet to a particular port on the MAX and the MAX provides Immediate Modem dialout service. The port number configured for Immediate Modem dialout tells the MAX that all telnet sessions initiated with that port number want modem access. Immediate Modem service has its own password (up to 64 characters. If the Imm. Modem Pwd is non-null, users will be prompted for a password before being allowed access to a modem.

How the modem dialout works

If you enable dialout (not Immediate Modem), users can access a modem as follows: Telnet to the MAX from a workstation. For example:

```
Telnet max01
```

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.

```
^C^C^C
```

5 To resume the suspended virtual connection:

```
ascend% resume
```

6 To terminate a virtual connection:

```
ascend% close
```

How immediate modem works

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 dialout configuration

This example enables direct access on port 5000:

1 Open Ethernet > Mod Config > TServ Options.

2 Enable the use of the modem dialout.

3 Enable the direct access (immediate modem) feature.

```
Ethernet
   Mod Config
      TServ options...
         Modem dialout=Yes
         Immediate Modem=Yes
```

4 Specify on which port the immediate modem feature will function.

5 Specify a password for modem access.

```
Ethernet
   Mod Config
      TServ options...
         Imm. Modem port=5000
         Imm. Modem Pwd=dialoutpwd
```

6 Close the Ethernet profile.

Configuring T-Online for Deutsche Telekom

T-Online is a customized application designed for Deutsche Telekom. The following sections discuss DTPT encapsulation, PRI-PRI switching, and supporting status window changes.

For RADIUS-related configuration of T-Online, see Chapter 4, "Setting Up WAN Connections in RADIUS," in the *RADIUS Configuration Guide*.

DTPT encapsulation for T-Online PPP sessions

The call management encapsulation type DTPT supports Deutsch Telekom's need for multiple simultaneous PPP sessions between an Ascend router and a T-Online access host (a ZGR).

Overview

You can configure the MAX as a gateway for PPP clients. These clients can call into the MAX, be authenticated in the conventional manner, and then send IP packets whose destination address is a T-Online ZGR. Though in many respects the ZGR functions like an IP router using PPP, it can only accept packets from a single source address on any given B channel. Therefore, the MAX must establish a separate call, on a separate B channel, for each source address sending packets through the gateway. The MAX can make several simultaneous calls to one destination—T-Online's ZGR—but the link differs from an MP or MP+ session in the following ways:

- Each call appears to the ZGR as an independent PPP call from the MAX.
- Each call carries packets from a single source address.

In this release, for the ZGR, you can define a user profile that specifies the new DTPT encapsulation type so that each B-channel connection to the ZGR carries only one user's traffic.

User interface changes

This release includes the following user interface changes:

- In the Connection profile, you can specify DTPT for the Encaps value. You must set Encaps=DTPT for each Connection Profile that will connect to a ZGR.
- When you set Encaps=DTPT, the Encaps Options submenu contains a subset of the parameters found there when Encaps=PPP:

  ```
  90-103 T-Online

     Encaps options...
        Send Auth=PAP
        Send PW=*****
        MRU=1524
        Link Comp=Stac
        VJ Comp=Yes
  ```

  You set each parameter as you would for any other profile. The parameters function identically to those in the Encaps Options submenu for PPP, except that you can specify only PAP for Send Auth.
- When you set Encaps=DTPT, AnsOrig to N/A in the Telco Options submenu.

- When you set Encaps=DTPT, set the Private and RIP parameters to N/A (and internally forced to not advertise the route) in the IP Options submenu.

All parameters in all other submenus apply as they would for an ordinary PPP call. For example, you can set the Idle parameter in the Connection profile's Session Options submenu to specify the number of seconds the MAX waits before clearing a call when a session is inactive.

How DTPT connections work

The end user's connection to the MAX, the MAX unit's connection to the ZGR, the IP routing scheme, and the algorithms for call disconnects are in many respects similar to their non-DTPT counterparts. Security and reliability considerations vary with the authentication process in use.

End user's connection to the MAX

The T-Online user's connection to the MAX shares many characteristics of other, more conventional connections:

- The user can use PPP, MP, or MP+ to connect to the MAX. Only the MAX unit's connection to the ZGR limits each address to one B channel.
- The user establishes a PPP session on the MAX by either of the following means:
  - A digital PPP call
  - An analog call to the terminal server, followed by a command to enter PPP mode.
- Once having thereby established a PPP, MP, or MP+ session with the MAX, the user can receive any conventional routing services. The MAX appears to the user as a conventional access router, regardless of whether the destination is a ZGR. In fact, the user can access the ZGR and other destinations in the same session.
- A user not directly logged into the MAX, but with access to the LAN by other means, can forward IP packets via the MAX if you configure the routing table to permit it.
- If a user sends the MAX an IP packet with a destination of the ZGR, and the MAX does not have a call active to the ZGR, the MAX places a call to the ZGR and routes the subscriber's packet over the connection.
- The MAX forwards any traffic destined for a user with an active PPP session, including packets arriving from the ZGR.
- The MAX forwards any traffic with a destination on the LAN, including packets arriving from the ZGR.

The T-Online user's connection to the MAX differs from a conventional connection in the following ways:

- The MAX places a new call to the ZGR for each user on the basis of the user's IP address. That is, the MAX places a call for each source IP address, and sends only traffic from that address via the B channel to the ZGR.
- If the MAX has an active call to the ZGR, and additional packets for the ZGR arrive from the IP address for which the MAX initiated the call, the MAX sends the packets via the existing call.

MAX unit's connection to the ZGR

A Connection profile defines a call from the MAX to the ZGR, which in most respects resembles, and functions as, a conventional PPP dial-out profile:

- Each call from the MAX to the ZGR appears to the ZGR as a PPP call.
- Using the DTPT encapsulation type, the MAX internally manages a set of calls to the ZGR as a *bundle*, which is a single interface analogous to an MP or MP+ bundle.
- Authentication of the MAX-to-ZGR call takes place as defined in the Connection profile. The MAX reports its system name to the ZGR, and submits the password you specify using the Send PW parameter in the Encaps Options submenu of the Connection profile. For the Send Auth parameter, you can only select PAP.
- You can set the MRU, Link Comp, and VJ Comp parameters just as you would for a PPP call.
- The MAX dedicates particular E1 lines for calls to the ZGR. You direct calls to the appropriate line by using a trunk group (for switched calls) or a nailed group (for nailed-up calls). You can also use this mechanism to direct ZGR traffic to a particular B channel on a given E1 line.

The connection between the MAX and the ZGR differs from a conventional PPP connection in the following ways:

- The Connection profile uses DTPT to tell the MAX to perform outgoing call management according to the requirements of the ZGR.
- In contrast to MP or MP+, the MAX selects a channel on the basis of the source IP address. The MAX maintains a table of active sessions for this purpose. No Dynamic Bandwidth Allocation takes place, nor are packets statistically multiplexed among channels.
- During PPP negotiation with the ZGR, the MAX transmits the IP address of the user on whose behalf the call is being placed. (In this respect alone, the information the MAX sends to the ZGR is different from the information it supplies in an ordinary PPP call.)

Call disconnects

For a ZGR user, call disconnects work in the conventional manner in the following respects:

- The call from the user to the MAX is in all respects an ordinary PPP call. Therefore, the MAX can disconnect it for any of the ordinary reasons, such as the caller hanging up, the Connection profile's Idle parameter value being exceeded, or a lower layer failure.
- A call from the MAX to the ZGR can be disconnected for any of the reasons applicable to an ordinary PPP connection, including termination by the ZGR.
- Calls placed in response to packets received over the LAN do not automatically terminate when the source of the packets stops sending them, unless you set a value for the Idle parameter in the Connection profile.
- If you set in the Idle parameter in the Connection profile, and the MAX terminates the connection because the Idle value has been exceeded, the arrival of a subsequent packet from the associated user causes the MAX to re-establish the call to the ZGR.

For a ZGR connection, call disconnects have the following special features:

- If the connection to the user terminates for any reason, the MAX terminates the associated call to the ZGR.

- Although in some respects the set of calls to the ZGR resembles an MP or MP+ bundle, disconnection of one call does not imply disconnection of the entire bundle. They are separate PPP calls.
- No disconnection takes place based on Dynamic Bandwidth Allocation.

IP routing

IP routing works in the conventional manner in two respects. First, the ZGR has one IP address, so the MAX unit's routing table contains a single route to the ZGR, regardless of how many calls are actually active. As is the case for MP or MP+, the MAX selects a specific B channel appropriate to the encapsulation and call management type.

Second, with the exception of packets destined for the ZGR, the MAX routes any packets it receives from the user in the usual manner.

IP routing for the ZGR also differs from conventional routing in two ways. First, every ZGR shares the same IP address, so the ZGR does not advertise the MAX unit's route. The Private and RIP parameters in the IP Options menu are N/A, causing the routes to remain private.

Second, packets received over a given WAN interface and destined for the ZGR must all have the same source address. More specifically, if the user's equipment is a gateway with other IP addresses behind it, equipment using those IP addresses cannot send packets to the ZGR. A call to the ZGR via the MAX has the same one-IP-address restriction as does a call directly to the ZGR. This restriction does not apply to packets received over the LAN.

Security and reliability considerations

Network integrity depends on the authentication process by which users gain access to the MAX. The MAX can gain access to the ZGR automatically. Each B channel is reserved for one user at a time, so the ZGR connection is subject to denial-of-service attacks if the MAX places calls to the ZGR without proper authentication. Call authentication covers access to the MAX from the WAN; the design of the rest of the network must ensure security on the LAN.

The number of source addresses on the LAN can vary, so up to a number larger than the number of interfaces on a MAX, it is impossible to guarantee that there will be an outgoing B channel available for every attempted access to the ZGR. In the presence of LAN-initiated calls to the ZGR, access might fail for LAN users, WAN users, or both. If you use the Idle parameter in the Connection profile, some users might obtain a connection to the ZGR on an initial attempt, but not on a reconnect attempt that occurs after the value of the Idle parameter has been exceeded.

PRI-PRI switching

PRI-PRI switching for T-Online provides a network-side implementation of NET-5 to support switching calls from Deutsche Telekom's public network to a T-Online server.

If you enable T-Online, the MAX can switch calls from the public network to a T-Online server based on a match defined by Deutsche Telekom. The match can be one of the following:

- The caller's phone number matches a value specified in RADIUS, and the caller's subaddress matches a subaddress specified in the same RADIUS profile.

- The caller's phone number matches a value specified in RADIUS, and the caller does not have an associated subaddress.
- The caller's subaddress matches a value specified in RADIUS, and the caller does not have an associated phone number.
- The caller does not specify a subaddress or phone number.

T-Online status window changes

For E1 lines configured for T-Online, the Line Stat window replaces the LA link status with new values:

- NT

  This value specifies that the line's link status is up and it is physically connected to the ZGR server (1st Line or 2nd line parameter is set to T-Online-ZGR).

- TE

  This value specifies that the line's link status is up and it is physically connected to the switch, allowing the user to dial in (1st Line or 2nd Line parameter is set to T-Online-USER).

For example, the T-Online Line Status display for line #1 in slot #1 connecting to a ZGR server, would look like the following:

```
10-100 1234567890
 L1/NT ----------
3456789012345678901
---s---------------
```

Configuring Frame Relay

4

This chapter covers these topics:

Using the MAX as a Frame Relay concentrator

In a Frame Relay backbone, every access line connects directly to a Frame Relay (FR) switch. In the past, most connections to the Frame Relay network were relatively high speed, such as full T1 or E1 lines. With recent changes in Frame Relay pricing, many sites now want to concentrate many low-speed dial-in connections into one high-speed nailed connection to a frame relay switch. When you can configure the MAX as a Frame Relay concentrator, it accepts incoming dial-in connections as usual and forwards them out to a frame relay switch.

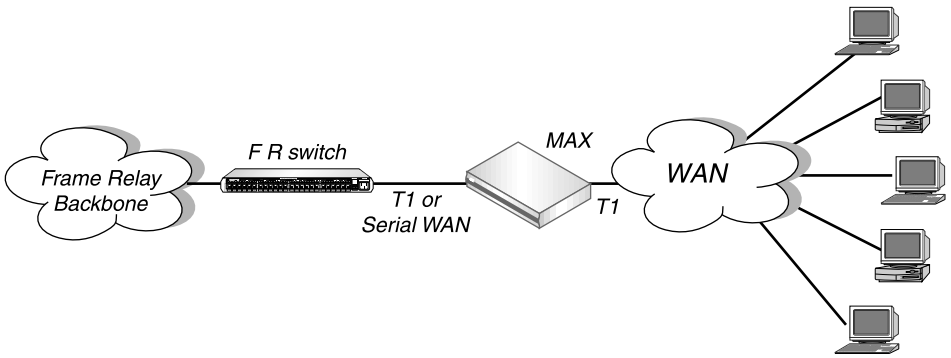


Figure 4-1. The MAX operating as a Frame Relay concentrator

As a Frame Relay concentrator, the MAX can accept up to 96 low-speed connections in North America or Japan, or 120 low-speed connections in Europe. If all of the Frame Relay connections are concentrated onto the single 2-Mbps serial WAN interface, the MAX turns a single high-cost Frame Relay port on a traditional Frame Relay switch into approximately 100 operational ports.

Configuring the MAX as a Frame Relay concentrator involves the following elements:

- An interface to the Frame Relay switch (usually nailed T1, nailed E1, or serial WAN).
- A logical datalink to the Frame Relay switch (defined in a Frame Relay profile)

- User connections (defined in Connection profiles or RADIUS)

Kinds of physical network interfaces

The MAX typically uses serial WAN, nailed T1, or nailed E1 to connect to a Frame Relay switch. For details on configuring these interfaces, see Chapter 2, "Configuring the MAX for WAN Access."

Kinds of logical interfaces to a Frame Relay switch

Figure 4-2 shows the types of Frame Relay interfaces supported in the MAX:

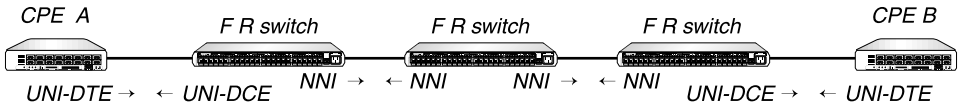


Figure 4-2. Types of logical interfaces to Frame Relay switches

Note: As a Frame Relay concentrator, the MAX can operate as a CPE (Customer Premise Equipment) device or as a FR switch, or both. In Figure 4-2, all of the elements could be Ascend units, but are not necessarily so.

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

Network to Network Interface (NNI)

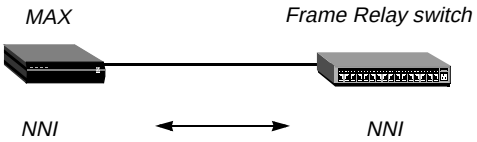


Figure 4-3. Network to Network interface (NNI) in a MAX unit

An NNI interface connection allows the MAX to appear as a Frame Relay network interface based on the NNI specifications. It performs both DTE and DCE link management, and allows two separate Frame Relay networks to connect via a common protocol. See "Configuring an NNI interface" on page 4-6.

User to Network Interface—Data Communications Equipment (UNI-DCE)

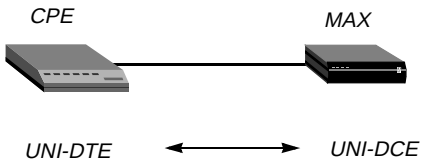


Figure 4-4. User to Network Interface-Data Communications Equipment (UNI-DCE)

UNI is the interface between an end-user and a network end point (a router or a switch) on the Frame Relay network. In a UNI-DCE connection, the MAX operates as a Frame Relay router

communicating with a DTE device. To the DTE devices, it appears as a Frame Relay network end point. See “Configuring a UNI-DCE interface” on page 4-7.

User to Network Interface—Data Terminal Equipment (UNI-DTE)

In a UNI-DTE connection, configure the MAX as a UNI-DTE communicating with a Frame Relay switch. It acts as a Frame Relay *feeder* and performs the DTE functions specified for link management. See “Configuring a UNI-DTE interface” on page 4-7.

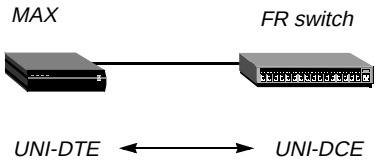


Figure 4-5. User to Network Interface - Data Terminal Equipment (UNI-DTE)

Note: For NNI or UNI-DTE connections, the MAX is able to query the device at the other end of the link about the status of the DLCIs in the connection. If any of the DLCIs become unusable and the DLCI’s Connection profile has a specified Backup connection, the MAX dials the Connection profile specified in the Backup parameter in Connections > Session Options. See the *MAX Reference Guide* for details on the Backup parameter.

Types of Frame Relay connections

For Frame Relay connections, the MAX supports the following:

Gateway connections

The MAX receives an incoming PPP call, examines the destination IP address, and brings up the appropriate Connection profile to that destination, as usual. If the Connection profile specifies Frame Relay encapsulation, the Frame Relay profile, and a DLCI, the MAX encapsulates the packets in Frame Relay (RFC 1490) and forwards the data stream out to the Frame Relay switch using the specified DLCI. The Frame Relay switch uses the DLCI to route the frames. This is known as gateway mode.

Frame Relay circuits

A circuit is a permanent virtual circuit (PVC) segment that consists of two DLCI end points and possibly two Frame Relay profiles. It requires two and only two DLCI numbers: data drops if the circuit has only one DLCI and if Frame Relay defines more than two DLCI, Frame Relay only uses two DLCI numbers. You define circuits in two Connection profiles. Data coming in on the DLCI configured in the first Connection profile switches to the DLCI configured in the second one.

Redirect connections (rarely used)

When the MAX receives an incoming PPP call for which the session options specify FR Direct, it ignores the destination IP address in the packets from the dial-in client. Instead, the MAX routes the packet using the FR DLCI specified in the session options. In effect, the MAX does not route packets from the client in the usual sense, it simply passes them on to the Frame

Relay network and assumes that another device routes the packets based on the destination IP address. This is known as redirect mode, and is not commonly used.

Configuring the logical link to a Frame Relay switch

The Frame Relay profile specifies a link, usually across a single cable, to the Frame Relay network. This link can support many permanent virtual circuits (PVCs), each with a different endpoint. These are the Frame Relay parameters:

```
Ethernet
   Frame Relay
      Name=NNI
      Active=Yes
      Call Type=Nailed
      FR Type=NNI
      LinkUp=Yes
      Nailed Grp=1
      Data Svc=64k
      PRI # Type=N/A
      Dial #=N/A
      Bill #=N/A
      Call-by-Call=N/A
      Transit #=N/A
      Link Mgmt=Q.933A
      N391=6
      DTE N392=3
      DTE N393=4
      DCE N392=3
      DCE N393=4
      T391=10
      T392=15
      MRU=1532
```

For more information about each of these parameters, see the *MAX Reference Guide*.

Understanding the Frame Relay parameters

This section provides some background information about the Frame Relay parameters:

Specifying a profile name and activating the profile

User connections link up with the Frame Relay connection specified in this profile by specifying its profile name. The name must be unique and cannot exceed 15 characters.

Set the Active parameter to Yes to make this profile available for use.

Bringing down the datalink when DLCIs are not active

LinkUp indicates that the datalink comes up automatically and stays up even when the last DLCI has been removed. If you set this parameter to No, the datalink 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 datalink connections by using 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 there is a DLCI profile invoking the datalink.

Defining the nailed connection to the switch

Nailed is the default for Frame Relay connections. When you define the call type as 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 that are available are 64K or 56K.

Specifying the type of Frame Relay interface

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). See “Kinds of logical interfaces to a Frame Relay switch” on page 4-2.

Link management protocol

The Link Mgmt setting may be None (no link management), T1.617D (for T1.617 Annex D), and Q.933A (for Q.933 Annex A).

Frame Relay timers and event counts

Frame Relay timers and event counts are as follows:

- N391 specifies the interval at which the MAX requests a Full Status Report (between 1 and 255 seconds). It is N/A if FR Type is DCE.
- DCE N392 specifies the number of errors during DCE N393 monitored events which causes the network side to declare the user side procedures inactive. Its value should be less than DCE N393 (between 1 and 10). It is N/A when FR Type is DTE.
- DCE N393 specifies the DCE monitored event count (between 1 and 10). It is N/A when FR Type is DTE.
- DTE N392 specifies the number of errors during DTE N393 monitored events which cause the user side to declare the network side procedures inactive. Its value should be less than DTE N393 (between 1 and 10). It is N/A when FR Type is DCE.
- DTE N393 specifies the DTE monitored event count (between 1 and 10). It is N/A when FR Type is DCE.
- T391 specifies the Link Integrity Verification polling timer (between 5 and 30 seconds). Its value should be less than T392. It is N/A when FR Type is DCE.
- T392 specifies the time for Status Enquiry messages (between 5 and 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 1532 is the right setting, unless the far end device requires a lower number.

Example Frame Relay profile configurations

This section shows an example Frame Relay profile configuration for each type of Frame Relay interface (NNI, UNI-DCE, and UNI-DTE).

Configuring an NNI interface

In this example, the MAX has a nailed connection to another Frame Relay switch and also has an NNI interface configuration to that switch. Figure 4-6 shows the connection.

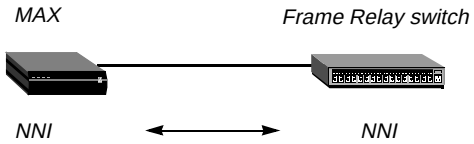


Figure 4-6. Example NNI interface to another switch

To configure the Frame Relay profile for this NNI interface:

1. Open a Frame Relay profile.
2. Assign the profile a name and activate it.

```
Ethernet
   Frame Relay
      Name=ATT-NNI
      Active=Yes
```

3. Set the FR Type to NNI.

```
      FR Type=NNI
```

4. Set up the nailed connection to the remote switch and specify the data service for the link. For example:

```
      Call Type=Nailed
      Nailed Grp=1
      Data Svc=64k
```

5. Specify the link management protocol and its configuration parameters. For example:

```
      Link Mgmt=T1.617D
      N391=6
      T391=10
      T392=15
      MRU=1532
```

6. Close the Frame Relay profile.

Configuring a UNI-DCE interface

In this example, the MAX has a nailed connection to customer premises equipment (CPE) and also has a UNI-DCE interface configuration to that equipment. Figure 4-7 shows the connection.

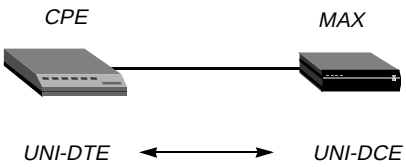


Figure 4-7. Example UNI-DCE interface to an end-point (DTE)

To configure the Frame Relay profile for this UNI-DCE interface:

1 Open a Frame Relay profile.

2 Assign the profile a name and activate it.

```
Ethernet
   Frame Relay
      Name=ATT-DCE
      Active=Yes
```

3 Set the FR Type to DCE.

```
FR Type=DCE
```

4 Set up the nailed connection to the remote switch and specify the data service for the link. For example:

```
Call Type=Nailed
Nailed Grp=1
Data Svc=64k
```

5 Specify the link management protocol and its configuration parameters. For example:

```
Link Mgmt=T1.617D
DCE N392=3
DCE N393=4
T392=15
```

6 Close the Frame Relay profile.

Configuring a UNI-DTE interface

In this example, the MAX has a nailed connection to a Frame Relay switch configured as a DCE and has a UNI-DTE interface configuration that switch. Figure 4-8 shows the connection.

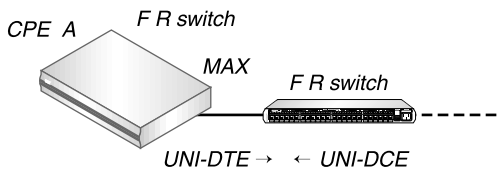


Figure 4-8. UNI-DTE interface to a Frame Relay switch

To configure the Frame Relay profile for this UNI-DTE link:

1 Open a Frame Relay profile.

2 Assign the profile a name and activate it.

```
Ethernet
   Frame Relay
      Name=ATT-DTE
      Active=Yes
```

3 Set the FR Type to DTE.

```
      FR Type=DTE
```

4 Set up the nailed connection to the remote switch and specify the data service for the link. For example:

```
      Call Type=Nailed
      Nailed Grp=1
      Data Svc=64k
```

5 Specify the link management protocol and its configuration parameters. For example:

```
      Link Mgmt=Q.933A
      N391=6
      DTE N392=3
      DTE N393=4
      T391=10
```

6 Close the Frame Relay profile.

Configuring Connection profiles for Frame Relay

All connections that use Frame Relay must specify the name of a configured Frame Relay profile as the datalink between the MAX and the Frame Relay network. Forwarded or routed connections over the Frame Relay link use the following parameters:

```
Ethernet
   Answer
      Encaps...
         PPP=Yes
         FR=Yes

      PPP Options...
         Route IP=Yes
```

For gateway connections:

```
Ethernet
   Connections
      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
```

```
Encaps=FR_CIR
Encaps options...
   FR Prof=pacbell
   DLCI=16
   Circuit=circuit-1
```

For redirect connections:

```
Ethernet
   Connections
      Encaps=PPP
      Route IP=Yes
      Ip options...
         LAN Adrs=10.2.3.4/24
      Session options...
         FR Direct=Yes
         FR Prof=pacbell
         FR DLCI=16
```

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

Understanding the Frame Relay connection parameters

This section provides some background information about the Frame Relay connection parameters:

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.

The far end specified in a Frame Relay encapsulated Connection profile lies at the end of a PVC, whose first hop is known by the DLCI named in the Connection profile. 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 switches to the DLCI configured in the other. Data drops if the circuit has only one DLCI. If more than two Connection profiles specify the same circuit name, the MAX uses only two DLCI.

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.

Redirect connections (FR Direct=Yes)

In an FR Direct connection, the MAX simply *attaches* a Frame Relay PVC to multiple Connection profiles. It does so on 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).

In this unusual mode called *Frame Relay redirect*, the MAX ignores the destination of these packets. It assumes that some device at the far end of the PVC makes the routing decisions. However, the Connection profile must use IP routing to enable the MAX to route data back to the client.

Example connection configurations

This section shows example Connection profile configurations for Frame Relay gateway, circuit, and redirect configurations.

Configuring a Frame Relay gateway connection

This example configuration shows how to configure a Frame Relay gateway connection. It presumes that dial-in users who need to reach the distant IP network have valid Connection profile (or RADIUS user profiles). This example shows the Connection profile that assigns a DLCI and passes the data stream out to a Frame Relay switch. The example network is shown in Figure 4-9:

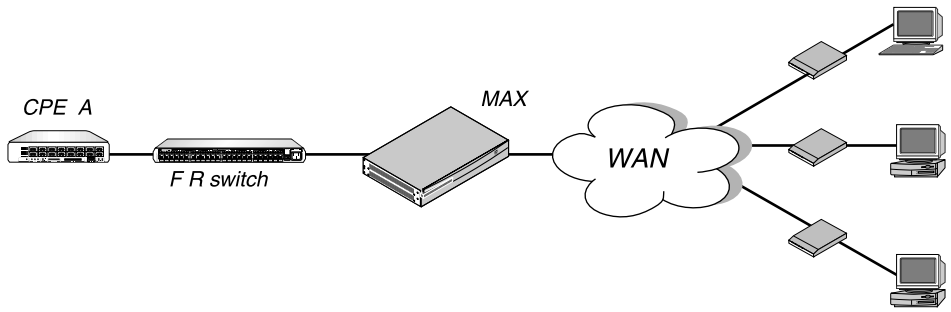


Figure 4-9. Gateway connections

In this example, the MAX communicates with a remote Frame Relay switch using ATT-NNI, a Frame Relay profile. To configure this link:

1 Open a Connection profile.

2 Specify the station name, activate the profile, and specify FR encapsulation.

```
Ethernet
   Connections
      Station=gateway-1
      Active=Yes
      Encaps=FR
```

3 Enable IP routing and specify the address of the remote IP router.

```
      Route IP=Yes
      Ip options...
         LAN Adrs=10.2.3.4/24
```

4 Open the Encaps Options subprofile and specify the name of the Frame Relay profile with a nailed connection to the Frame Relay switch, and a DLCI assigned by the Frame Relay administrator.

```
Encaps options...
   FR Prof=ATT-NNI
   DLCI=55
   Circuit=N/A
```

5 Close the Connection profile.

Configuring a Frame Relay circuit

This example configures a circuit between a UNI-DCE and NNI datalinks. Configure a circuit between any two interfaces within the MAX in the same way. Figure 4-10 shows an example of a Frame Relay circuit network:

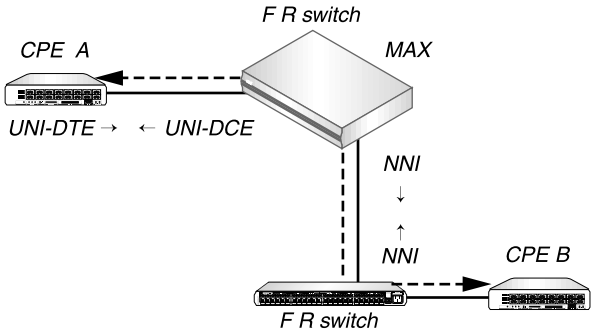


Figure 4-10. A Frame Relay circuit

ATT-DCE is the Frame Relay profile for the UNI-DCE interface in the MAX. ATT-NNI is the Frame Relay profile for the NNI interface. To configure this circuit:

1 Open the first Connection profile.

2 Specify the station name, activate the profile, and specify FR_CIR encapsulation.

```
Ethernet
   Connections
      Station=victor
      Active=Yes
      Encaps=FR_CIR
```

3 Open the Encaps Options subprofile and specify the name of the Frame Relay profile with a nailed connection to the Frame Relay switch, a DLCI assigned by the Frame Relay administrator, and a name for the Frame Relay circuit.

```
Encaps options...
   FR Prof=ATT-DCE
   DLCI=18
   Circuit=Circuit-1
```

4 Close the Connection profile.

5 Open the second Connection profile.

6 Specify the station name, activate the profile, and specify FR_CIR encapsulation.

```
Ethernet
   Connections
      Station=marty
      Active=Yes
      Encaps=FR_CIR
```

7 Open the Encaps Options subprofile and specify the name of the Frame Relay profile with a nailed connection to the Frame Relay switch, a DLCI assigned by the Frame Relay administrator, and a name for the Frame Relay circuit.

```
Encaps options...
   FR Prof=ATT-NNI
   DLCI=23
   Circuit=Circuit-1
```

8 Close the second Connection profile.

Configuring a redirect connection

This example shows the configuration of two PPP dial-in connections to be redirected out to the Frame Relay network.

Note: A Frame Relay redirect connection is not a full-duplex tunnel between the PPP dial-in and the switch. MAX router software handles IP packets coming back from the Frame Relay switch, so they must contain the PPP caller's IP address for accurate routing back across the WAN. Figure 4-11 shows an example of a redirect connection.

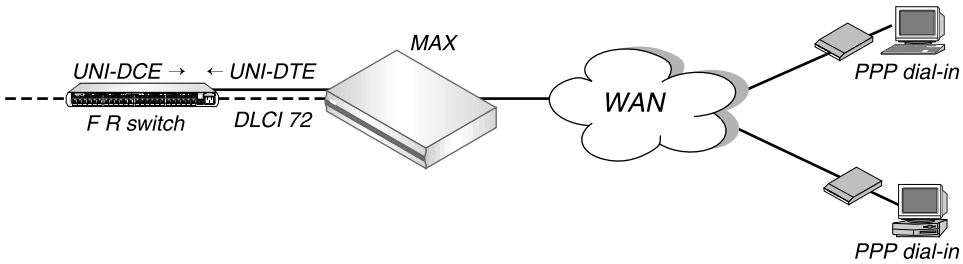


Figure 4-11. Redirect connection

In this example, the MAX communicates with ATT-DTE, a Frame Relay switch using a Frame Relay profile. To configure two PPP dial-in connections to be redirected using the same DLCI:

1 Open a Connection profile.

2 Specify the station name, activate the profile, and specify PPP encapsulation.

```
Ethernet
   Connections
      Station=caller-1
      Active=Yes
      Encaps=PPP
```

3 Make sure you enable IP routing.

```
Route IP=Yes
```

4 Open the Session Options subprofile, enable FR Direct, and specify the name of the Frame Relay profile to use.

```
Session options...
   FR Direct=Yes
   FR Prof=ATT-DTE
```

5 Assign a DLCI available for this redirect connection, which may already be in use by other redirect Connection profiles.

```
FR DLCI=72
```

6 Close the Connection profile.

7 Open a second Connection profile.

8 Specify the station name, activate the profile, and specify PPP encapsulation.

```
Ethernet
   Connections
      Station=caller-2
      Active=Yes
      Encaps=PPP
```

9 Make sure you enable IP routing.

```
      Route IP=Yes
```

10 Open the Session Options subprofile, enable FR Direct, and specify the name of the Frame Relay profile to use.

```
      Session options...
         FR Direct=Yes
         FR Prof=ATT-DTE
```

11 Assign a DLCI available for this redirect connection. For example, you may assign the same DLCI used in the previous redirect Connection profile.

```
         FR DLCI=72
```

12 Close the Connection profile.

Monitoring Frame Relay connections

The terminal server command-line interface has new Show FR commands for monitoring Frame Relay in the MAX. To see the options, invoke the terminal server interface (System > Sys Diag > Term Serv) and then use the `Show FR` command. For example:

```
ascend% show fr ?

show fr ?           Display help information
show fr stats       Display Frame Relay information
show fr lmi         Display Frame Relay LMI information
show fr dlci [name] Display all DLCI information or just for [name]
show fr circuits    Display the FR Circuit table
```

Displaying Frame Relay statistics

To display Frame Relay statistics:

```
ascend% show fr stats

Name         Type   Status    Speed    MTU     InFrame     OutFrame
fr1          DCE    Down     64000    1532           0           1
fr1-temp     DCE      Up     64000    1532           0           1
fr1-temp-9   DCE      Up     64000     1532          0           0
```

The output contains these fields:

- Name: The name of the Frame Relay profile associated with the interface.
- Type: The type of interface.
- Status: The status of the interface. “Up” means the interface is functional, but is not necessarily handling an active call. “Down” means the interface is not functional.

- Speed: The data rate in bits per second.
- MTU: The maximum packet size allowed on the interface.
- InFrame: The number of frames the interface has received.
- OutFrame: The number of frames transmitted.

Displaying link management information

To display LMI (Link Management Information) for each link activated by a Frame Relay profile, enter this command:

```
ascend% show fr lmi

T1_617D LMI for fr1
  Invalid Unnumbered info        0  Invalid Prot Disc
0
  Invalid Dummy Call Ref         0  Invalid Msg Type
0
  Invalid Status Message         0  Invalid Lock Shift
0
  Invalid Information ID         0  Invalid Report Type
0
  Num Status Enqs Sent           0  Num Status Msgs Rcvd
0
  Num Update Status Rcvd          0  Num Status Timeouts
2779

LMI is not on for fr1-temp

LMI is not on for fr1-temp-9
```

ANSI T1.617 Annex D local in-channel signaling protocol is the basis for this information. (See Annex D for a full definition of each of the fields reported.)

Displaying DLCI status

To display the status of each DLCI:

```
ascend% show fr dlci

DLCIs for fr1

DLCIs for fr1-temp

eng-lab-236-Cir   DLCI =   17    Status = ACTIVE
        input pkts              0        output pkts             0
        input octets            0        output octets           0
        input FECN              0        input DE                0
        input BECN               0
last time status changed: 03/05/1997  14:44:17

DLCIs for fr1-temp-9

eng-lab-236-Cir-9  DLCI =   16    Status = ACTIVE
        input pkts              0        output pkts             0
        input octets            0        output octets           0
        input FECN              0        input DE                0
        input BECN               0
last time status changed: 03/05/1997  14:45:07

DLCIs not assigned
```

The MAX reports DLCI information using these fields:

- DLCI: The DLCI number.
- Status: ACTIVE if the connection is up or INACTIVE if not.
- input pkts: The number of frames the interface has received.
- output pkts: The number of frames the interface has transmitted.
- input octets: The number of bytes the interface has received.
- output octets: The number of bytes the interface has transmitted.
- in FECN pkts: The number of packets received with the FECN (Forward Explicit Congestion Notification) bit set. This field always contains a 0 (zero) because congestion management is not currently supported.
- in BECN pkts: The number of packets received with the BECN (Backward Explicit Congestion Notification) bit set. This field always contains a 0 (zero) because congestion management is not currently supported.
- in DE pkts: The number of packets received with the DE (Discard Eligibility) indicator bit set.
- last time status changed: The last time the DLCI state changed.

Displaying circuit information

The `Show FR Circuit` command shows the Frame Relay profile name, DLCI, and status of configured circuits.

```
ascend% show fr circuits

cir-9 User Setting Up
fr1-temp-9                  16          Up
fr1-temp                    17          Up
```

Turning off a circuit without disabling its endpoints

The `Set Circuit` command enables you to *turn off* traffic going through a Frame Relay circuit without disabling the circuit endpoints. This command prevents traffic from going between endpoints without disrupting the state of the DLCI. To see the support options:

```
ascend% set circuit ?

set circuit ?       Display help information
set circuit active [name]  Set the CIRCUIT to active
set circuit inactive [name]  Set the CIRCUIT to inactive
```

To allow data to flow through a circuit, use the active parameter; for example:

```
ascend% set circuit active circuit-1
```

- To turn off data flow without disrupting the state of the DLCIs, use the inactive parameter; for example:

```
ascend% set circuit inactive circuit-2
```

AppleTalk Routing

5

This chapter covers the following topics:

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. The following AppleTalk protocols are supported:

- 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

With AppleTalk routing, 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:

- Reducing broadcast and multicast traffic over the WAN
- Providing 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. Since 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 above, 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 are comprised 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 set into 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, since some routers regard zone names as case-sensitive, it is advisable to be consistent in spelling zone names when you configure multiple connections or routers.

Extended and non-extended AppleTalk networks

AppleTalk subnetworks are either non-extended or extended. Non-extended networks theoretically allow up to 254 nodes. A non-extended network has one network number (not a range) and one zone. Examples of non-extended networks are LocalTalk and ARA dial-up networks.

An extended network is a group of non-extended 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 set into 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 0 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.

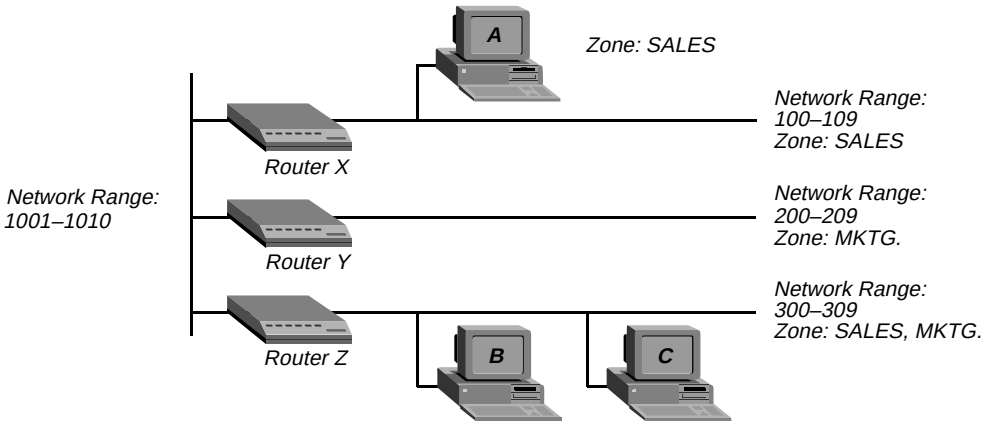


Figure 5-1. AppleTalk LAN

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.

How AppleTalk works

The following is a brief description of how the workstation user sees a typical AppleTalk connection and describes in a general way what is happening as the user makes the choices that lead to a connection. This example supposes a connection between a workstation on a MAX 4000 connected to Pipeline 75 over a synchronous PPP connection, as shown in Figure 5-2.

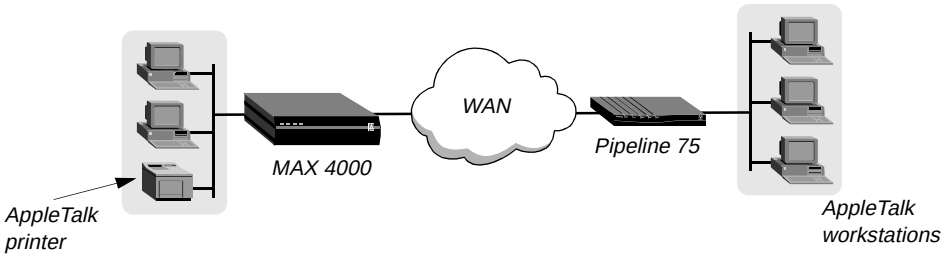


Figure 5-2. Routed connection

1 An AppleTalk workstation user opens the Chooser for the first time since it has been attached to the router and configured.

The zones that appear are in the local Ethernet zone (in this case the WAN zone is the same as the local Ethernet zone), configured in the Connection profile for the MAX. This information is stored in the MAX.

2 The workstation sends a ZIP Query to obtain an updated zone list from the 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 an NBP Broadcast Request to the MAX, which checks its Zone Information Table to determine which subnetwork that printer is located in, and sends the request to the other 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 hear and pick up the NBP Lookup.

7 The selected printer obtains the sender's address from the Lookup packet (in this case the routers are *forwarders*; 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 MAXs continue to pass routing information.

How AppleTalk works

Figure 2 shows a typical AppleTalk connection. The AppleTalk workstation is part of an Ethernet LAN connected to a Pipeline 75, which has a synchronous PPP WAN connection to a MAX 4000. One of the MAX 4000 ports is on a LAN that includes an Apple Laserwriter printer. Following is a brief, generalized description of how the workstation sends a file to the Laserwriter for printing:

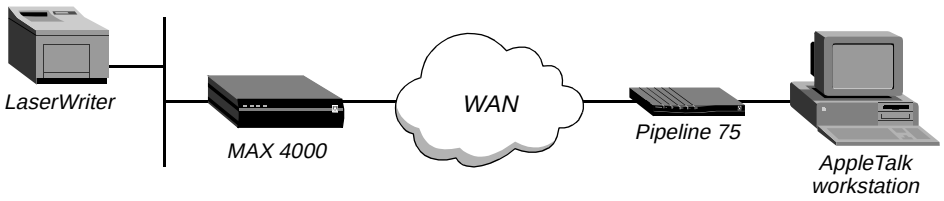


Figure 5-3. Routed connection

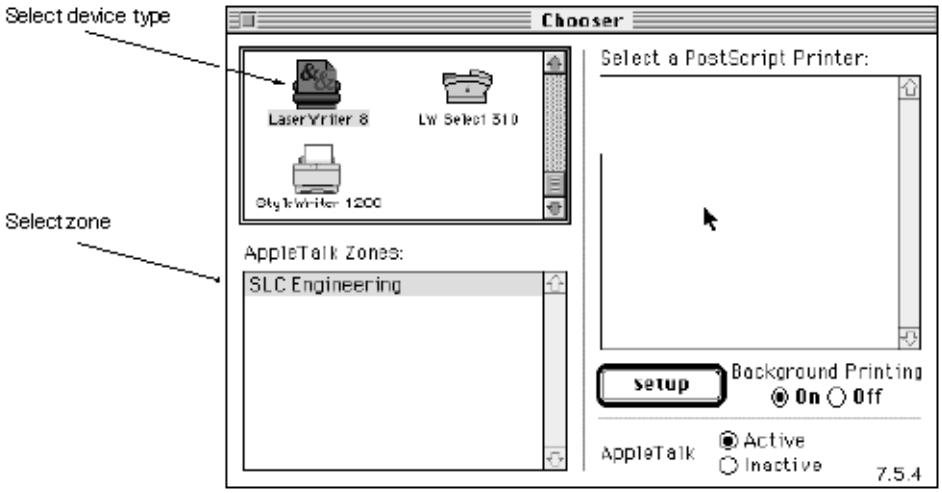
1 The AppleTalk workstation user opens the Macintosh Chooser.

The screen displays the network zones specified by the Connection profile stored in the Pipeline. (The first time a user opens the chooser, only the local Ethernet zones appear. That is, the WAN zone is the same as the local Ethernet zone.)

2 The Pipeline places the call and negotiates the WAN connection with the MAX 4000.

3 The workstation sends a ZIP Query to obtain an updated zone list from the MAX 4000, and the MAX returns the updated zone list. The new list, which might contain different zones from the initial zone list, replaces the initial list in the display and updates the Connection profile in the Pipeline.

4 The user selects a zone and a specific device in the Chooser. For example:



5 The workstation sends a Name Binding Protocol (NBP) Broadcast Request to the Pipeline, which checks its Zone Information Table to identify the subnetwork in which that printer is located, and then sends the request to the MAX via the port configured in the Connection Profile.

6 The MAX determines the port to which the printer's subnetwork is attached, and looks up the printer by searching the multicast address assigned to the zone specified by the Pipeline.

7 All devices in the zone detect and process the NBP-lookup packet.

8 The selected printer obtains the sender's address from the lookup packet (sent by the workstation and forwarded by the routers), and sends the reply through the routers to the workstation.

9 The user sends the print job to the printer.

10 When the print job is complete and no data packets are passing through the connection, the MAX and the Pipeline continue to pass routing information until the idle timeout closes the connection. RTMP and ZIP packets do not reset the idle timer, but any other routeable packet to the network number or zone name specified for this connection does reset the timer.

After the link is dropped, the Pipeline retains in memory the last zone list displayed. If the workstation user opens the Chooser again, the list reappears and the process can begin again.

Configuring AppleTalk routing

To configure AppleTalk routing, you must complete the steps outlined in "System-level AppleTalk routing parameters" and "Per-connection AppleTalk routing parameters" (if required).

System-level AppleTalk routing parameters

To set the required parameters in the Ethernet Configuration profile,

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

2 Set AppleTalk to Yes.

You must set AppleTalk to Yes to be allowed to 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:

```
90-B00 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:

```
90-B00 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 non-seed router boots, it has no local network configuration. It examines local network traffic and learns its local network configuration.

Note: You should configuring the MAX as a non-seed 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 non-seed 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'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 to 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.

The Default Zone and additional zone list need to be identical for any AppleTalk router sharing the local network segment.

Note: Zones can be shared across network segments.

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.)

The Default Zone and additional zone list need to be identical for any AppleTalk router sharing the local network segment.

Note: Zones can be shared across network segments.

Answer profile parameter

If you configure the MAX to authenticate via names and passwords, enable AppleTalk routing in the Ethernet > Answer profile by selecting Route AppleTalk=Yes. For example:

```
90-700 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 the 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 option 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 Ascend unit 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 to 65,534. If there are other AppleTalk routers on the network, it is necessary to configure the network ranges to coincide with the other routers on the LAN.

Configuring an AppleTalk connection with RADIUS

You can configure an AppleTalk-routed connection via a RADIUS user profile and configure static AppleTalk routes in a RADIUS pseudo-user file. See the MAX *RADIUS Configuration Guide* for more information.

Additional information about AppleTalk

This feature note 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

This chapter covers these topics:

Introduction to Ascend X.25 implementation

This chapter describes X.25 support on the MAX. The CCITT Blue Book Recommendation X series 1988 has full technical specifications for X.25, X.3, X.28, X.29, and LAPB (Link Access Protocol–Balanced). IETF RFC 1356 has 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, transfer of expedited data, 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 switch involves the following elements:

- A physical interface to the X.25 switch

  The MAX typically has a nailed connection to an X.25 switch via serial WAN, T1 or E1 PRI, or BRI. (X.25 PAD connections require a leased line or nailed ISDN connection.) The MAX supports only one physical connection for X.25 support. For details on configuring these interfaces, see Chapter 2, “Configuring the MAX for WAN Access.”

- A logical datalink to the X.25 DCE (defined in an X.25 profile)

  The MAX unit’s logical link is usually a switched virtual circuit (SVC). See “Configuring the logical link to a X.25 switch” on page 6-2.

- Dial-in connections that use X.25 (defined in Connection profiles)

  The application layer of an X.25 connection may be a TCP/IP network connection or terminal emulation using X.25 PAD (Packet Assembler/Disassembler). See “Configuring X.25 IP connections” on page 6-7 and “Configuring X.25 PAD connections” on page 6-10.

Configuring the logical link to a X.25 switch

A X.25 profile defines the logical data link between the MAX and a remote X.25 switch. The Ethernet menu contains X.25 profiles, with following parameters:

```
Ethernet
      X.25...
      Name=x25prof
      Active=Yes
      Call Type=Nailed
      Nailed Grp=32
      Data Svc=64K
      PRI # Type=N/A
      Dial #=N/A
      Bill #=N/A
      Call-by-Call=N/A
      Transit #=N/A
      LAPB T1=3
      LAPB T2=0
      LAPB 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=4096
      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 R22=1
      X.25 T23=18
      X.25 R23=1
      X.121 src addr=
      VCE Timer Val=300
```

For more information about each of these parameters, see the *MAX Reference Guide*.

Understanding the X.25 parameters

This section provides some background information about the X.25 parameters.

Profile name and activation

User connections link up with the X.25 connection specified in this profile by specifying the profile name. The name must be unique and cannot exceed 15 characters.

Set the Active parameter to Yes to make this profile available for use.

Physical connection type

The call type may be nailed or switched (X.25 PAD requires nailed). If it is a nailed connection, specify the Nailed Grp number. If it is a switched call, specify the Dial # and telco options.

LAPB and reliable data transfer

The X.25 frame layer implements LAPB (Link Access Protocol–Balanced), an HDLC-like protocol that facilitates the exchange of information packets.

- LAPB T1 is the maximum number of seconds the transmitter waits for acknowledgment before initiating a recovery procedure (Response timeout). The default is 3 seconds.
- LAPB T2 is maximum number of milliseconds LAPB waits for outgoing data before sending a Restart-Request packet to the network. The default zero means immediate acknowledgment.
- LAPB N2 specifies 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 specifies the maximum number of sequentially numbered frames that may 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.

- X.25 Seq Number Mode selects between modulo 8 or modulo 128 sequence number mode. NORMAL is modulo 8 (the default), EXTENDED is modulo 128.
- 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 comes up sending a DISC, and the packet layer sends a Restart-Request packet at initialization. In PASSIVE disconnect mode the link layer comes up sending SABM(E), and issues a restart to the network only upon receipt of a request restart token. 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 DCE.
- X.25 window size establishes the maximum number of data packets that can be outstanding before the MAX requires an acknowledgment. The default is 2.
- X.25 packet sizes specify the default, maximum, and minimum number of bytes in the data field of a data packet.

X.25 PVC and SVC numbers

- The highest and lowest PVC numbers define a range of PVCs between 1 and 4096. If the lowest PVC number is zero, no PVCs are supported.
- The highest and lowest SVC numbers define a range of SVCs between 1 and 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 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

X.25 options can be set to None (no options) or NPWS (specifying that the MAX negotiates packet and window size). None is the default.

X.25 reverse charge accept

This parameter specifies whether the MAX accepts call packets with "0101" in the facility field to request reverse charge. The default is No.

X.25 network type

Currently, the MAX supports only the CCITT network type.

Controlling Restart-Requests

X.25 T20 sets the duration of the Restart timer (the number of ten-second ticks the MAX waits before retransmitting a Restart-Request packet) and the corresponding X.25 R20 parameter specifies the number of Restart-Request retransmits the MAX sends before waiting indefinitely for a response.

Controlling Call-Requests

X.25 T21 sets the duration of the Call-Request timer (the number of ten-second ticks the MAX waits before clearing an unacceptable outgoing call).

Controlling Reset-Requests

X.25 T22 sets the duration of the Reset-Request timer (the number of ten-second ticks the MAX waits before retransmitting a Reset-Request packet) and the corresponding R22 parameter specifies the number of times the MAX retransmits a Reset-Request packet before clearing a call.

Controlling Clear-Requests

X.25 T23 sets the duration of the Clear-Request timer (the number of ten-second ticks the MAX waits before retransmitting a Clear-Request packet) and the corresponding R23 parameter specifies the number of Clear-Request retransmits the MAX sends before waiting indefinitely for a response.

X.121 source address is MAX source address for logical links using this profile.

An X.121 address contains between 1 and 15 decimal digits, such as 031344159782738.

Setting the VCE (Virtual Call Establishment) timer value

Virtual Call Establishment timer interval 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 disables this timer system-wide regardless of the value of the VC timer enable flag per connection. The default is 300 seconds.

Example X.25 profile configuration

This example configuration shows an example 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 on configuring physical nailed connections, see Chapter 2, “Configuring the MAX for WAN Access.”

Note: You must obtain a copy of the telco’s subscription form containing the values provisioned in the switch and configure the MAX X.25 profile to comply with those values.

Table 6-1 shows a sample telco subscription form for X.25 service:

Table 6-1. Sample Telco subscription form

Subscription Form	Value	X.25 Profile
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 may 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

Table 6-1. Sample Telco subscription form (continued)

Subscription Form	Value	X.25 Profile
Maximum packet size:	2048	X.25 Max pkt size=2048
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 highest 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:	2048	X.25 Max pkt size=2048

To configure the X.25 profile to comply with this subscription form:

1 Open the X.25 profile, assign the profile a name, and activate it.

```
Ethernet
   X.25...
      Name=ATT
      Active=Yes
```

2 Set the 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=4096
```

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. These are the related parameters:

```
Ethernet
   Answer
      Encaps...
      X25/IP=Yes

Ethernet
   Connections
      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 more 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.

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.

LCN (logical channel number) number

The LCN specifies the logical channel number to use in the case of a PVC. The default zero means the MAX does not provide LCN, so the connection is not a PVC.

Encapsulation type

The encapsulation type may be RFC877 for backward compatibility, SNAP, or NULL (multiplexing) encapsulation. This fields 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.

X.25 reverse charge

This 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

This parameter 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

This parameter 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

This parameter 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.

Maximum number of unsuccessful calls

You can specify the maximum number of unsuccessful X.25 calls the MAX tries to place before dropping the modem connection. The default zero means an unlimited number.

Inactivity timer

The inactivity timer specifies the number of seconds to allow a connection to remain inactive before dropping the virtual circuit.

MRU

This parameter specifies the maximum number of bytes the MAX can receive in a single IP packet on the X.25 link. The IP packet is further fragmented/reassembled to fit the maximum X.25 packet size, if the MRU is larger than the X.25 packet size. The default is 1500 bytes.

Call mode

The call mode specifies whether the MAX can initiate a call request on this connection.

- Incoming means 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 address matches the Answer X.121 address (below), the MAX accepts the call.
- Outgoing means the MAX issues a call request to the Remote X.121 address (below) 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 means the MAX accepts both incoming and outgoing call requests if the CUD indicates encapsulation that are supported. The called address must match the Answer X.121 address. If the MAX does not establish a virtual circuit and IP packets show up, the MAX issues a call request to the Remote X.121 address.

Answer X.121 address

This specifies the X.121 address of the remote X.25 host to which this profile connects. The remote host also supports RFC1356 encapsulation of IP packets. This field cannot be left empty if you set Call Mode to Both or Incoming.

Remote X.121 address

This specifies the X.121 address of the remote X.25 host to which this profile connects. The remote host also supports RFC1356 encapsulation of IP packets. This field cannot be left empty 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 using PPP encapsulation. You must specify the address of the remote Ascend unit in the LAN Adrs parameter. If you are using numbered interfaces, you can also specify local IF Adrs and a remote WAN Alias value. For details on IP routing configurations, see Chapter 10, “Configuring IP Routing.”

Example X.25 IP configuration

This section shows an example configuration enabling two IP networks to connect through a Public or Private Packet Switched Network (PSPDN).

Figure 6-1. Example X.25 IP connection

To configure this example 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
      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. For example, set it to 30 seconds.

```
         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 PAD (Packet Assembler/Disassembler) 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 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 types PAD 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 may see the terminal-server command line or be directed immediately to an X.121 host. If the connection auto-calls an X.121 host, the initial session display looks like this:

```
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 instead. 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
```

See "X.25 PAD commands" on page 6-17 for more details. This section describes how to configure these X.25 PAD connections. These are the related parameters:

```
Ethernet
   Answer
      X25 Options...
         X25/PAD=Yes
         X.25 Prof=ATT
         Recv PW=localpw
         LCN=0
         X.3 Param Prof=CRT
         Max Unsucc. calls=0
         VC Timer enable=DISABLE
         Auto-Call X.121 addr=
         Reverse Charge=No
         X.3 Custom=

Ethernet
   Connections
      Encaps=X25/PAD
      Encaps options...
         X.25 Prof=ATT
         Recv PW=localpw
         LCN=0
         X.3 Param Prof=CRT
         Max Unsucc. calls=0
         VC Timer enable=DISABLE
         Auto-Call X.121 addr=
         Reverse Charge=No
         RPOA=1234
         CUG Index=
          NUI=
         X.3 Custom=
```

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

Understanding the X.25 PAD connection parameters

This section provides some background information about the X.25 PAD connection parameters.

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 cannot be saved unless you name the X.25 profile and make it active.

Receive password

This specifies a case-sensitive password to use to authenticate the caller.

LCN (logical channel number) number

The LCN specifies the logical channel number to use in the case of a PVC. The default zero means the MAX provides no LCN, so the connection is not a PVC.

X.3 parameter profile

Table 6-3 on page 17 lists supported X.3 parameter profile. You can specify a profile using a PAD command, and you can specify a connection default profile in the X.3 Param Prof parameter. A profile specified on the command line overrides this default for the length of the current session.

Maximum number of unsuccessful calls

You can specify the maximum number of unsuccessful X.25 calls the MAX tries to place before dropping the modem connection. The default zero means an unlimited number.

VC (Virtual Call Establishment) timer enabled

You can enable or disable use of the VCE timer on a per-user basis. The VCE timer 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.

Auto-call to an X.121 address

The Auto-Call X.121 Addr specifies an X.25 host to call immediately when the MAX establishes an X.25/PAD session via this Connection profile. If this parameter specifies an address, the PAD session can begin automatically; otherwise, the MAX displays the terminal-server prompt, where the user can issue the `pad` command to begin a session.

X.25 reverse charge

This parameter specifies whether the X.25 facility field indicates *reverse charge request* when the X.25 user calls a host. The default is No.

X.3 Custom

Ascend's X.25/PAD implementation contains ten permanent X.3 parameter profiles that contain settings for a range of devices, such as terminals and printers. However, these profiles do not cover all devices. You can define a new profile that describes a device not specified by the permanent profiles.

Example X.25 PAD configuration

This section shows an example configuration in which the MAX directs the X.25 modem caller immediately to a PAD interface on the host whose X.121 address appears in Figure 6-2.

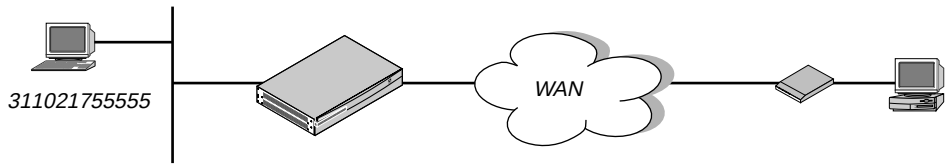


Figure 6-2. Example X.25 PAD connection

To configure this example 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
      Name=rchan
      Active=Yes
```

3 Enable X.25/PAD encapsulation and then open the Encaps Options subprofile.

```
      Encaps=X25/PAD
```

4 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 to auto-call.

```
         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

The user's terminal or host DTE can modify operations the PAD performs by setting one or more X.3 parameters or by applying an X.3 profile. This section lists the X.3 parameters and profiles and then describes how to set them from the PAD. These are the X.3 parameters, numbered 1 through 22.

Table 6-2. X.3 parameters

Parameter	Description	Possible values
1r	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
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

Table 6-2. X.3 parameters (continued)

Parameter	Description	Possible values
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 the 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 ...
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)

Table 6-2. X.3 parameters (continued)

Parameter	Description	Possible values
13	Linefeed insertion after carriage return	0—Option not selected 1—Linefeed insertion after a carriage return in data the PAD sends to the DTE-C 2—Linefeed insertion after a carriage return in data the PAD receives from the DTE-C 4—Linefeed insertion after echo of each carriage return to the 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 the International Alphabet #5)
17	Line delete	0–127 (a character from the International Alphabet #5)
18	Line display	0–127 (a character from the International Alphabet #5)
19	Editing PAD service signals	0—No editing PAD service signals 1—Editing PAD service signals
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 supported X.3 profiles, shown with the profile name and the settings of each X.3 parameter in that profile.

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
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.

To display a list of all X.25 PAD commands and syntax, use the Help command. Underlined letters in a command indicate the minimum string you have to type to execute the command. For example:

```
HELP
```

Commands for working with X.3 parameters and profiles

These 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, it 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 17), 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>,...]]

  This command is identical to the Set command immediately above, 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 non-standard X.3 parameters that control tab expansion. You cannot access these parameters by the remote host using Q-bit packet PAD commands. You must keep the PAD's view of the current screen position accurate by setting EXP to 0 (zero) and LCL to the number of columns to which your terminal expands tabs. These settings enable the PAD to perform correct line folding, line deletion, and character deletion.

  – The LCL keyword 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 between 0 and 16. Zero specifies that no expansion takes place.

  – The REM keyword 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 between 0 and 16. Zero specifies that no expansion takes place.

  – The EXP keyword enables (1) or disables (0) tab expansion locally. If you specify 1 after this keyword, the MAX expands tabs according to the LCL specification.

There 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, it 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>,...]]
  This command is identical to the Set command immediately above, except that it displays all X.3 parameter values after setting those specified on the command line.

X.25 PAD commands for managing calls

These are the commands you can enter 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 uses 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.
  - When 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 value you specify from hexadecimal format and 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 details on these features, see "X.3 parameters and profiles" on page 6-14.

  If you disable echo, the amount of processing the PAD must do 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.

  – When you specify an asterisk (*), the MAX does not echo any characters.

  – When 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.

  – When 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 using any previously entered Half command.

- INTERRUPT

  The Interrupt command generates an Interrupt packet. An Interrupt packet can transmit between 1 and 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 and flow-control packets.

- LISTEN [ADDR=<address> | DATA=<data>]

  The Listen command specifies the match pattern for accepting an incoming call. It uses this 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 on this asynchronous port.

  – 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 on this asynchronous port.

- RESET

  The Reset command resets a virtual circuit by generating a Reset-Request packet with 0 (zero) cause (DTE originated) and 0 (zero) diagnostic.

- STATUS

  The Status command requests the status of a virtual call placed to a remote DTE.

PAD service signals

The PAD transmits PAD service signals to the terminal server in order to acknowledge PAD commands and to inform the user about the internal state of the PAD. The terminal server user

can suppress the reception of PAD service signals by setting PAD parameter #6 to 0 (zero). The following table 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 entered an X.25/PAD command using faulty syntax.
CLR	A virtual circuit has been cleared.
ENGAGED	In response to the STAT command, this signal indicates that a virtual call is up.
FREE	In response to the STAT command, this signal indicates that a virtual call is 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

Table 6-5. Clear cause codes (continued)

Hex value	Cause code
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

Table 6-6. X.25 diagnostic field values (continued)

Hex value	Dec value	Diagnostic
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
29	41	Restart packet with non-zero 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 all 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

Table 6-6. X.25 diagnostic field values (continued)

Hex value	Dec value	Diagnostic
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

Monitoring X.25 and PAD service

The terminal server supports two commands for obtaining information about X.25 and PAD service. To invoke the terminal server, select System > Sys Diag > Term Serv and press Enter.

Displaying information about PAD sessions

To display information about PAD sessions:

```
ascend% show pad

Port   State        LCN        BPS       User     Called Addr.
1     connected      0         9600      rchan     419342855555
2     connected      0         9600      dhersh
```

The output includes the following fields:

- Port: The port for the X.25 connection.
- Stat: The state of the connection.
  - Idle means the PAD is open, but no call has been issued.
  - Calling means a call has been issued and is awaiting acceptance.
  - Connected means the call is connected and in session.

  - Clearing means a Clear command has been issued and the transmitter is awaiting a clear confirmation.
- LCN: The logical channel number for a PVC. An LCN of 0 means this is not a PVC (it is a switched virtual circuit instead).
- BPS: The data rate of the connection in bits per second.
- User: The Connection profile name of the caller.
- Called Add: The X.121 address of the remote node.

Displaying information about X.25

To view information about X.25 frame and packet layers:

```
ascend% show x25

Frame     State           BytesIn        BytesOut
 1        LinkUp            15             45


Packet     State          BytesIn         BytesOut
 1         Ready             0              0
```

The output includes these fields:

- Frame: The frame layer and Packet means the packet layer.
- Stat: The state of the connection at that layer.

  For the frame layer, these states can occur:

  - SABMSent: The MAX sends an SABM (Set Asynchronous Balanced Mode) message to establish the operating mode as LAPB (Link Access Balanced Protocol), and the transmitter is waiting for a UA (Unnumbered Acknowledge response).
  - DISCSent: The MAX sends a DISC message to disconnect the frame level, and the transmitter is waiting for a UA (Unnumbered Acknowledge response).
  - FRMRSent: The MAX sends an FRMR message, indicating that the MAX received a malformed frame, and the sender is waiting for a SABM message.
  - LinkUp: The link is up and sending I-frames and S-frames.
  - Disconnected: The MAX requests a disconnect, and the sender is waiting for a SABM message.

  For the packet layer, these states can occur:

  - Ready: The packet level is ready to send and receive data.
  - DTERestart: The DTE issues a Restart-Request.
  - DCERestart: The DCE issues a Restart-Request.
  - BothRestart: The MAX sends Restart-Requests to both the DTE and the DCE.
  - InitState: Indicates the initial state of a call.
- BytesIn: The number of bytes the MAX receives from the remote node.
- BytesOut: The number of bytes the MAX transmits to the remote node.

Setting up ISDN D-channel X.25 support

In addition to supporting X.25 over ISDN B-channels, the MAX can also support X.25 over the signaling D-channel.

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 value is 23. If you set TEI to 0, the Ascend unit 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 the T3POS protocol, which can be used to send point of sale (POS) data over the ISDN D channel.

The MAX provides X25 Transaction Processing Protocol for Point-of-Service (T3POS) support over the existing Ascend X.25 stack. T3POS is a character-oriented, frame-formatted protocol designed for point-of-service (POS) transactions through an X.25-based packet switched network. T3POS allows 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). See Figure 6-3.

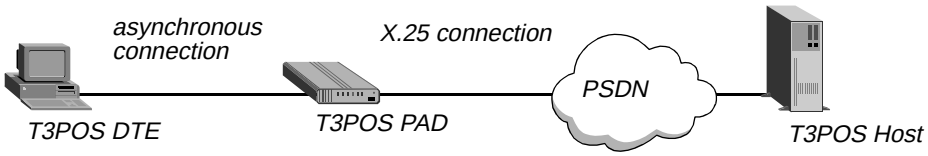


Figure 6-3. T3POS set up

A typical use of T3POS performs credit card authorization over the D channel while using the B channels to transmit inventory control data and other traffic. Figure 6-4 is an example of T3POS setup.

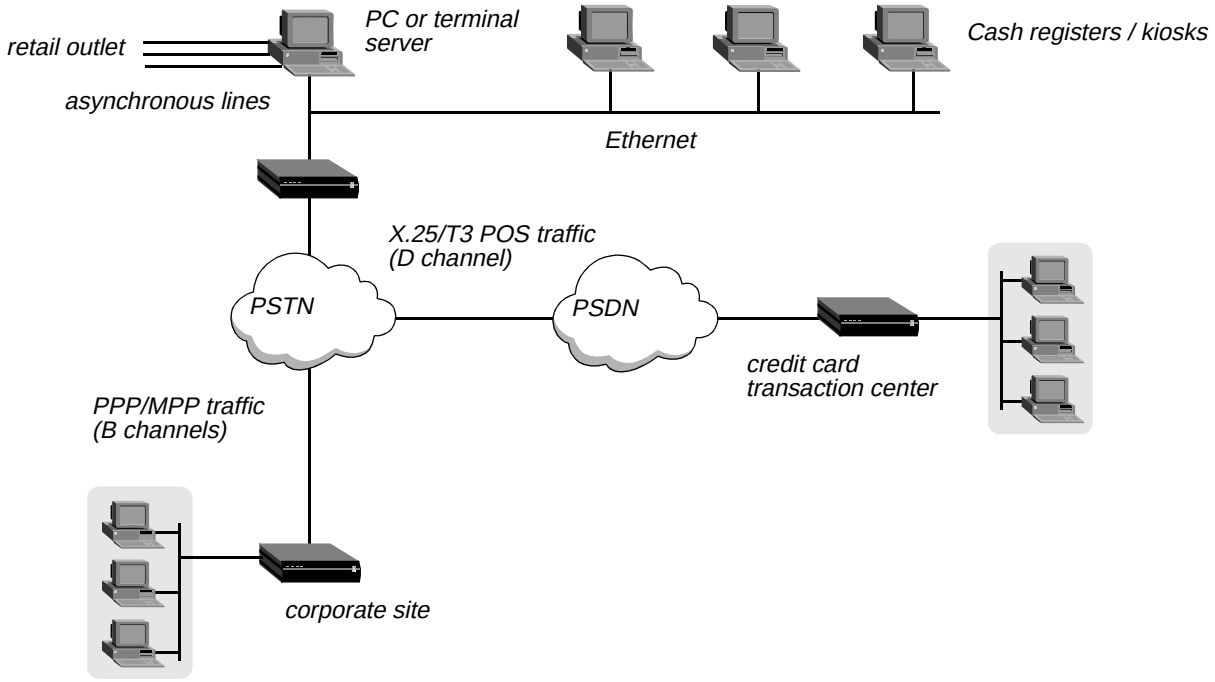


Figure 6-4. Example T3POS configuration

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 on the protocol and the MAX X.25 PAD, refer to the documents listed in “References” on page 6-29.

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 is capable of being transmitted over a packet network. It also ensures reliability and efficiency as described in the protocol.

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 bit no parity, or more accurately 7 bits, 1 parity, but the MAX ignores the parity bit.

T3POS frame types

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). Furthermore, in Local and Binary-local modes and in opening frames, general frames are encapsulated in the 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 control frames only when the MAX establishes 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, the operating mode as well as called number and call user data and some user facilities can be overridden by using a control frame. A control frame is a supervisory frame of the format:

<SOH MSS CUD STX [data] ETX XRC>

where:

- SOH is the ascii character \001
- MSS is the Mode Selection Signal that can be (optionally) used to indicate the mode for the call
- CUD is the Called User Data
  This may 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 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 triggers a call to the host using the settings in the Answer profile (or the Connection profile). When the MAX receives a control frame from the DTE, it also triggers a call to the host. In this case, however, the MAX uses the mode and called address specified in the control frame (if any) for the call, overriding any setting configured in the MAX.

Host-initiated calls

This implementation does not directly support incoming calls to the DTE. Instead, the DTE answers any calls initiated by the host connecting to the T3POS PAD and *listening* for host-initiated calls. The host must send a called address matching the pattern the DTE is listening for. This pattern does not need to be a complete X.121 address, but could be a sub-pattern (including wildcard characters).You configure the listening pattern using the Listen X.121 Addr parameter described in the *MAX Reference Guide*.

Flow control

Flow control should not be an issue for the X25 T3POS implementation. This is 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 to account for the fact that the MAX buffers the data before forwarding it. Note that the current Ascend modem code does RTS/CTS flow control all the time and this cannot be disabled.

References

The T3POS protocols 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.

Refer to the MAX 4.6C and 5.0A addenda for information on the MAX X25/PAD.

Configuring a T3POS connection

You can configure a T3POS connection using either the Connection profile (for authenticated users) or an Answer profile (for unauthenticated users).

Note: For more complete information about each of the T3POS parameters, see the *MAX Reference Guide*.

Configuring a T3POS connection consists of these general steps:

- Create a Connection profile or an Answer profile for the user connecting to the T3POS.
- Create an X.25 profile that defines the X.25 connection the T3POS PAD uses.

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 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 used to authenticate the caller.
7. 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 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. Specify the parameters used for the T3POS connection.
7. Exit and save the Answer profile.

Accessing the T3POS

User 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

This following example describes how to access 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 the port 150 of the MAX.

Note: Telnet client programs should use 8 bit mode to connect to the MAX.

1. 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).
3. Both the Connection and Answer profiles specify that the user is an X.25 user (that is, Encaps is set to X25/T3POS) as well as an X.25 profile that 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, including timers, window size, and so on. For LAPB, the X.25 profile also specifies the nailed group to use for the logical call.
4. The connection is then established using the settings in both the Connection profile (or Answer profile) and the X.25 profile and the call is directed to the T3POS.
5. The user then must use the normal X.25/PAD commands as explained in the MAX 4.6C and 5.0A addenda.

Accessing the T3POS from the MAX terminal server interface

This following example describes how to access the X.25/T3POS from the MAX terminal server interface or through Telnet.

1. From the terminal server prompt, the user enters the T3POS command. For example:

   ```
   ascend% t3pos
   ```
2. The user is then directed to the T3POS PAD and T3POS traffic can now be transmitted.

Accessing the T3POS through immediate mode

To allow access the T3POS PAD immediately upon connecting, set Immediate Service to X25/T3POS in the Ethernet > Mod Config > TServ options submenu. This is typically how users connect to the T3POS PAD.

We recommend that when use immediate service, you suppress the terminal server banner (using the Banner parameter) as well as reducing the PPP delay parameter to its minimum. Both these parameters are in the Ethernet > Mod Config > TServ options submenu.

Defining Static Filters

7

This chapter covers these topics:

Introduction to Ascend filters

A packet filter contains rules describing packets and what to do when those packets are encountered. When you apply a packet filter to an interface, the MAX monitors the data stream on that interface and takes a specified action when packet contents match the filter rules. Depending on the filter definition, it may apply to inbound or outbound packets, or both. In addition, filter rules are flexible enough to take 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. See “Predefined filters” on page 7-20.

Packet filters and firewalls

The MAX supports these types of *static* packet filters:

- Generic filters, which examine the byte- or bit-level contents of any packet.

  Generic filters focus on certain bytes or bits in a packet and compare the contents of that location with a value defined in the filter. To use generic filters effectively, you need to know the contents of certain bytes in the packets you wish to filter. Protocol specifications are usually the best source of such information.
- IP filters, which examine higher-level fields specific to IP packets.

  IP filters focus on known fields in IP packets, such as source or destination address, protocol number, and so forth. They operate on logical information, which is relatively easy to obtain.
- IPX filters, which examine higher-level fields specific to IPX packets.

  IPX filters focus on known fields in IPX packets, such as source or destination address, node, socket, and so forth. They operate on logical information, which is relatively easy to obtain.

The MAX also supports Secure Access, which provides *dynamic* firewalls. Firewalls differ from filters in that they alter their behavior as traffic passes through them, where filters remain

unchanged through their lifetimes. Unlike the static packet filters, which have a limited number of rules, router memory is the only limitation in Secure Access firewalls.

If your MAX unit has Secure Access support installed, see the *Ascend Secure Access User's Guide* (part number 7820-0429-001) for complete instructions on creating and applying firewalls. You can refer to a 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 which packets can or cannot cross the interface
- A call filter, to define which packets 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 apply both a data and call filter, the data filter comes 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 (Figure 7-1).

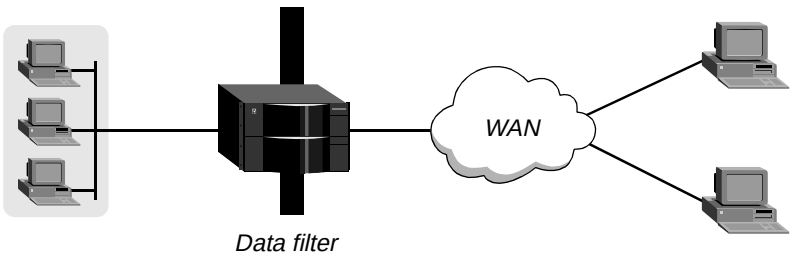


Figure 7-1. Data filters can drop or forward certain packets

Call filters for managing connections

A call filter defines which packets can or cannot bring up a connection or reset the idle timer for an established link (Figure 7-2).

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 (forward or drop) does not affect which packets the MAX sends across an active connection. The forwarding action of a call filter determines which packets 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.

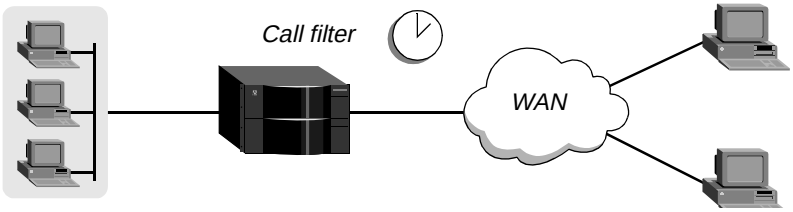


Figure 7-2. Call filters can prevent certain packets from resetting the timer

How packet filters work

This section provides an overview of packet filters and the processes they follow. For more details on filter matching a value in a packet, see "Understanding the packet filter parameters" on page 7-5.

A Filter profile can contain up to 12 input and output filter specifications (rules). Each rule has its own forwarding action—forward or drop. A match occurs at the first successful comparison between a filter and the packet being examined. When a comparison succeeds, the filtering process stops and the forward action in that rule is applied to the packet.

If no comparisons succeed, the packet does not match this filter. However, this does not mean that the MAX forwards the packet. When no filter is in use, the MAX forwards all packets, but once you apply a filter to an interface, this default is *reversed*. For security purposes, the MAX does not automatically forward non-matching packets. It requires a rule that explicitly allows those packets to pass. 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 7-13.

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 only input rules are defined, output packets will keep a connection active, or vice versa.

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 equals or do not equal that number.

In an IP filter, a set of distinct comparisons are made in order. When a comparison fails, the MAX allows a packet to go on to the next comparison. When a comparison succeeds, the filtering process stops and the MAX applies the forward action in that rule to the packet. The IP filter tests proceed in this order:

1. Compare source address parameters to the source address of the packet. If they are not equal, the comparison fails.
2. Compare destination address parameters to the destination address in the packet. If they are not equal, the comparison fails.
3. If the protocol parameter is zero (which matches any protocol), the comparison succeeds. If it is non-zero and not equal to the protocol field in the packet, the comparison fails.

4 If the Src Port Cmp parameter is not set to none, compare the source 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 destination 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 Yes and the protocol number is 6, the comparison succeeds.

Defining packet filters

Filter profiles provide rules for defining which packets will be affected. The rules are the same for Input or Output filters. These are the filter parameters:

```
Ethernet
   Filters
      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
```

Note that the parameters for defining the actual packet conditions are identical for Input and Output filters. For more information about each parameter, see the *MAX Reference Guide*.

Understanding the packet filter parameters

This section provides some background information on configuring packet filters.

Assigning a name to 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.

Enabling a specific In or Out filter

Valid enables or disables the current In or Out filter. When you deactivate a filter, all of its parameters do not apply. (You cannot configure the filter until you enable it.)

Specifying a generic or IP filter type

Set Type to GENERIC or IP. Only the parameters in the corresponding subprofile (Generic or Ip) are applicable.

Generic filter rules

Generic filters can affect any packet, regardless of its protocol type or header fields. They use these parameters:

```
Generic...
   Forward=No
   Offset=14
   Length=8
   Mask=ffffffffffffffff
   Value=aaaa0300000080f3
   Compare=Equals
   More=No
```

This section provides some background information on how these parameters work together.

Defining the action to take when a packet matches the filter

Forward 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.

Specifying an offset to the bytes in a packet to be examined

Offset specifies a byte-offset from the start of a frame to the data in the packet to be tested against this filter. 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 first two byes in the packet (2A and 31) are ignored due to 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.

Specifying the number of bytes to test

Length specifies the number of bytes to test in a frame, starting at the specified Offset. The MAX compares the contents of those bytes to the value specified in the filter's Value parameter. For example, with this 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 applies the mask only to the eight bytes following the two-byte offset.

Masking the value before comparison

Mask is a 16-bit mask to apply to the Value before comparing it to the packet contents at the specified offset. You can use it to fine-tune exactly which bits you want to compare.

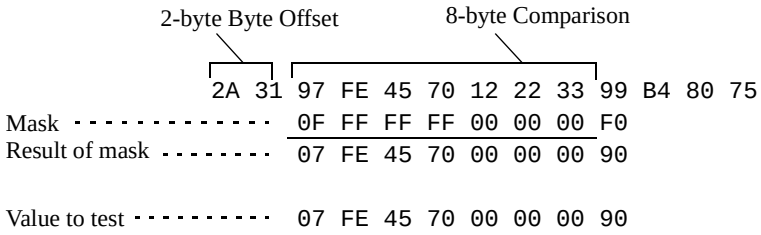
The MAX applies the mask to the specified value using a logical *AND* after the mask and value are both translated into binary format. The mask hides the bits that appear behind each binary 0 (zero) in the mask. A mask of all ones (FF FF FF FF FF FF FF FF) masks no bits, so the full Compare To value 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 as shown below, resulting in a value that matches the Value.



The packet matches this filter. The Filter Action is “Discard”, so the MAX drops the packet. The byte comparison works as follows:

– 2A and 31 are ignored due to the two-byte offset.

– 9 in the lower half of the third byte is ignored, because the mask has a 0 in its place. The 7 in the third byte matches the value parameter’s 7 in the upper half of that byte.

– F and E in the fourth byte match the value parameter for that byte.

– 4 and 5 in the fifth byte match the value parameter for that byte.

– 7 and 0 in the sixth byte match the value parameter for that byte.

- 12 and 22 and 33 in the seventh, eighth and ninth bytes are ignored because the mask has a 0 in those places.
- 9 in the tenth byte equals the matches the value parameter's 9 in the lower half of that byte. The second 9 in the upper-half of the packet's tenth byte is ignored because the mask has a 0 in its place.

The value to match up in the packet contents

Value specifies a hexadecimal number to be compared to specific bits contained in packets after the Offset, Length, and Mask calculations have been applied.

The type of comparison to be performed when matching the packet

Compare specifies the type of comparison to make between the specified value and the packet's contents: less than, equal, greater than, or not equal.

Linking the filter to the next In filter or Out filter in sequence

More specifies whether the MAX includes the next filter condition before determining whether the frame matches the filter. If checked, the MAX links the current filter condition to the one immediately following it, so the filter can examine multiple non-contiguous bytes within a packet. In effect, this parameter *marries* the current filter to the next one, so that the MAX applies the next filter before the MAX decides the forwarding decision. The match occurs only if *both* non-contiguous bytes contain the specified values. The next filter must be enabled; otherwise, the MAX ignores the filter.

IP filter rules

IP filter rules affect only IP and related packets. IP filters use these parameters:

```
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 on how these parameters work.

Defining what action to take when a packet matches the filter

Forward 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 discards matching packets.

Specifying which part of the source IP address to use for comparison

Src Mask 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 applies the mask to the address using a logical *AND* after the mask and address are both translated into binary format. The mask hides the portion of the address that appears behind each binary 0 (zero) 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 matched.

Filtering the packet's source IP address

This 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.

Specifying which part of the destination IP address to use for comparison

Dst Mask specifies a mask to apply to the Dst Adrs 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 applies the mask to the address using a logical *AND* after the mask and address are both translated into binary format. The mask hides the portion of the address that appears behind each binary 0 (zero) 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 matched.

Filtering on the packet's destination IP address

Dst Adrs specifies a destination IP address. After you modify this value by applying the specified Mask, the MAX compares it to a packet's destination address.

Filtering on the protocol number field in IP packets

If you specify a protocol number, the MAX compares it to the protocol number field in packets to match them to this filter. The default protocol number of zero matches all protocols. A list of common protocols appears below. For a complete list of protocol numbers, see the section on Well-Known Port Numbers in RFC 1700, *Assigned Numbers*, by Reynolds, J. and Postel, J., October 1994.

- 1: ICMP
- 5: STREAM
- 8: EGP
- 6: TCP
- 9: Any private interior gateway protocol (such as Cisco's IGRP)
- 11: Network Voice Protocol
- 17: UDP
- 20: Host Monitoring Protocol
- 22: XNS IDP

- 27: Reliable Data Protocol
- 28: Internet Reliable Transport Protocol
- 29: ISO Transport Protocol Class 4
- 30: Bulk Data Transfer Protocol
- 61: Any Host Internal Protocol
- 89: OSPF

Filtering on source port numbers

Src Port # 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; 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 Src Port Cmp parameter specifies the type of comparison to be made.

Filtering on destination port numbers

Dst Port # 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.

Filtering based only on established TCP sessions.

TCP Estab can be used to restrict the filter to packets in an established TCP session. You can only use it if the Protocol number has been set to 6 (TCP). Otherwise, it is not applicable.

Example filter specifications

This section shows some example 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. It 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: AARP (AppleTalk Address Resolution Protocol) packets, AppleTalk packets that are not addressed to the AppleTalk multicast address (such as regular traffic related to an actual AppleTalk File Server connection), and all non-AppleTalk traffic.

The filter then specifies that AEP (AppleTalk Echo Protocol) and NBP (Name Binding Protocol) packets should be dropped. To define this filter:

1 Open a Filter profile and assign it a name. For example:

```
Ethernet
   Filters
      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 specify the following rules:

```
Generic...
   Forward=Yes
   Offset=14
   Length=8
   Mask=ffffffffffffffff
   Value=aaaa0300000080f3
   Compare=Equals
   More=No
```

These rules 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 specify the following rules:

```
Generic...
Forward=Yes
   Offset=32
   Length=6
   Mask=ffffffffffff0000
   Value=090007ffffff0000
   Compare=NotEquals
   More=No
```

These rules specify the multicast address used by AppleTalk broadcasts. The MAX forwards any AppleTalk packet that does not match the specified rules.

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 specify the following rules:

```
Generic...
   Forward=Yes
   Offset=14
   Length=8
   Mask=ffffffffffffffff
   Value=aaaa03080007809b
   Compare=NotEquals
   More=No
```

These rules define the bytes in AppleTalk packets that specifies the protocol type number (0x809b).These rules define non-AppleTalk traffic (packets that do not contain that value in the specified location). The MAX will forward 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 specify the following rules:

```
Generic...
   Forward=No
   Offset=32
   Length=3
   Mask=ffffffffffffffff
   Value=0404040000000000
   Compare=Equals
   More=No
```

These rules specify AEP packets. For details, see *Inside AppleTalk* (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 specify the following rules:

```
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 specify the following rules:

```
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 occurs when a remote device illegally acquires a local address to break through a firewall. This example filter first defines input filters that drop packets whose source address is on the local IP network or the loopback address (127.0.0.0). In effect, these filters say: "If you see an inbound packet with one of these source addresses, drop the packet." The third input filter defines every other source address (0.0.0.0) and specifies "Forward everything else to the local network."

Note: If you apply this filter to the Ethernet interface, the MAX drops IP packets it receives from local LAN and you will not be able to Telnet to the unit.

This example filter then defines an output filter that specifies: "If an outbound packet has a source address on the local network, forward it; otherwise, drop it." The MAX drops all outbound packets with a non-local source address. This filter uses a local IP network address of 192.100.50.128, with a subnet mask of 255.255.255.192. These addresses are just examples. To define this IP filter:

1 Open a Filter profile and assign it a name. For example:

```
Ethernet
   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 specify the following rules:

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

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

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 specify the following rules:

```
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 rules 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 specify the following rules:

```
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 rules specify every other source address (0.0.0.0) If an incoming packet has any non-local source address, the MAX forwards it onto the Ethernet.

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 specify the following rules:

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

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

12 Close the Filter profile.

Defining a filter for more complex IP security issues

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

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

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

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

To define this filter:

1 Open a Filter profile and assign it a name.

```
Ethernet
   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 specify the following rules:

```
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 forward 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 specify the following rules:

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

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 specify the following rules:

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

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 specify the following rules:

```
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. ICMP does not use ports like TCP and UDP, so a port comparison is unnecessary.

11 Close the Filter profile.

Applying packet filters

Filters must be applied to an interface to examine packets passed across that interface in the MAX. They can be applied as a data filter, to forward or drop certain packets, or as a call filter, to affect which packets reset the Idle timer. See “Introduction to Ascend filters” on page 7-1 for background information on these two applications. These are the relevant parameters:

```
Ethernet
   Answer
      Session options...
         Data Filter=0
         Call Filter=0
         Filter Persistence=No

Ethernet
   Connections
      Session options...
         Data Filter=5
         Call Filter=0
         Filter Persistence=No

Ethernet
   Mod Config
      Ether options...
         Filter=1
```

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

Understanding how filters are applied

This section provides some background information about the parameters for applying filters to a local or WAN interface.

- Applying filters in the Answer profile

  The MAX does not apply filters in the Answer profile if the caller has a Connection profile. Use filters only if configured profiles are not required for callers, or if the caller is authenticated using a Name profile. If you use the Answer profile filters, they have the same effect as those ordinarily specified in a Connection profile, described next.

- Specifying a data filter

  A data filter affects the actual data stream on the WAN interface, forwarding or dropping packets according to its rules. See “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 up 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 reset the idle time if the connection is active. See "Call filters for managing connections" on page 7-2.

  If you apply both a data filter and call filter, the data filter comes first. This means that only those packets that pass the data filter reach the call filter.

- Filter persistence

  Before the MAX supported Secure Access, the MAX simply 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 Secure Access firewalls. Filter Persistence is needed to allow firewalls to persist across connection state changes, but it is not needed for filters. If you do set it for a static packet filter, the filter persists across connection state changes. See the *MAX Security Supplement* for details.

- 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 which packets are allowed to reach the Ethernet or 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.

Example configurations applying filters

After you create a filter, as described in "Defining packet filters" on page 7-4, you can apply it as a data filter or call filter. This section shows some example configurations.

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
      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 and resetting the idle timer

When you apply a call filter in a Connection profile, it determines which packets reset the idle timer for a connection. In this example, the idle timer is reset to 20 seconds, so if no packets pass the call filter for 20 seconds, the MAX terminates the connection.

To apply a call filter and reset the idle timer in a Connection profile:

1. Open Connections > 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. Specify 20 seconds in the Idle parameter.

```
Ethernet
   Connections
      Session options...
         Data Filter=0
         Call Filter=2
         Filter Persistence=No
         Idle=20
```

   Or, if the profile specifies a terminal server call, use the TS Idle Mode and TS Idle parameters instead; for example:

```
Ethernet
   Connections
      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.
2. Specify the filter's number in the Filter parameter. For example:

```
Ethernet
   Mod Config
      Ether options...
         Filter=1
```

   (Call filters are not applicable to the local network interface.)
3. Close the Ethernet profile.

Predefined filters

The MAX ships with three predefined Filter profiles, one for each commonly used protocol suite. Some sites modify the predefined call filters to make them more full-featured for the types of packets commonly seen at that site. As shipped, they 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. These 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 definitions 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=0000000000000000
                  Value=0000000000000000
                  Compare=None
                  More=No
         Output filters...
            Out filter 01
               Valid=Yes
               Type=GENERIC
               Generic...
                  Forward=Yes
                  Offset=0
                  Length=0
                  Mask=0000000000000000
                  Value=0000000000000000
                  Compare=None
                  More=No
```

The IP Call filter contains one input filter, which defines all inbound packets, and one output filter, which defines all outbound packets (all outbound packets destined for the remote network).

NetWare Call filter

The design of predefined NetWare Call filter prevents SAP (Service Advertising Protocol) 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, which identify outbound SAP packets and prevent them from resetting the Idle Timer or initiating a call. The definitions 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=fffffffffff0452
               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 based on AppleTalk activity on the LAN, but to prevent inbound packets or AppleTalk Echo (AEP) packets from resetting the timer or initiating a call. It 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 allows all other outbound packets to reset the timer or initiate a call.

```
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

This chapter covers these topics:

Introduction to Ascend bridging

This section provides an overview of packet bridging and explains how the MAX brings up a bridging connection.

The MAX is used as a bridge 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 any nonrouted protocol connectivity with another site
- Link any 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 (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 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, bridging is disabled.

How a bridged WAN connection is initiated

When the MAX is configured 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 is connected).
- 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

A broadcast address is recognized by multiple nodes in a network. 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. When configured as a router only, the MAX discards broadcast packets. When configured 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.

How the MAX establishes a bridged connection

The MAX uses station names and passwords to sync up a bridging connection, as shown in Figure 8-1.

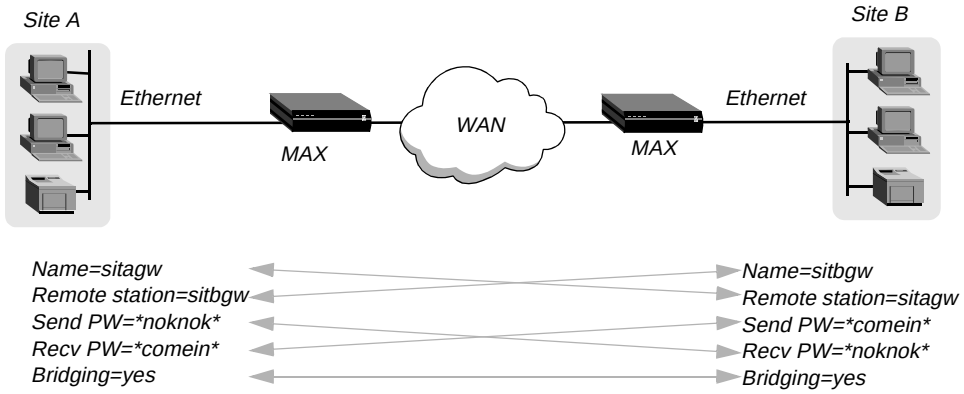


Figure 8-1. Negotiating a bridge connection (PPP encapsulation)

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 may 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 shown above. 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 that the wrong name is specified for the MAX or the remote device. Often case changes are not specified, or a dash, space, or underscore is not entered.

Enabling bridging

The MAX has a system-wide bridging parameter that must be enabled 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 profiles. Bridge profiles are analogous to static routes in a routing environment. You can define up to 99 destination nodes and their connection information in Bridge profiles.

Transparent bridging

The MAX is a transparent bridge (also termed a *learning bridge*). It keeps track of where a particular address is located, and of the Connection profile that specifies the interface to which the packet should be forwarded. As it forwards 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 is configured as a bridge.

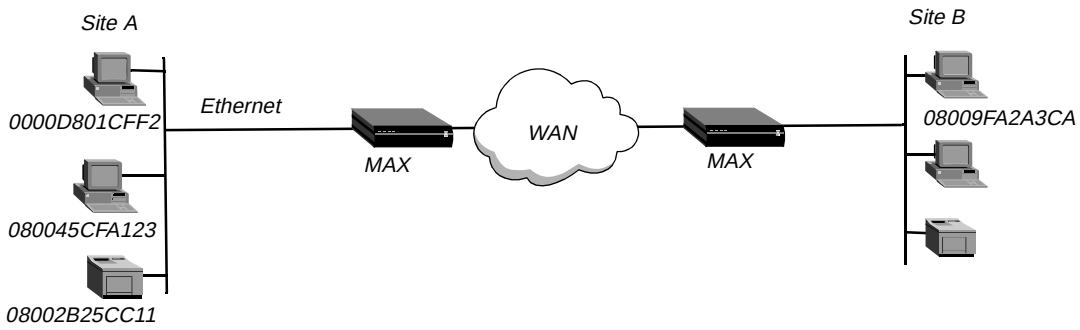


Figure 8-2. How the MAX creates a bridging table

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 like this:

```
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 may be the dial-on-broadcast feature or a Bridge profile (Ethernet > Bridge Adrs). If a connection has an associated Bridge profile, it does not need dial-on-broadcast. You can define up to 100 Bridge profiles.

These are the bridging parameters with example 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
```

For more information on each parameter, see the *MAX Reference Guide*.

Understanding the bridging parameters

This section provides some background information on the bridging parameters.

Bridging in the Answer profile

Both the Bridge parameter and a form of password authentication must be enabled 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. See “Enabling bridging” on page 8-3.

Station name and password

Name and password authentication is required, as described in “How the MAX establishes a bridged connection” on page 8-3.

Bridging and dial broadcast in a Connection profile

Bridge specifies that the Connection will bridge 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. See “How the MAX establishes a bridged connection” on page 8-3.

IPX bridging options

See “IPX bridged configurations” on page 8-8.

Names and passwords

The MAX uses station names and passwords to sync up a bridged connection. These may be provided in a Connection profile, a Name profile, or an external authentication profile.

Bridge profile parameters

If a Connection profile does not use dial broadcast, it must have a bridge table entry for the MAX to be able to bring up the connection on demand. The Bridge profile defines a bridge table entry by specifying three parameters:

Ethernet address

Each bridge table entry specifies an Ethernet (node) address that is not on the local segment. See “Physical addresses and the bridge table” on page 8-2 for details on Ethernet addresses.

Network address

If you are bridging between two segments *of the same IP network*, you can use the Net Adrs parameter in a Bridge profile to enable the MAX to respond to ARP requests while bringing up the bridged connection. See “Configuring proxy mode on the MAX” on page 8-12.

Connection number

You associate bridge 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 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 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.

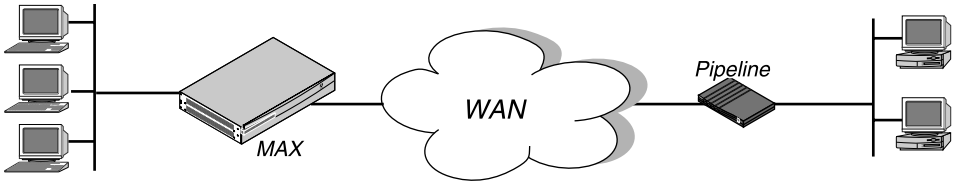


Figure 8-3. An example connection bridging AppleTalk

The most common cause of trouble when initially setting up a bridged connection is that you may have the wrong name specified for the MAX or the remote device. Often, you have not specified case changes, or you did not enter 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 profile is specified. This is not required. You can turn on Dial Brdcast and omit the Bridge profile if you prefer.

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 these 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 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 on the remote network, and the number of the Connection profile to bring up a link to that network.

```
Ethernet
   Bridge Adrs
      Enet Adrs=0080AD12CF9B
```

```
      Net Adrs=0.0.0.0
      Connection #=5
```

8 Close the Bridge profile.

To configure the site B Pipeline unit for the bridged connection:

1 If necessary, assign the remote Pipeline 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 Pipeline unit's Answer profile.

```
Ethernet
   Answer
      PPP options...
         Bridge=Yes
         Recv Auth=Either
```

3 Open Connection profile #2 on the Pipeline and set these 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 profile, configured next.

4 Configure password authentication.

```
      Encaps options...
         Send Auth=CHAP
         Recv PW=remotepw
         Send PW=localpw
```

5 Close Connection profile #2.

6 Open a Bridge profile.

7 Specify a node's Ethernet address on the remote network, and the number of the Connection profile to bring up a link to that network.

```
Ethernet
   Bridge Adrs
      Enet Adrs=0CFF1238FFFF
      Net Adrs=0.0.0.0
      Connection #=2
```

8 Close the Bridge 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 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 does not describe the general bridging parameters explained earlier, although those parameters do apply to an IPX bridging connection. It focuses only on IPX issues.

These are the related parameters:

```
Ethernet
   Mod Config
      Ether options...
         IPX Frame=802.2

Ethernet
   Connections
      Route IPX=No
      IPX options...
         Handle IPX=Client
         NetWare t/o=N/A
```

Here is some background information about these parameters:

IPX frame type

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 Handle IPX parameter sets to N/A, but acts as if set to Server.

How IPX bridged packets are handled

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 do not remain up permanently.

Note: If NetWare servers are supported on both sides of the WAN connection, we strongly recommend that you use an IPX routing configuration instead of bridging IPX. If you bridge IPX in that type of environment, client-server logins will be 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 for remote clients, but to bring down inactive connections whenever possible. To enable this, set the Netware t/o timer. The timer begins counting down as soon as the link goes down. At the end of the specified time, the MAX stops responding to watchdog packets and the client-server connections may be released by the server. If there is a reconnection of the WAN session before the end of the selected time, the timer is reset.

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 will be spoofed.

Example 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. That way, local clients can locate a NetWare server across the WAN, but routine broadcasts do not keep the connection up unnecessarily.

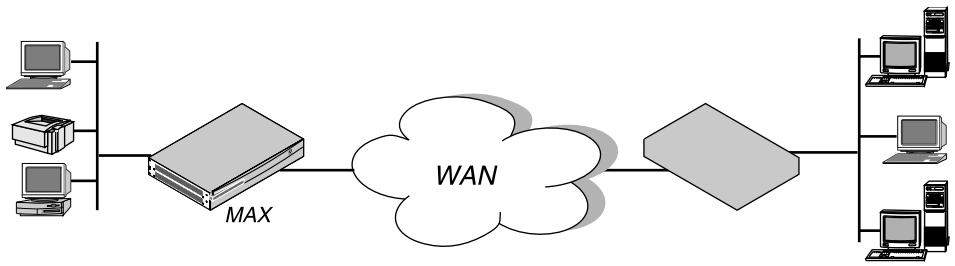


Figure 8-4. An example IPX client bridged connection

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.

```
Ethernet
   Mod Config
      Ether options...
         IPX Frame=802.3
```

3. Enable bridging and specify an authentication protocol in the Answer profile.

```
Ethernet
   Answer
      PPP options...
         Bridge=Yes
         Recv Auth=Either
```

4. Open a Connection profile and set these 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.

```
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 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, a process called *watchdog spoofing*.

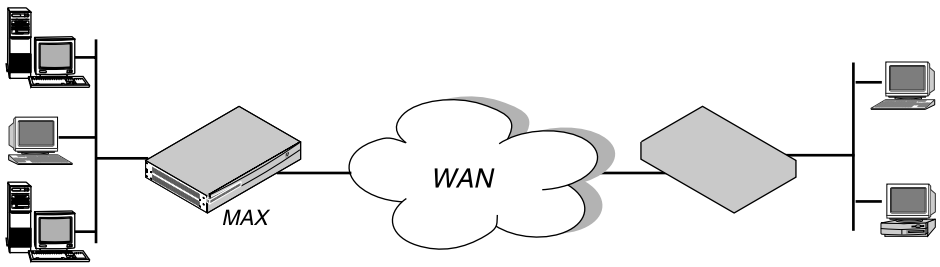


Figure 8-5. An example IPX server bridged connection

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.

```
Ethernet
   Mod Config
      Ether options...
         IPX Frame=802.3
```

3 Enable bridging and specify an authentication protocol in the Answer profile.

```
Ethernet
   Answer
      PPP options...
         Bridge=Yes
         Recv Auth=Either
```

4 Open a Connection profile and set these parameters:

```
Ethernet
   Connections
      Station=SITEBGW
      Active=Yes
      Encaps=PPP
      Route IPX=No
      Bridge=Yes
      Dial Brdcast=Yes
```

5 Configure password authentication.

```
Encaps options...
   Send Auth=CHAP
   Recv PW=localpw
   Send PW=remotepw
```

6 Specify IPX server bridging and configure the timer for watchdog spoofing when an inactive connection has been brought down.

```
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 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 profile, the MAX responds to the ARP request with the Ethernet (physical) address specified in the Bridge 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

This chapter covers these topics:

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 on each of its two local Ethernet interfaces 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 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 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, where 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 that requires password authentication, unless you configure IP routing in the same Connection Profile.

Note: If you have a MAX running Multiband Simulation, IPX routing is disabled.

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. This is analogous to proxy ARP in an IP environment.

Then the client transmits packets whose destination address is the internal address of the server. When the MAX receives those packets, it consults its RIP table. If it finds an entry for that destination address, it brings up the connection or forwards the packet across the active connection.

IPX RIP (Routing Information Protocol) 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 those 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 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 periodically and when you establish a WAN connection. The MAX receives RIP broadcasts from a remote device, adds 1 to 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 it 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 towards 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.

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 where it is physically located. 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 manually activated. 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 9-17, 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 which 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 9-18.

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 on the network with the lowest connection costs. (See your NetWare documentation for more information.)

Consideration	Recommendation
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. (See your NetWare documentation for more information.)
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. The related parameters are:

```
Ethernet
   Mod Config
      IPX Routing=Yes
      Ether options…
         IPX Frame=802.2
         IPX Enet #=00000000
         IPX Pool #=CCCC1234
```

For details on each parameter, see the *MAX Reference Guide*.

Understanding the global IPX parameters

This section provides some background information about IPX routing in the Ethernet profile.

Enabling IPX routing

IPX Routing 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.

Specifying which frame type to route and spoof

The MAX routes and spoofs only one IPX frame type (IEEE 802.2 by default), 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, it bridges them. If you are not familiar with the concept of packet frames, see the Novell documentation.

Setting or learning the proper IPX network number

IPX Enet 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. This causes the MAX to listen for its network number and acquire it from another router on that 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.

Defining a virtual IPX network for dial-in 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. If the client does not have a unique node address, the MAX assigns the node address as well.

Example IPX routing configurations

This section shows the simple configuration, where 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, where these values are entered 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 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 these:

```
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 shown above specifies the number CF0123FF.

Note: IPX network numbers on each network segment and internal network within a server on the *entire WAN* must have a unique network number. 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.

```
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. See Chapter 6, "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 typing Ctrl-C.

Configuring IPX routing connections

This section describes how to configure IPX routing connections. The related Answer and Connection parameters are:

```
Ethernet
   Answer
      PPP options...
         Route IPX
         Recv Auth=Either

      Session options…
         IPX SAP Filter=1

Ethernet
   Connections
      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
```

For more information on each parameter, see the *MAX Reference Guide*.

Understanding the IPX connection parameters

This section provides some background information about IPX connections.

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 which 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.

Applying IPX SAP filters

You can apply an IPX SAP filter to exclude or explicitly include certain remote services from the MAX SAP table. If you apply a SAP filter in a Connection profile, you can exclude or explicitly include services in both directions. See “Creating and applying IPX SAP filters” on page 9-18.

Specifying the station name and password 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 an IPX network address. To allow those clients an IPX routing connection to the local network, the clients must dial in using 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 (see “Understanding the global IPX parameters” on page 9-4).

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 as well. It does not send RIP and SAP advertisements across the connection and 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

IPX RIP and IPX SAP in a Connection profile define how the MAX handles RIP and SAP packets across this WAN connection.

Set IPX RIP to Both by 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 by 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

Dial Query configures the MAX to bring up a connection when it receives a SAP query for service type 0004 (File Server) and 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 chooses to bring up that connection as opposed to 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. It is rarely needed, and is provided only for those remote-end routers that require the MAX to know that router's network number before connecting. The IPX Alias is a second IPX network number, to be used only when connecting to non-Ascend routers that use numbered interfaces.

IPX client or server bridging

Handle IPX defines the handling of bridged connections. When you enable IPX routing for a connection, IPX Routing = N/A. See Chapter 8, "Configuring Packet Bridging."

Watchdog spoofing

Netware t/o defines the number of minutes the MAX enables clients to remain logged in even though their connection terminates.

NetWare servers send out NCP watchdog packets to monitor which logins are active and logout inactive clients. Only clients that respond to watchdog packets remain logged in.

Repeated watchdog packets would cause a WAN connection to stay up, but if the MAX simply filtered those packets, client logins would be dropped by the remote server. To prevent repeated client logouts while allowing WAN connections to be brought down in times of inactivity, the MAX responds to NCP watchdog requests as a proxy for clients on the other side of an offline IPX routing or IPX bridging connection. Responding to these 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 client-server connections may be released by the server. If there is a reconnection of the WAN session 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)

This provides the ability to configure the MAX to forward SAP broadcasts to specified IPX networks to assure 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 travelling, the initial SAP Request could receive responses from different servers and attaching you to different servers. This new feature adds the ability for you to direct SAP Requests to specific networks. The SAP Responses come from servers on these specified networks rather than coming from servers that are near the MAX. To configure this parameter, see "Configuring the NetWare SAP Home Server Proxy" on page 9-16.

Example IPX routing connections

This section shows example 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 9-4.

Configuring a dial-in client connection

In this example, a NetWare client dials into a corporate IPX network using PPP dial-in software. Figure 9-1 shows corporate network supporting both NetWare servers and clients.

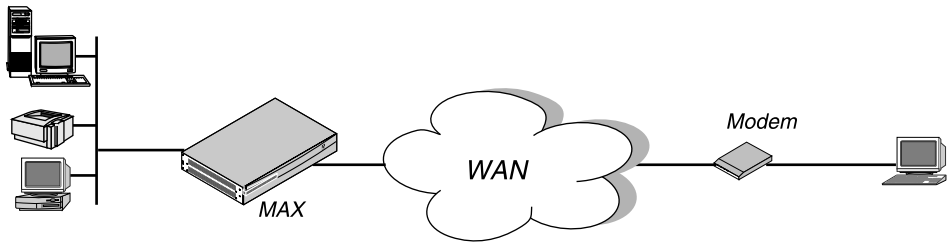


Figure 9-1. A dial-in NetWare client

To configure an IPX routing connection for this client:

1. Open Ethernet > Mod Config > Ether Options and verify that a 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.

```
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.

```
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. See Figure 9-2.

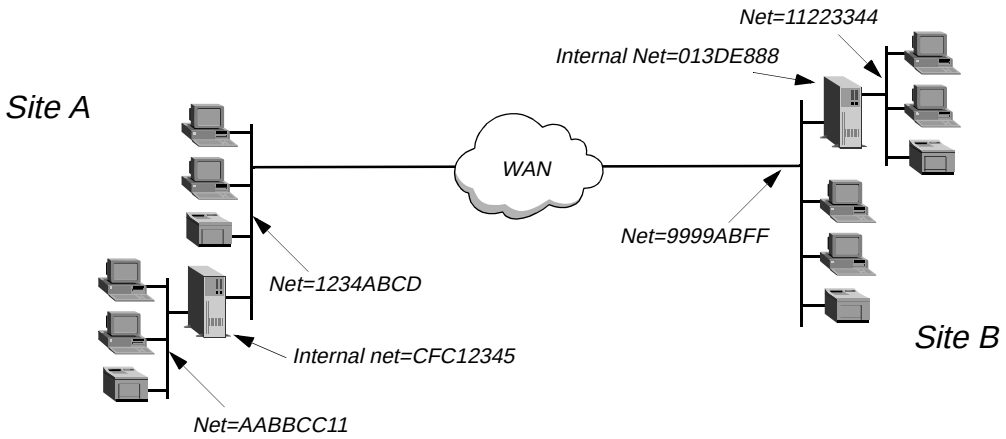


Figure 9-2. A connection with NetWare servers on both sides

Site A and site B both exist on Novell LANs that support NetWare 3.12 and NetWare 4 servers, NetWare clients, and a MAX. The NetWare server at site A has this configuration information:

```
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 this configuration information:

```
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:

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. (See "Enabling IPX routing in the MAX" on page 9-4.)

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 like this:

```
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.

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-2) using these 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 to 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 the MAX at site B:

1 Assign a system name to the Ascend unit at site B in the 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. (See "Enabling IPX routing in the MAX" on page 9-4.)

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 like this:

```
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) using these 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 to 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 example setup.

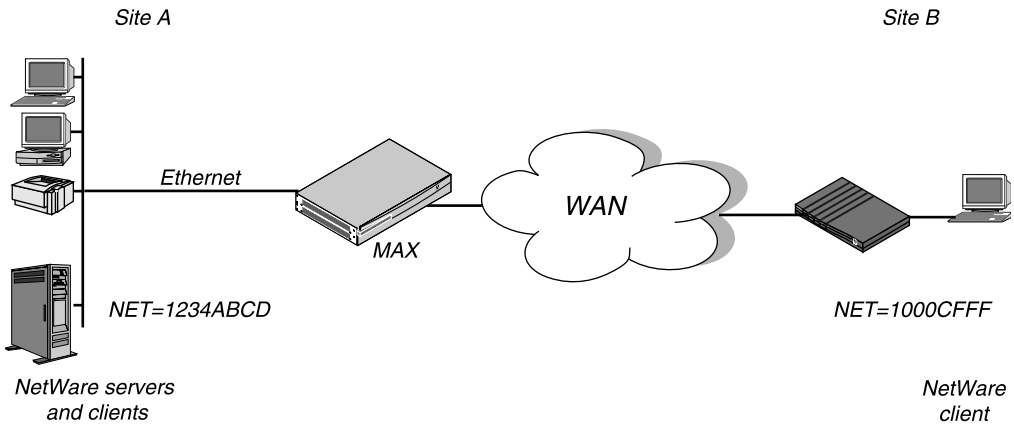


Figure 9-3. A dial-in client that belongs to its own IPX network

In this example, site A supports NetWare 3.12 servers, NetWare clients, and a MAX. The NetWare server at site A has this configuration information:

```
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 (e.g., 1000CFFF).

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. (It cannot be in use at site A or any network to which site A connects.)

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

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 like this:

```
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

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 like this:

```
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

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 indicates 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`.

Creating static IPX routes

Most sites configure only a few static IPX routes and rely on RIP for most other connections. IPX Route profiles define static IP routes. Each static route contains the information needed to reach one NetWare server.

The related parameters are:

```
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
```

For details on each parameter, see the *MAX Reference Guide*.

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.

Understanding the static route parameters

This section provides some background information on static route configurations.

- Specifying the 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.

- Entering the route in the internal RIP table

  Ative must be set to Yes for the MAX to read this route into its internal IPX RIP table.

- Specifying the server's internal network and node numbers

  The network number to enter here is the internal network number of the server. If you are not familiar with internal network numbers, see the Novell documentation. The default 0000000000001 is typically the node number for NetWare file servers.

- The server 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 may 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 on that network that uses a well-known socket number.

- Server type

  SAP advertises services by a type number. For example, NetWare file servers are SAP Service type 0004.

- Hop and tick counts to the server

  Usually the default hop count of 2 and tick count of 12 are appropriate, but you may need to increase these value for very distant servers. Ticks are IBM PC clock ticks (1/18 second). Note that the MAX calculates the best routes based on tick count, not hop count.

- Identifying the Connection profile needed to reach the server

  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 Connection menu.

Example 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 include or exclude services from the MAX service table or from being sent across the WAN to be made visible to remote sites. 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. See "Understanding the IPX connection parameters" on page 9-7.

The parameters related to IPX SAP filters are:

```
Ethernet
   IPX SAP Filters
      Name=optional
      Input SAP filters...
         In SAP filter 01–08
            Valid=Yes
            Type=Exclude
            Server Type=0004
            Server Name=SERVER-1
      Output SAP filters
```

```
            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
```

For more information on each parameter, see the *MAX Reference Guide*.

Understanding the SAP filter parameters

This section provides some background information on SAP filters.

Input and Output filters

Each filter contains up to 8 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 (or include) them from 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 (or includes) services from the response packet as specified by the Output filters.

Activating the current Input or Output filter

Valid enables the filter for use.

The type of action to take (include or exclude)

Type specifies whether this filter includes the service or excludes it.

Specifying the name of a NetWare server

Server Name can be a local or remote NetWare server name.

If the server is on the local network and this is an Output filter, the Type parameter specifies whether to include or exclude advertisements for this server in SAP response packets.

If the server is on the remote IPX network and this is an Input filter, the Type parameter specifies whether to include or exclude this server in the MAX service table.

Specifying a service type

Server Type specifies a hexadecimal number representing a type of NetWare service; for example, the number for file services is 0004.

In an Output filter, the Type parameter specifies whether to include or exclude advertisements for this service type in SAP response packets.

In an Input filter, the Type parameter specifies whether to include or exclude remote services of this type in the MAX service table.

Applying 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 includes or excludes specific servers or services from the MAX unit's SAP 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 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, and how to apply that 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, 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:

5 Open Answer > Session Options.

6 Specify IPX SAP Filter profile #1, and then close the Answer profile.

```
Ethernet
   Answer
      Session options...
         IPX SAP Filter=1
```

7 Repeat the same assignment in Connections > Session Options.

```
Ethernet
   Connections
      Session options...
         IPX SAP Filter=1
```

8 Close the Connection profile.

Monitoring IPX connections

The terminal server command-line interface supports Show commands for monitoring IPX connections in the MAX. To use these commands, invoke the terminal server interface (System > Sys Diag > Term Serv).

Verifying the transmission path to NetWare stations

The IPXping command enables you to verify the transmission path to NetWare stations at the network layer. It works on the same LAN as the MAX or across a WAN connection that has IPX Routing enabled. It uses this format:

```
ipxping [-c <count>] [-i <delay>] [-s <packetsize>] <hostname>
```

The arguments to the IPXping command are:

- <hostname>: The IPX address of the host, or if the host is a NetWare server, its hostname.
- [-c <count>](Optional): Stop the test after sending and receiving the number of packets specified by count.
- [-i <delay>](Optional): Wait the number of seconds specified by wait before sending the next packet. The default is one second.
- [-s <packet-size>](Optional): Send the number of data bytes specified by packet-size.

where <hostname> is either the IPX address of the NetWare workstation or the advertised name of a server. The IPX address consists of the IPX network and node numbers for a station; for example:

```
ascend% ipxping CFFF1234:000000000001
```

If you are using IPXping to verify connectivity with an advertised NetWare server, you can simply enter the symbolic name of the server; for example:

```
ascend% ipxping server-1
```

You can terminate the IPXping at any time by typing Ctrl-C.

During the IPXping exchange, the MAX calculates and reports this information:

```
PING server-1 (EE000001:000000000001): 12 data bytes
52 bytes from (EE000001:000000000001): ping_id=0 time=0ms
52 bytes from (EE000001:000000000001): ping_id=1 time=0ms
52 bytes from (EE000001:000000000001): ping_id=2 time=0ms
?
--- novl1 Ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/MAX = 0/0/0 ms
```

These statistics include the following information:

- The IPX address of the source and destination nodes.
- The byte counts of the request and response packets.
- The ping ID of the command. (The ping Request # replied to by target host.)
- The number of milliseconds required to send the IPXping and receive a response.
- The number of packets transmitted and received.
- Duplicate or damaged packets, if applicable.
- Average round-trip times for the ping request and reply.
  In some cases, round-trip times cannot be calculated.

To display statistics related to the IPXping command, type:

```
ascend% show netware pings

InPing Requests/OutPing Replies OutPing Requests/InPing Replies
      10            10                  18            18
```

The output shows how many NetWare stations have pinged the MAX (InPing requests and replies) and how many times the IPXping command has been executed in the MAX.

Displaying IPX packet statistics

To display IPX packet statistics, enter this command:

```
ascend% show netware stats

27162 packets received.
25392 packets forwarded.
0 packets dropped exceeding maximum hop count.
0 outbound packets with no route.
```

The MAX drops packets that exceed the maximum hop count (that have already passed through too many routers).

Displaying the IPX service table

To display the IPX service table, enter this command:

```
ascend% show netware servers

IPX address                    type             server name
ee000001:000000000001:0040     0451             server-1
```

The output contains these fields:

- IPX address: The IPX address of the server. The address uses this format:

<network number>:<node number>:<socket number>

- type: The type of service available (in hexadecimal format). For example, 0451 designates a file server.
- server name: The first 35 characters of the server name.

Displaying the IPX routing table

To display the IPX routing table, enter this command:

```
ascend% show netware networks

network     next router        hops        ticks   origin
CFFF0001    00000000000        0         1       Ethernet        S
```

The output contains these fields:

Fields	Descriptions
network	The IPX network number.
next router	The address of the next router, or 0 (zero) for a direct or WAN connection.
hops	The hop count to the network.
ticks	The tick count to the network.
origin	The name of the profile used to reach the network.

Note: An S or an H flag can appear next to the origin. S indicates a static route. H indicates a hidden static route. Hidden static routes occur when the router learns of a better route.

Configuring IP Routing

10

This chapter covers these topics:

Introduction to IP routing and interfaces

The first task described 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 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.

Note: If you have a MAX running Multiband Simulation, IP routing is disabled.

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 a default mask on the basis of address class. The

default subnet mask is the default number of network bits for the address's class. Table 10-1 shows the classes and the default number of network bits for each class.

Table 10-1.IP address classes and default subnet masks

Class	Address range	Network bits
Class A	0.0.0.0 — 127.255.255.255	8
Class B	128.0.0.0 — 191.255.255.255	16
Class C	192.0.0.0 — 223.255.255.255	24

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 can support up to 253 hosts.

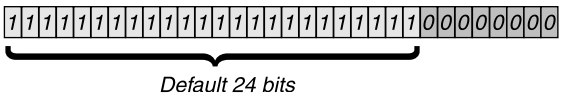


Figure 10-1. A class C IP address

For specifying a different subnet mask, the MAX supports a modifier that specifies the total number of network bits in the address. For example:

```
IP address = 198.5.248.40
Mask = 255.255.255.248
```

In the example address shown above, the mask specification indicates that 29 bits of the address will be used to specify the network. This is commonly referred to as a 29-bit subnet. The three remaining bits specify unique hosts.

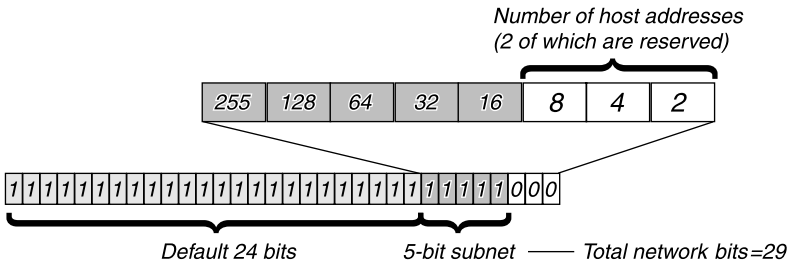


Figure 10-2. A 29-bit subnet mask and number of supported hosts

Three available bits allow eight possible bit combinations. Of the eight possible host addresses, two are reserved, as follows:

000 — Reserved for the network (base address)
001
010
100
110
101

011
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 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 (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 allow subnets to have base addresses that might 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 will 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
255.255.255.0	254 hosts + 1 broadcast, 1 network (base)
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`.

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 may appear in IP packets, and the Gateway field specifies the address of the next-hop router to reach that 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 the destination address in a packet, 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, it forwards the packet to that router.
- If the MAX does not find a matching entry or does not have a valid Default route, it drops the packet.

Static and dynamic routes

A static route is a manually configured path from one network to another, which specifies the destination network and the gateway (router) to use to get to that network.

- Each Static Rtes profile specifies one static route. If a path to a destination must be reliable, the administrator often configures more than one path (a secondary route), in which case the MAX chooses the route based on assigned metrics and availability.
- The Ethernet > Mod Config profile specifies a static connected route, which states “to reach system-A, send packets out this interface to system-A.” Connected routes are low cost, because no remote connection is involved.
- Each IP-routing Connection profile specifies a static route that states *to reach system-A, send packets out this interface to system-B*, where system-B is another router.

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. Routers that use RIP broadcast their 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:

- Connected routes have a default preference of 0.
- OSPF routes have a default preference of 10.
- ICMP redirects have a default preference of 30.
- RIP routes have a default preference of 100.
- Static routes have a default preference of 100.
- ATMP, PPTP routes have a default preference of 100.

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 might want to direct the MAX to use active routes, if available, rather than choose routes that are down.

MAX IP interfaces

Ethernet interfaces

The following example displays 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
```

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.

Following are descriptions of the interfaces created at startup:

- The Ethernet IP interface, labeled `ie0`, is always active, because it is always connected. Its IP address is assigned in Ethernet > Mod Config > Ether Options.

  The MAX creates two routing table entries: one with a destination of the network (labeled `ie0`), and the other with a destination of the MAX (labeled `local`).
- The black-hole (`bh0`) interface is always up. The black-hole address is 127.0.0.3. Packets routed to this interface are discarded silently.
- The loopback (labeled `local`) interface is always up. The loopback address is 127.0.0.1/32.
- The reject (labeled `rj0`) interface is 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 interfaces 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 is an inactive interface. It is created when you configure a Connection profile. The inactive interface is where all routes point when their WAN connections are down. The inactive interface label is `wanidle0`.

WAN IP interfaces

WAN interfaces are created 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 a both a system-based and interface-based router. Interface-based routing uses numbered interfaces. Some routers or applications require numbered interfaces, and 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 allows the MAX to operate in much the same way as a multihomed Internet host.

Figure 10-3 shows a sample interface-based routing connection.

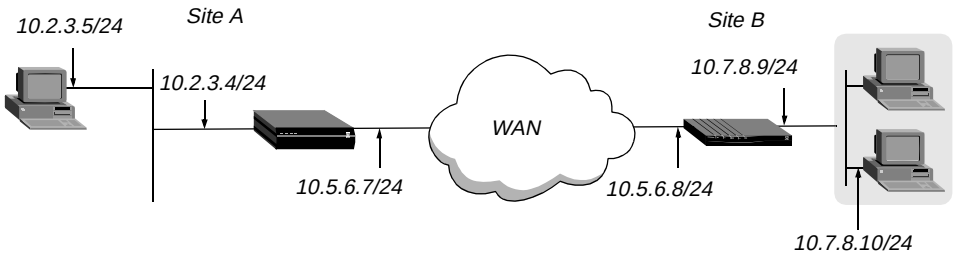


Figure 10-3. Interface-based routing example

The IP addresses 10.5.6.7 and 10.5.6.8 are assigned to the WAN interfaces. The site A MAX routes packets to the remote network 10.7.8.0 by means of the addresses assigned the WAN interfaces.

With system-based routing, these addresses are not assigned. The site A MAX routes packets to the remote network on the basis of the WAN interface it created when the connection was brought up, rather than a configured IP address.

Interface-based routing means that in addition to the system-wide 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 may omit the remote side's system-based IP address from the Connection profile and use interface-based routing exclusively. This is an appropriate mechanism, for example, if the remote system is on a backbone net that might 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 link-specific IP addresses are specified in the following parameters:

- Connections > IP Options > IF Adrs (the near end numbered interface)
- Connections > IP Options > LAN Adrs (the far end numbered interface)

Note that IP Address must always be filled in, so if the only known address is the interface address, you must place it in the IP Address parameter rather than the WAN Alias parameter. In this case, a host route is created to the interface address (IP address), a net route is created to the subnet of the remote interface, and incoming calls must report their IP addresses as the value in the IP Address parameter.

It is also possible, although not recommended, to specify the local numbered interface (Interface Address) and use the far end device's system-wide IP address (IP Address). In this case, the remote interface must have an address on the same subnet as the local, numbered interface.

If a MAX is using a numbered interface, note the following differences and similarities in operation, compared to unnumbered (system-based) routing:

- IP packets generated in the MAX and sent to the remote address will have an IP source address corresponding to the numbered interface, not the system-wide (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 may 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 configures system-global parameters that affect all IP interfaces in the MAX. These are the related parameters:

```
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. The information is organized by functionality rather than by parameter. For more information on each parameter, see the *MAX Reference Guide.*

Primary IP address for each Ethernet interface

The IP Address parameter specifies the MAX unit's IP address for each local Ethernet interface. When specifying IP addresses for the MAX's Ethernet interfaces, 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 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 load of routing traffic to a large subnet, by assigning IP addresses on that subnet to two or more routers on the backbone. When the routers have a direct connection to the subnet as well as to the backbone network, they route packets to the subnet and include the route in their routing table updates.

Dual IP also allows 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 an example IP network to which a MAX is connected:

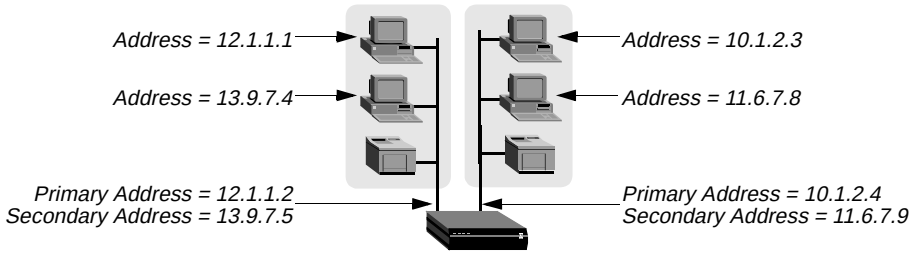


Figure 10-4. Sample dual IP network

Two IP addresses are assigned to each of the MAX's Ethernet interfaces. 10.1.2.4 and 11.6.7.9 are assigned to Ethernet 1. 12.1.1.2 and 13.9.7.5 are assigned to Ethernet 2. In this example, the MAX routes between all displayed networks. The MAX enables the host assigned 12.1.1.1 to communicate with the host assigned 13.9.7.4 and the host assigned 10.1.2.3.

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.

Enabling RIP on the Ethernet interface

You can configure each IP interface to send RIP updates (informing other local routers of its routes), receive RIP updates (learning about networks that can be reached via 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 the MAX is configured to ignore the default route, RIP updates do not modify the default route in the MAX routing table.

Proxy ARP and inverse ARP

The MAX can be configured to respond to ARP requests for remote devices that have been assigned an address dynamically. It responds to the ARP request with its own MAC address while bringing up the connection to the remote device. This feature is referred to as Proxy ARP.

The MAX also supports Inverse Address Resolution Protocol (Inverse ARP). Inverse ARP allows 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 is the MAX unit's IP address on Ethernet.
- ARP source-hardware address is the Q.922 address of the local DLCI.

For the details of Inverse ARP, see RFCs 1293 and 1490.

Specifying address pools

You can define up to 10 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 255). Addresses in a pool do not accept a netmask modifier, 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 may 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 allow a caller to spoof a local address. The Pool Only parameter instructs 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.

Pool Summary indicates the route summarization is in use; that is, a series of host routes will be summarized into a network route advertisement. Packets destined for a valid host address on that network are routed to the host, and packets destined for an invalid host address are rejected 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 Start address must be the first host address. Subtract one from the Pool 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 the Pool Count to a value that is 2 less than a power of 2. For example, you may use values 2, 6, 14, 30, 62, 126 or 253. The netmask will be deduced from a value that is 2 greater than Pool Count. For example, with this configuration:

```
Pool Summary=Yes
Pool#1 start=10.12.253.1
Pool#1 count=126
```

The network alignment address is Pool Start address –1: 10.12.253.0 and the netmask is Pool Count +2 addresses: 255.255.255.128. The resulting address pool network is:

10.12.253.0/25

For an example configuration that shows route summarization, see “Configuring DNS” on page 10-15.

- Sharing Connection profiles

  The Shared Prof parameter specifies whether the MAX will allow more than one incoming call to share the same Connection profile. This feature is related to IP routing because sharing profiles cannot 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.

Telnet password

The Telnet password is required from all users attempting to access the MAX unit via Telnet. Users are allowed three tries to enter the correct password, after which the connection attempt fails.

BOOTP Relay

By default, a MAX does not relay BOOTP (Bootstrap Protocol) requests to other networks. If BOOTP is enabled, the MAX can relay BOOTP requests to another network. However, SLIP BOOTP must be disabled 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 can support BOOTP on only one connection. If both SLIP BOOTP and BOOTP relay are enabled, you will receive an error message.

You can specify the IP address of one or two BOOTP servers. 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 each server is used. The order of the BOOTP servers in the BOOTP Relay menu does not necessarily determine which server is tried first.

Local domain name

The Domain Name is used for DNS lookups. When the MAX is given a hostname to look up, it tries various combinations including appending the configured domain name. The secondary domain name (Sec Domain Name) can specify another domain name that the MAX can search using DNS. The MAX searches the secondary domain only after the domain specified in 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 use the List Attempt parameter to enable the user to try one entry in the DNS list of hosts, and if that connection fails, to try the next entry, and so on, without losing the WAN session. 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 SNTP (Simple Network Time Protocol—RFC 1305) to set and maintain its system time by communicating with an SNTP server. SNTP must be enabled for the MAX to communicate using that protocol. In addition, you must specify your time zone as an offset from the UTC (Universal Time Configuration). UTC is in the same time zone as Greenwich Mean Time (GMT), and the offset is specified in hours using a 24-hour clock. Because some time zones, such as Newfoundland, cannot use 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 ahead of UTC, which is represented as follows:

```
UTC +0130
```

For San Francisco, which is 8 hours ahead of UTC:

```
UTC +0800
```

For Frankfurt, which is 1 hour behind UTC:

```
UTC -0100
```

Specifying SNTP server addresses

The host parameter lets you specify up to three server addresses. The MAX attempts to communicate with the first address. It attempts the second only if the first is inaccessible, and 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 use the Adv Dialout Routes parameter to instruct the MAX to stop advertising IP routes that use dial services if its trunks are in the alarm condition. Otherwise, it continues to advertise its dialout routes, which prevents the redundant unit from taking over the routing responsibility.

Example IP network configurations

This section shows some example Ethernet profile IP configurations. For a more complete example that shows an Ethernet profile, Route profile, and Connection profile configuration that work together, see “Configuring DNS” on page 10-15.

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):

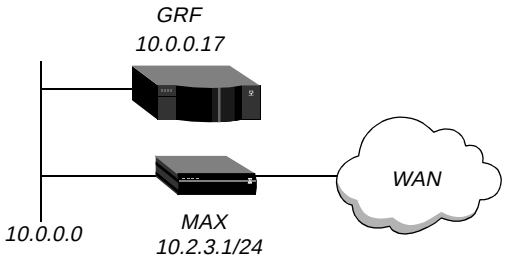


Figure 10-5. Creating a subnet for the MAX

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.

See “Configuring IP routes and preferences” on page 10-32 for more information about IP Route profiles. To verify that the MAX is up on the local network, invoke the terminal server interface and enter the Ping command to a local IP address or hostname. For example:

```
ascend% ping 10.1.2.3
```

You can terminate the Ping exchange at any time by typing Ctrl-C.

Configuring DNS

The DNS configuration enables the MAX to use local DNS or WINS servers for lookups. In this example 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 host name 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 host names 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 includes additional information for each table entry. The information is in the following two fields, which are updated when the system matches the table entry with a host name that was not found by the remote server:

- # Reads (the number of reads since entry was created)

  This field is updated each time a local name query match is found in the local DNS table.
- Time of Last Read

You can check the list of host names and IP addresses in the table using the termserv 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.

```
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: ""                    ------          -------
```

Figure 10-6. Local DNS table example

New terminal server command changes

New *`show`* and *`dnstab`* commands have been added to help you view, edit, or make entries in 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 these variations:

Table 10-3.`dnstab` commands

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 Profile: 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

- Must be unique in the table.
- Must start with an alphabetic character, which may be either upper- or lower-case.
- Must be less than 256 characters
- Names can be local names or fully qualified names that include the domain name.

Periods at the end 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 host name, 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 10-17.)

   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 **`0`** 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 and then Enter.

     If you enter a valid name, the system places it in the table (or leaves it there is you accepted 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 10-17)

     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.

   – If you are changing the name of the entry but not the IP address, press Return.

   – To change the IP address, type the new IP address

   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 **`0`** 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 Return.

3 Press the spacebar and then press Return.

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 a connection has been terminated, 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.

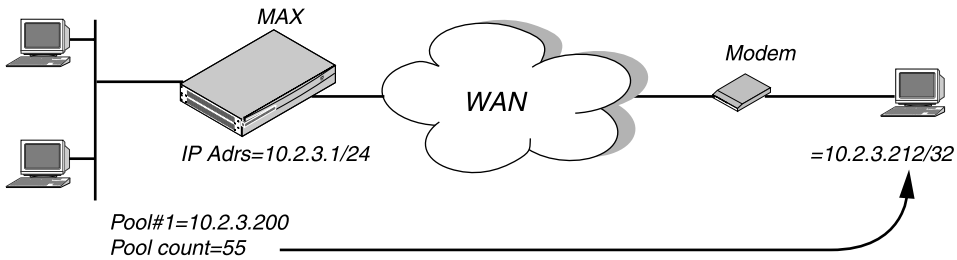


Figure 10-7. Address assigned dynamically from a pool

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 Connection profile route private, which are requirements when using route summarization.

These are the rules for network-aligned address pools:

- The Pool Count must be two less than the total number of addresses in the pool.

  Add two to Pool Count for the total number of addresses in the subnet, and calculate the netmask for the subnet based on this total.

- The Pool Start address must be the first host address.

  Subtract 1 from the Pool Start address for the base address for the subnet.

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 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 the 255.255.255.192 netmask. Note that 10.12.253.64, 10.12.253.128, and 10.12.253.192 are also valid zero addresses for the same netmask. The resulting address pool network is 10.12.253.0/26.

Pool Count is set to 62. When you add two to the Pool Count, you get 64. The netmask for 64 addresses is 255.255.255.192 (256–64 = 192). The Ascend subnet notation for a 255.255.255.192 netmask is /26.

After verifying that *every one* of the configured address pools is network-aligned, you must enter a static route for them. These static routes handle all IP address that have not been given to users by routing them to the reject interface or the blackhole interface. (See “MAX IP interfaces” on page 10-5.)

Note: The MAX creates a host route for every assigned address from the pools and host routes override subnet routes. So, 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 might improperly send the MAX a packet to an inactive IP address. Depending on the static route specification, these packets are either bounced with an ICMP unreachable or silently discarded.

For example, the following static route specifies the blackhole 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 will contain 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 the Private parameter is set 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 IP routing is enabled and addresses are specified in a Connection profile, it defines an IP WAN interface. These are the related options:

```
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 more information on each parameter, see the *MAX Reference Guide.*

Enabling dynamic address assignment for answered calls

Assign Adrs must be set to Yes in the Answer profile 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 Pools Only parameter is set to Yes in the Ethernet profile, the MAX terminates connections that reject the assigned address during PPP negotiation. See "Configuring dynamic address assignment to a dial-in host" on page 10-24 for related information.

Enabling IP routing for WAN connections

Route IP in Answer > PPP Options must be set 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 IP routing is enabled, IP packets are always routed, they are never bridged.

Configuring the remote IP address

The LAN 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 may be one of the following values:

- IP address of a router

  If the remote device is an IP router, specify its address including its netmask modifier. (See "IP addresses and subnet masks" on page 10-1 for background information.) If you omit the netmask, the MAX inserts a default netmask which 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 netmask modifier 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 will accept dynamic address assignment, leave the remote-address 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

This 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. The caller must be using a numbered interface, and its interface address must agree with the WAN Alias setting.

Specifying a local IP interface address

This is another local IP interface address, to be used as the local numbered interface instead of the default (the Ethernet IP Adrs).

Assigning metrics and preferences

Connection profiles often represent switched connections, which have an initial cost that can be avoided if a nailed-up link to the same destination can be used. To favor nailed-up links, you can assign a higher metric to switched connections than any of the nailed-up links that can go to the same place.

Each connection represents a static route, which has a default preference of 100. (See "Route preferences and metrics" on page 10-5.) For each connection, you can fine-tune the route preference and assign a 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 might want to 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 this 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 caller will be assigned 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. See "Configuring DNS" on page 10-15.

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: IP Direct connections are typically configured with RIP turned off. If you set the IP Direct configuration with RIP set to receive, all RIP updates will be forwarded to the specified address. This is typically not desirable since RIP updates are designed to be stored locally by the IP router (the MAX, in this case).

Configuring RIP on this interface

You can configure an IP interface to send RIP updates (informing other routers on that interface of its routes), receive RIP updates (learning about distant networks from other routers on that interface), 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

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 the TCP/IP networking software. The software is included with Windows 95, but the user may need to purchase and install it separately if the computer has a previous version of Windows or OS/2.

Macintosh software

Macintosh computers need MacTCP or Open Transport software for TCP/IP connectivity. MacTCP is included with all Apple system software including and after Version 7.1. 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 will obtain its IP address dynamically from the MAX, the TCP/IP software must be configured to allow dynamic allocation. If a DNS server is supported on your local network, 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 IP routing connections

This section provides example Connection profile configurations for IP routing. These examples all presume that the Ethernet profile has been configured 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 will accept an IP address assignment from the MAX dynamically. Figure 10-8 shows an example network.

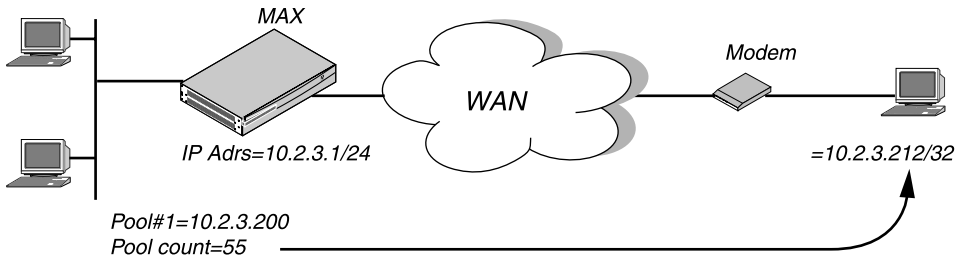


Figure 10-8. A dial-in user requiring dynamic IP address assignment

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, this example 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 Type 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 IP routing and dynamic address assignment.

```
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.

```
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

This type of connection 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 those 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. See "IP addresses and subnet masks" on page 10-1 for details on the /32 netmask.

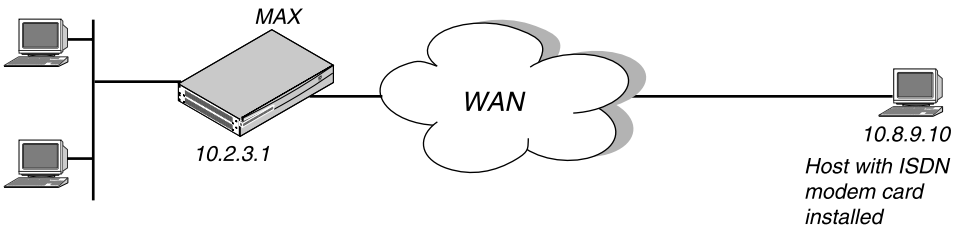


Figure 10-9. A dial-in user requiring a static IP address (a host route)

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
Netmask=255.255.255.255
Default Gateway=N/A (or None)
Name Server=10.7.7.1
Domain suffix=abc.com
VAN Jacobsen compression ON
```

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.

```
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.

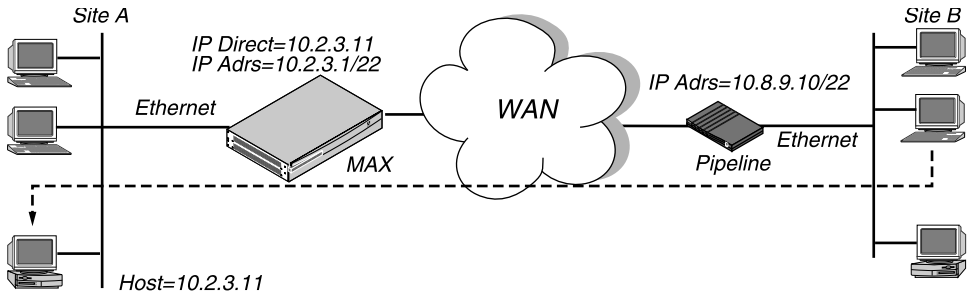


Figure 10-10. Directing incoming IP packets to one local host

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.

```
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.

```
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 all incoming packets on this connection will be directed. When you use the IP Direct feature, a user cannot Telnet directly to the MAX from the far side. All incoming IP traffic is directed to the specified address on the local IP network.

Configuring a router-to-router connection

In this example, the MAX is connected to a corporate IP network and needs a switched connection to another company that has its own IP configuration. Figure 10-11 shows an example network diagram.

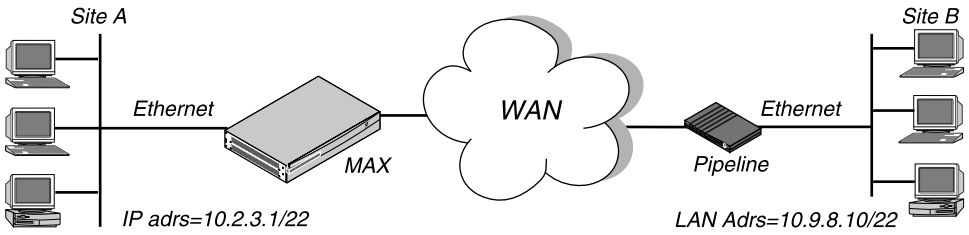


Figure 10-11. A router-to-router IP connection

This example assumes that the Answer profile in both 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.

```
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.

```
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 this example network, the MAX is used to connect telecommuters with their own Ethernet networks to the corporate backbone. The MAX is on a subnet, and assigns subnet addresses to the telecommuters' networks.

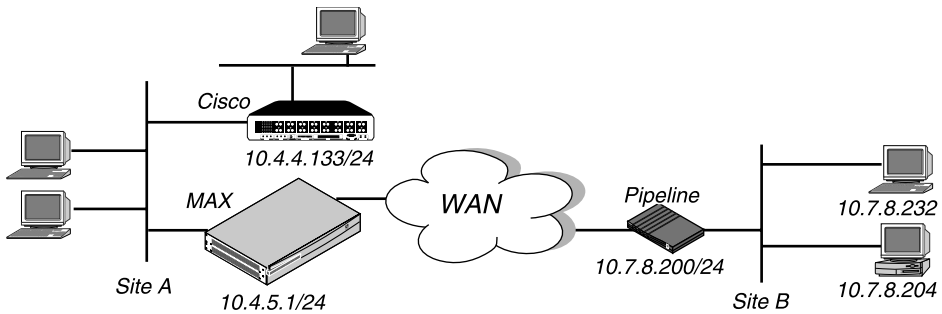


Figure 10-12. A connection between local and remote subnets

This example assumes that the Answer profile in both devices enables IP routing. Because the MAX specifies a netmask 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 must either have a default route configuration to a router in its own subnet (such as the Cisco router in Figure 5-12) or it 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.

```
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:

5 Open the Default IP Route profile.

6 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
```

7 Close the IP Route profile.

To configure the site B Pipeline unit for a connection to site A:

8 Open the Connection profile in the Pipeline unit for the site A MAX.

9 Specify the site A MAX unit's name, activate the profile, and set encapsulation options.

```
Ethernet
   Connections
      Station=MAXA
      Active=Yes
      Encaps=MPP
      Encaps options...
         Send Auth=CHAP
         Recv PW=localpw
         Send PW=remotepw
```

10 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:

11 Open the Default IP Route profile in the site B Pipeline.

12 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
```

13 Close the IP Route profile.

Configuring a numbered interface

If you are not familiar with numbered interfaces, see “Numbered interfaces” on page 10-6. In the following example, the MAX is a system-based router but supports a numbered interface for one of its connections. The arrow in Figure 10-13 indicates the numbered interfaces for this connection:

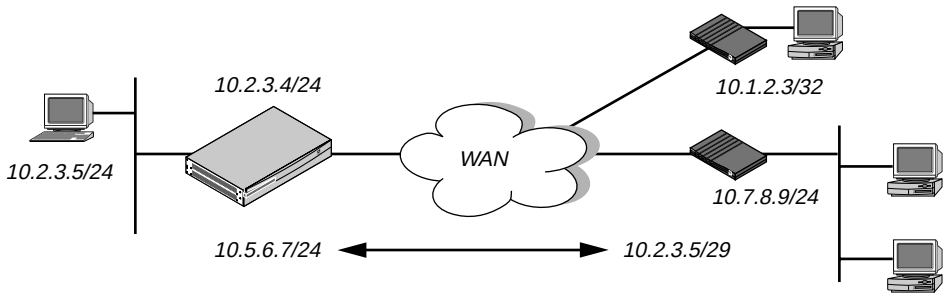


Figure 10-13. Example numbered interface

The numbered interface addresses are:

- IF Adrs=10.5.6.7/24
- WAN Alias=10.7.8.9/24

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 numbered interface:

1 Open Ethernet > Mod Config > Ether Options and verify that the IP Adrs parameter is set correctly.

```
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 remote device in 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 Specify the numbered interface address for the 50 in the IF Adrs parameter.

```
      IP options...
         IF Adrs=10.5.6.7/24
```

7 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. These are the parameters for configuring static routes:

```
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
      ASE-type=Type1
      ASE=tag=c0000000
```

```
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
```

```
Ethernet
   Mod Config
      Ether options…
         IP Adrs=10.2.3.1/24
```

```
   2nd Adrs=0.0.0.0/0
   RIP=Off
Route Pref…
   Static Preference=100
   Rip Preference-100
   RipAseType-Type2
   Rip Tag=c8000000
   OSPF Preference=10
   OSPF ASE Preference=150
```

Understanding the static route parameters

This section provides some background information on static routes. For more information on each parameter, see the *MAX Reference Guide.*

Route names

IP Route are indexed by name. You can assign any name less than 31 characters.

Activating a route

A route must be active to affect packet routing. An inactive route is ignored.

Route's destination address

The destination address of a route is the target network—the destination address in a packet. Packets destined for that host will 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).

Route's gateway address

The gateway-address parameter specifies the IP address of the router or interface to use to reach the target network.

Metrics, costs, and preferences

The metric parameter is a hop count for this route (a number between 1 to 15). When RIP was originally developed, the hop count was a number that showed how many routers needed to be crossed to reach the destination. For example, a destination with a hop count of 10 meant that to get a packet there requires crossing 10 routers. A route with a shorter hop count to a destination is more desirable than one with a larger hop count, since it most likely is a shorter, faster route.

The hop count can also be manually configured to give a route a "virtual" hop count. In this way you can manually configure which routes are more desirable than others in your environment. The higher the metric, the less likely that the MAX will use a route.

The cost parameter specifies the cost of an OSPF link. The cost is a configurable metric that can be used to take into account the speed of the link and other issues. The lower the cost, the

more likely the interface will be used to forward data traffic. For details, see Chapter 11, "Configuring OSPF Routing."

The preference parameter specifies a route preference. Zero is the default for connected routes (such as the Ethernet). When choosing which route to use, the router first compares the preference values, preferring the lower number. If the preference values are equal, the router compares the metric values, using the route with the lower metric. The value of 255 means "Do not use this route." See "Route preferences and metrics" on page 10-5.

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 might want to direct the MAX to use active routes, if available, rather than choose routes that are down.

Tagging routes learned from RIP

The rip-tag field 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.

Type-1 or type-2 metrics for routes learned from RIP

The rip-ase-type parameter can be set to 1 or 2. Type-1 is a metric expressed in the same units as the link-state metric (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 eliminates the need for conversion of external costs to internal link-state metrics.

Making a route private

Private routes are used internally but are not advertised.

Note: Typically, default routes should not be advertised to other routers. They are designed for the internal use of the specific router on which they are configured.

Routes for Connection profile interfaces

When an IP routing connection is brought up, the MAX activates the route for that WAN interface. The Destination for the route is the remote device's address (LAN Adrs), and the metric and preference values are specified in the Connection profile. If the profile uses numbered interface, an additional route is created for that interface.

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 might want to direct the MAX to use active routes, if available, rather than choose routes that are down.

A connected route for the Ethernet IP interface

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.

Static route preferences

By default, static routes and RIP routes have the same preference, so they compete equally. ICMP redirects take precedence over both and OSPF take precedence over everything. If a dynamic route's preference is lower than that of the static route, the dynamic route can overwrite or "hide" a static route to the same network. This can be seen in the IP routing table: there will be two routes to the same destination. The static route has an "h" flag, indicating that it is hidden and inactive. The active, dynamically learned route is also in the routing table. However, dynamic routes age and if no updates are received, they eventually expire. In that case, the hidden static route reappears in the routing table.

RIP and OSPF preferences

Because OSPF typically involves a complex environment, its router configuration is described in a separate chapter. See Chapter 11, "Configuring OSPF Routing."

Tagging routes learned from RIP

The RIP Tag field 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.

Metrics for routes learned from RIP

The RipAseTag parameter can be type 1 or 2. Type-1 is a metric expressed in the same units as the link-state metric (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 eliminates the need for conversion of external costs to internal link-state metrics.

Example static route configurations

For example Connection profile configurations, see "Configuring IP routing connections" on page 10-21. Each of these results in a static route. 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 10-14.

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.

The name of the default IP Route profile is always Default, and its destination is always 0.0.0.0. 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 are reachable through the remote device, such as the remote network shown in Figure 10-14.

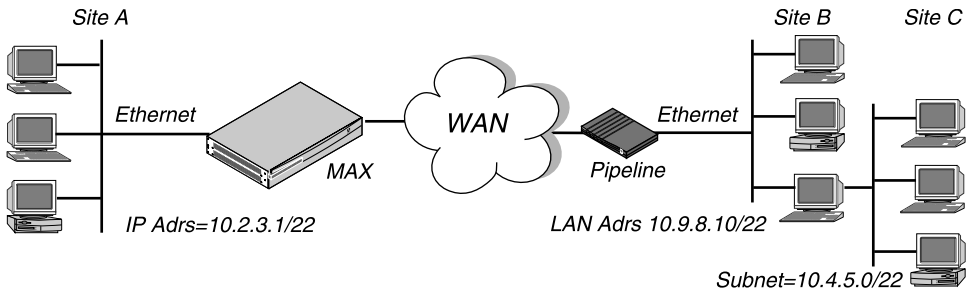


Figure 10-14. Two-hop connection that requires a static route when RIP is off

To enable the MAX to route to site C without using RIP, you must configure an IP Route profile like this:

```
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 route preferences configuration

This example increases the preference value of RIP routes, instructing the router to use static routes 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

Each active interface may be configured to send or receive RIP or OSPF updates. The Ethernet interface can also be configured to accept or ignore ICMP redirects. All of these routing mechanisms modify the IP routing table dynamically.

These are the parameters that enable the MAX to receive updates from RIP or ICMP. (For information on OSPF updates, see Chapter 11, “Configuring OSPF Routing.”)

```
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
      IP options...
         Private=No
         RIP=On
```

Understanding the dynamic routing parameters

This section provides some background information about the dynamic routing options.

RIP (Routing Information Protocol)

You can configure the router to send or receive RIP updates (or both) on the Ethernet interface and on each WAN interface. The Answer profile setting applies to Name profiles and profiles retrieved from RADIUS. You can also choose 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.

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 to be 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 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.

RIP policy and RIP summary

The RIP Policy and RIP Summary parameters have no effect 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 were 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 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;" in our example, the MAX advertises a route only to 200.5.8.13.

Ignoring ICMP Redirects

ICMP was designed 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 and one of the least secure, because it is possible to counterfeit ICMP Redirects and change the way a device routes packets.

Private routes

If you configure a profile with Private=Yes, the router will not disclose its route in response to queries from routing protocols.

Examples of RIP and ICMP configurations

The following sample configuration instructs the router 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 router 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 router will learn about networks that are reachable via other local routers. However, it will 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 router 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 will be 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.

Managing IP routes and connections

This section describes how to monitor TCP/IP/UDP and related information in the terminal server command-line interface. To invoke the terminal-server interface, select System > Sys Diag > Term Serv and press Enter.

Working with the IP routing table

The terminal-server IProute commands display the routing table and enable you to add or delete routes. The changes you make to the routing table using the IProute command last only until the MAX unit resets. To view the IProute commands:

```
ascend% iproute ?

iproute ?       Display help information
iproute add     iproute add <destination/size> <gateway> [ pref ] [ m
iproute delete  iproute delete <destination/size> <gateway> [ proto ]
iproute show    displays IP routes (same as "show ip routes" command)
```

Displaying the routing table

Note that the IProute Show command and the Show IP Routes command have identical output. To view the IP routing table:

```
ascend% iproute show

Destination        Gateway        IF       Flg Pref  Met   Use   Age
0.0.0.0/0          10.0.0.100     wan0     SG   1     1     0     20887
10.207.76.0/24     10.207.76.1    wanidle0 SG   100   7     0     20887
10.207.77.0/24     10.207.76.1    wanidle0 SG   100   8     0     20887
127.0.0.1/32       -              lo0      CP   0     0     0     20887
10.0.0.0/24        10.0.0.100     wan0     SG   100   1     21387 20887
10.1.2.0/24        -              ie0      C    0     0     19775 20887
```

```
10.1.2.1/32         -               lo0      CP   0     0     389   20887
255.255.255.255/32 -                ie0      CP   0     0     0     20887
```

The columns in the table display the following information:

- Destination

  The Destination column indicates the target address of a route. To send a packet to this address, the MAX will use this route. Note that the router will use the most specific route (having the largest netmask) that matches a given destination.

- Gateway

  The Gateway column specifies the address of the next hop router that can forward packets to the given destination. Direct routes (without a gateway) no longer show a gateway address in the gateway column.

- IF

  The Interface column shows the name of the interface through which a packet addressed to this destination will be sent.

  ie0 is the Ethernet interface

  lo0 is the loopback interface

  wanN specifies each of the active WAN interfaces

  wanidle0 is the inactive interface (the special interface for any route whose WAN connection is down).

- Flg

  The Flg column can contain the following flag values:

  – C (A directly connected route such as Ethernet)

  – I (ICMP Redirect dynamic route)

  – N (Placed in the table via SNMP MIB II)

  – O (A route learned from OSPF)

  – R (A route learned from RIP)

  – r (A RADIUS route)

  – S (A static route)

  – ? (A route of unknown origin, which indicates an error)

  – G (An indirect route via a gateway)

  – P (A private route)

  – T (A temporary route)

  – * (A hidden route that will not be used unless another better route to the same destination goes down)

- Pref

  The Preference column contains the preference value of the route. Note that all routes that come from RIP will have a preference value of 100, while the preference value of each individual static route may be set independently.

- Metric

  The Metric column shows the RIP-style metric for the route, with a valid range of 0-16. Routes learned from OSPF show a RIP metric of 10. OSPF Cost infinity routes show a RIP metric of 16.

- Use

  This is a count of the number of times the route was referenced since it was created. (Many of these references are internal, so this is not a count of the number of packets sent using this route.)

- Age

  This is the age of the route in seconds. It is used for troubleshooting, to determine when routes are changing rapidly or flapping.

The first route in the default route (destination 0.0.0.0/0), which is pointing through the active Connection profile.

```
0.0.0.0/0          10.0.0.100     wan0     SG   1     1     0     20887
```

In this example, the IP Route profile for the default route specifies a Preference of 1, so this route is preferred over dynamically learned routes. The next route is specified in a Connection profile that is inactive.

```
10.207.76.0/24     10.207.76.1    wanidle0 SG   100   7     0     20887
```

The next route in the table is a static route that points through an inactive gateway:

```
10.207.77.0/24     10.207.76.1    wanidle0 SG   100   8     0     20887
```

The static route is followed by the loopback route:

```
127.0.0.1/32       -              lo0      CP   0     0     0     20887
```

The loopback route says that packets sent to this special address will be handled internally. The C flag indicates a Connected route, while the P flag indicates that the router will not advertise this route.

The next route is specified in a Connection profile that is currently active:

```
10.0.0.0/24        10.0.0.100     wan0     SG   100   1     21387 20887
```

These are followed by the connection to the Ethernet interface. It is directly connected, with a Preference and Metric of zero.

```
10.1.2.0/24        -              ie0      C    0     0     19775 20887
```

The last two routes are a private loopback route, and a private route to the broadcast address:

```
10.1.2.1/32        -              lo0      CP   0     0     389   20887
255.255.255.255/32 -              ie0      CP   0     0     0     20887
```

The private loopback route is a host route with our Ethernet address. It is private, so it will not be advertised. The private route to the broadcast address is used in cases where the router will want to broadcast a packet but is otherwise unconfigured. It is typically used when trying to locate a server on a client machine to handle challenges for a token security card.

Adding an IP route

To add a static route to the MAX unit's routing table that will be lost when the MAX resets, use the IProute Add command in this format:

```
iproute add <destination> <gateway> [<metric>]
```

where <destination> is the destination network address, <gateway> is the IP address of the router that can forward packets to that network, and <metric> is the virtual hop count to the destination network (default 8). For example:

```
ascend% iproute add 10.1.2.0 10.0.0.3/24 1
```

The command shown immediately above adds a route to the 10.1.2.0 network and all of its subnets through the IP router located at 10.0.0.3/24. The metric to the route is 1 (it is one hop away).

If you try to add a route to a destination that already exists in the routing table, the MAX replaces the existing route, but only if the existing route has a higher metric. If you get the message "Warning: a better route appears to exist", the MAX rejected your attempt to add a route because the routing table already contained the same route with a lower metric. Note that RIP updates can change the metric for the route.

Deleting an IP route

To remove a route from the MAX unit's routing table, enter the IProute Delete command in this format:

```
iproute delete <destination> <gateway>
```

For example:

```
ascend% iproute delete 10.1.2.0 10.0.0.3/24
```

Note: RIP updates can add back any route you remove with IProute Delete. Also, the MAX restores all routes listed in the Static Route profile after a system reset.

Displaying route statistics

The Traceroute command is useful for locating slow routers or diagnosing IP routing problems. It traces the route an IP packet follows by launching UDP probe packets with a low TTL (Time-To-Live) value and then listening for an ICMP "time exceeded" reply from a router. Its syntax is:

```
traceroute [ -n ] [ -v ] [ -m max_ttl ] [ -p port ] [ -q nqueries ]
[ -w waittime ] host [ datasize ]
```

All flags are optional. The only required parameter is the destination hostname or IP address.

- -n
  Prints hop addresses numerically rather than symbolically and numerically (this eliminates a name server address-to-name lookup for each gateway found on the path).
- -v
  Verbose output. Received ICMP packets other than Time Exceeded and ICMP Port Unreachable are listed.
- -m <max_ttl>
  This sets the maximum time-to-live (maximum number of hops) used in outgoing probe packets. The default is 30 hops.
- -p <port>
  Sets the base UDP port number used in probes. Traceroute hopes that nothing is listening on any of the UDP ports from the source to the destination host (so an ICMP Port

Unreachable message will be returned to terminate the route tracing). If something is listening on a port in the default range, this option can be used to pick an unused port range. The default is 33434.

- -q <nqueries>
  Sets the maximum number of queries for each hop. The default is 3.
- -w <waittime>
  Sets the time to wait for a response to a query. The default is 3 seconds.
- host
  The destination host by name or IP address.
- datasize
  Sets the size of the data field of the UDP probe datagram sent by Traceroute. The default is 0. This results in a datagram size of 38 bytes (a UDP packet carrying no data).

For example, to trace the route to the host "techpubs":

```
ascend% traceroute techpubs

traceroute to techpubs (10.65.212.19), 30 hops MAX, 0 byte packets
 1  techpubs.eng.ascend.com (10.65.212.19)  0 ms  0 ms  0 ms
```

Probes start with a TTL of one and increase by one until of the following conditions occurs:

- The MAX receives an ICMP *port unreachable* message.
  The UDP port in the probe packets is set to an unlikely value, such as 33434, because the target host is not intended to process the packets. A "port unreachable" message indicates that the packets reached the target host and were rejected.
- The TTL value reaches the maximum value.
  By default, the maximum TTL is set to 30. You can specify a different TTL by using the –m option; for example:

```
ascend% traceroute -m 60 techpubs

traceroute to techpubs (10.65.212.19), 60 hops MAX, 0 byte packets
 1  techpubs.eng.abc.com (10.65.212.19)  0 ms  0 ms  0 ms
```

Three probes are sent at each TTL setting. The second line of command output shows the address of the router and round trip time of each probe. If the probe answers come from different gateways, the address of each responding system will be printed. If there is no response within a 3 second timeout interval, the command output is an asterisk. The following annotations may be included after the time field in a response:

- !H (Host reached.)
- !N (Network unreachable.)
- !P (Protocol unreachable.)
- !S (Source route failed. This may indicate a problem with the associated device.)
- !F (Fragmentation needed. This may indicate a problem with the associated device.)
- !h (Communication with the host is prohibited by filtering.)
- !n (Communication with the network is prohibited by filtering.)
- !c (Communication is otherwise prohibited by filtering.)
- !? (Indicates an ICMP sub-code. This should not occur.)
- !?? (Reply received with inappropriate type. This should not occur.

Pinging other IP hosts

The terminal-server Ping command is useful for verifying that the transmission path is open between the MAX and another station. It sends an ICMP echo_request packet to the specified station. It the station receives the packet, it returns an ICMP echo_response packet. For example, to ping the *host techpubs*:

```
ascend% ping techpubs

PING techpubs (10.65.212.19): 56 data bytes
64 bytes from 10.65.212.19: icmp_seq=0 ttl=255 time=0 ms
64 bytes from 10.65.212.19: icmp_seq=3 ttl=255 time=0 ms
^C
--- techpubs ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/MAX = 0/0/0 ms
```

You can terminate the Ping exchange at any time by typing Ctrl-C. When you press Ctrl-C, the command reports the number of packets sent and received, the percentage of packet loss, duplicate or damaged echo_response packets (if any), and round-trip statistics. In some cases, round-trip times cannot be calculated.

During the Ping exchange, the MAX displays information about the packet exchange, including the TTL (Time-To-Live) of each ICMP echo_response packet.

Note: The maximum TTL for ICMP Ping is 255 and the maximum TTL for TCP is often 60 or lower, so you might be able to ping a host but not be able to run a TCP application (such as Telnet or FTP) to that station. If you Ping a host running a version of Berkeley UNIX before 4.3BSD-Tahoe, the TTL report is 255 minus the number of routers in the round-trip path. If you Ping a host running the current version of Berkeley UNIX, the TTL report is 255 minus the number of routers in the path from the remote system to the station performing the Ping.

The Ping command sends an ICMP mandatory echo_request datagram, which asks the remote station “Are you there?” If the echo_request reaches the remote station, the station sends back an ICMP echo_response datagram, which tells the sender “Yes, I am alive.” This exchange verifies that the transmission path is open between the MAX and a remote station.

Configuring Finger support

You can configure the MAX to respond to Finger requests, as specified in RFC 1288—*The Finger User Information Protocol*.

To enable the MAX to respond to Finger requests:

1. Open the Ethernet > Mod Config.
2. Set Finger to Yes.
3. Exit and save the changes.

Displaying information

The following Show commands are useful for monitoring IP routing and related protocols:

```
show arp            Display the Arp Cache
show icmp           Display ICMP information
```

```
show if              Display Interface info. Type 'show if ?' for help.
show ip              Display IP information. Type 'show ip ?' for help.
show udp            Display UDP information. Type 'show udp ?' for help.
show tcp            Display TCP information. Type 'show tcp ?' for help.
show pools           Display the assign address pools.
```

Displaying the ARP cache

To view the ARP cache:

```
ascend% show arp
```

```
entry typ ip address      ether addr    if rtr pkt   insert
    0 DYN 10.65.212.199  00C07B605C07   0   0   0   857783
    1 DYN 10.65.212.91   0080C7C4CB80   0   0   0   857866
    2 DYN 10.65.212.22   080020792B4C   0   0   0   857937
    3 DYN 10.65.212.3    0000813DF048   0   0   0   857566
    4 DYN 10.65.212.250  0020AFF80F1D   0   0   0   857883
    5 DYN 10.65.212.16   0020AFEC0AFB   0   0   0   857861
    6 DYN 10.65.212.227  00C07B5F14B6   0   0   0   857479
    7 DYN 10.65.212.36   00C07B5E9AA5   0   0   0   857602
    8 DYN 10.65.212.71   0080C730041F   0   0   0   857721
    9 DYN 10.65.212.5    0003C6010512   0   0   0   857602
   10 DYN 10.65.212.241  0080C72ED212   0   0   0   857781
   11 DYN 10.65.212.120  0080C7152582   0   0   0   857604
   12 DYN 10.65.212.156  0080A30ECE6D   0   0   0   857901
   13 DYN 10.65.212.100  00C07B60E28D   0   0   0   857934
   14 DYN 10.65.212.1    00000C065D27   0   0   0   857854
   15 DYN 10.65.212.102  08000716C449   0   0   0   857724
   16 DYN 10.65.212.33   00A024AA0283   0   0   0   857699
   17 DYN 10.65.212.96   0080C7301792   0   0   0   857757
   18 DYN 10.65.212.121  0080C79BF681   0   0   0   857848
   19 DYN 10.65.212.89   00A024A9FB99   0   0   0   857790
   20 DYN 10.65.212.26   00A024A8122C   0   0   0   857861
   21 DYN 10.65.212.6    0800207956A2   0   0   0   857918
   22 DYN 10.65.212.191  0080C75BE778   0   0   0   857918
   23 DYN 10.65.212.116  0080C72F66CC   0   0   0   857416
   24 DYN 10.65.212.87   0000813606A0   0   0   0   857666
   25 DYN 10.65.212.235  00C07B76D119   0   0   0   857708
   26 DYN 10.65.212.19   08002075806B   0   0   0   857929
```

The ARP table displays this information:

- entry: A unique identifier for each ARP table entry.
- typ: How the address was learned, dynamically (DYN) or statically (STAT).
- ip address: The address contained in ARP requests.
- ether addr: The MAC address of the host with that IP address.
- if: The interface on which the MAX received the ARP request.
- rtr: The next-hop router on the specified interface.

Displaying ICMP packet statistics

To view the number of ICMP packets received intact, received with errors, and transmitted:

```
ascend% show icmp

3857661 packet received.
20 packets received with errors.
   Input histogram: 15070
2758129 packets transmitted.
0 packets transmitted due to lack of resources.
   Output histogram: 15218
```

The Input and Output histograms show the number of ICMP packets received and transmitted in each category.

Displaying interface statistics

To see the supported commands:

```
ascend% show if ?

show if ?           Display help information
show if stats       Display Interface Statistics
show if totals      Display Interface Total counts
```

To display the status and packet count of each active WAN link as well as local and loopback interfaces:

```
ascend% show if stats

Interface    Name    Status  Type     Speed    MTU   InPackets    Out-
packet
ie0        ethernet    Up    6     10000000   1500     107385     85384
wan0                 Down    1            0   1500       0          0
wan1                 Down    1            0   1500       0          0
wan2                 Down    1            0   1500       0          0
wanidle0               Up    6     10000000   1500       0          0
lo0       loopback     Up   24     10000000   1500       0          0
```

The output contains these fields:

- Interface: The interface name (see Chapter 10, “Configuring IP Routing.”)
- Name: The name of the profile or a text name for the interface
- Status: Up (the interface is functional) or Down.
- Type: The type of application being used on the interface, as specified in RFC 1213 (MIB-2). For example, 23 indicates PPP and 28 indicates SLIP.
- Speed: The data rate in bits per second.
- MTU: The maximum packet size allowed on the interface. MTU stands for Maximum Transmission Unit.
- InPackets: The number of packets the interface has received.
- OutPackets: The number of packets the interface has transmitted.

To display the packet count at each interface broken down by type of packet:

```
ascend% show if totals
```

```
Name  --Octets----Ucast-- -NonUcast- Discard -Error- Unknown -Same IF-
ie0  i:   7813606   85121     22383       0        0       0        0
     o: 101529978   85306       149       0        0       0        0
wan0 i:         0       0         0       0        0       0        0
     o:         0       0         0       0        0       0        0
wan1 i:         0       0         0       0        0       0        0
     o:         0       0         0       0        0       0        0
wan2 i:         0       0         0       0        0       0        0
     o:         0       0         0       0        0       0        0
wanidle0 i:     0       0         0       0        0       0        0
         o:     0       0         0       0        0       0        0
lo0  i:         0       0         0       0        0       0        0
     o:         0       0         0       0        0       0        0
```

The output contains these fields:

- Name: The interface name (see Chapter 10, “Configuring IP Routing.”)
- Octets: The total number of bytes processed by the interface.
- Ucast: Packets with a unicast destination address.
- NonUcast: Packets with a multicast address or a broadcast address.
- Discard: The number of packets that the interface could not process.
- Error: The number of packets with CRC errors, header errors, or collisions.
- Unknown: The number of packets the MAX forwarded across all bridged interfaces because of unknown or unlearned destinations.
- Same IF: The number of bridged packets whose destination is the same as the source.

Displaying IP statistics and addresses

To see the supported commands:

```
ascend% show ip ?
```

```
show ip ?           Display help information
show ip stats       Display IP Statistics
show ip address     Display IP Address Assignments
show ip routes      Display IP Routes
```

Note: For information on the Show IP Routes command, see “Working with the IP routing table” on page 10-39.

To display statistics on IP activity, including the number of IP packets the MAX has received and transmitted:

```
ascend% show ip stats
```

```
107408 packets received.
     0 packets received with header errors.
     0 packets received with address errors.
     0 packets forwarded.
     0 packets received with unknown protocols.
     0 inbound packets discarded.
107408 packets delivered to upper layers.
 85421 transmit requests.
     0 discarded transmit packets.
```

```
1 outbound packets with no route.
0 reassembly timeouts.
0 reassemblies required.
0 reassemblies that went OK.
0 reassemblies that Failed.
0 packets fragmented OK.
0 fragmentations that failed.
0 fragment packets created.
0 route discards due to lack of memory.
64 default ttl.
```

To view IP interface address information:

```
ascend% show ip address
```

```
Interface   IP Address    Dest Address   Netmask         MTU     Status
ie0         10.2.3.4      N/A            255.255.255.224   1500      Up
wan0        0.0.0.0       N/A            0.0.0.0           1500    Down
wan1        13.1.2.0      13.1.2.128     255.255.255.248   1500    Down
wan2        0.0.0.0       N/A            0.0.0.0           1500    Down
wan3        0.0.0.0       N/A            0.0.0.0           1500    Down
lo0         127.0.0.1     N/A            255.255.255.255   1500      Up
rj0         127.0.0.2     N/A            255.255.255.255   1500      Up
bh0         127.0.0.3     N/A            255.255.255.255   1500      Up
```

Displaying UDP statistics and listen table

To see the supported commands:

```
ascend% show udp ?
```

```
show udp ?          Display help information
show udp stats      Display UDP Statistics
show udp listen     Display UDP Listen Table
```

To display the number of UDP packets received and transmitted:

```
ascend% show udp stats
```

```
22386 packets received.
    0 packets received with no ports.
    0 packets received with errors.
    0 packets dropped
    9 packets transmitted.
```

In addition to the socket number, UDP port number and the number of packets queued for each UDP port on which the MAX is currently listening, the show udp listen command now shows these additional parameters:

- InQMax - The maximum number of queued UDP packets on the socket (See Queue Depth and Rip Queue Depth parameters.)
- InQLen - The current number of queued packets on the socket
- InQDrops - The number of packets discarded because it would cause InQLen to exceed InQMax
- Total Rx - The total number of packets received on the socket, including InQDrops

An example follows:

```
ascend% show udp listen

udp:
Socket Local Port InQLen InQMax    InQDrops    Total Rx
0        1023       0       1           0           0
1         520       0      50           0         532
2           7       0      32           0           0
3         123       0      32           0           0
4        1022       0     128           0           0
5        161       0      64           0           0
```

Displaying TCP statistics and connections

To see the supported commands:

```
ascend% show tcp ?

show tcp ?          Display help information
show tcp stats      Display TCP Statistics
show tcp connection Display TCP Connection Table
```

To display the number of TCP packets received and transmitted:

```
ascend% show tcp stats

     0 active opens.
    11 passive opens.
     1 connect attempts failed.
     1 connections were reset.
     3 connections currently established.
 85262 segments received.
 85598 segments transmitted.
   559 segments re-transmitted.
```

An active open is a TCP session that the MAX initiated, and a passive open is a TCP session that the MAX did not initiate.

To display current TCP sessions:

```
ascend% show tcp connection

Socket       Local              Remote                       State
0            *.23               *.*                        LISTEN
1            10.2.3.23          15.5.248.121.15003      ESTABLISHED
```

Displaying address pool status

To view the status of the MAX unit's IP address pool:

```
ascend% show pools

Pool #         Base        Count             InUse
1              10.98.1.2     55              27
2              10.5.6.1     128              0
   Number of remaining allocated addresses:    156
```

Configuring OSPF Routing

11

This chapter covers these topics:

Introduction to OSPF

OSPF (Open Shortest Path First) is the next generation Internet routing protocol. The *Open* in its name refers to the fact that OSPF was developed in the public domain as an open specification. The *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.

Note: If you have a MAX running Multiband Simulation, ospf is disabled.

RIP limitations solved by OSPF

The rapid growth of the Internet has pushed RIP (Routing Information Protocol) 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, when determining the best path to a destination network. 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 might want to direct the MAX to use active routes, if available, rather than choose routes that are down.

Problem	Description and solution
15-hop limitation	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.
Excessive routing traffic and slow convergence	RIP creates a routing table and then propagates it throughout the internet of routers, hop by hop. The time it takes for all routers to receive information about a topology change is called *convergence*. A 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 of OSPF at this release is to allow 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, we do 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, ASBR calculations are performed 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 ASE (autonomous system external). It redistributes those routes via OSPF ASE advertisements, and propagates its OSPF routes to remote WAN routers running RIP.

The MAX supports null and simple password authentication.

OSPF features

This section provides a brief overview of OSPF routing to help you configure the MAX properly. For full details about how OSPF works, see RFC 1583, “OSPF Version 2", 03/23/1994, J. Moy.

An AS (autonomous system) 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. They are referred to by the acronym EGP (exterior gateway protocol). The AS number may be used by border routers 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, as well as 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 can be used; 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 will not be able to 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 may have different sizes (different masks). This is commonly referred to as variable length subnet masks (VLSM), or Classless Inter-Domain Routing (CIDR). A packet is routed to the best (longest or most specific) match. Host routes are considered to be subnets whose masks are "all ones" (0XFFFFFFFF).

Note: Although OSPF is very useful for networks that use VLSM, we recommend that you attempt to assign subnets that are as contiguous as possible in order 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 that AS. All information exchanged within the AS is *interior.*

An AS border router (ASBR) is required to communicate with other autonomous systems by using an external gateway protocol (EGP), as shown in Figure 11-1. An EGP acts as a shuttle service between autonomous systems.

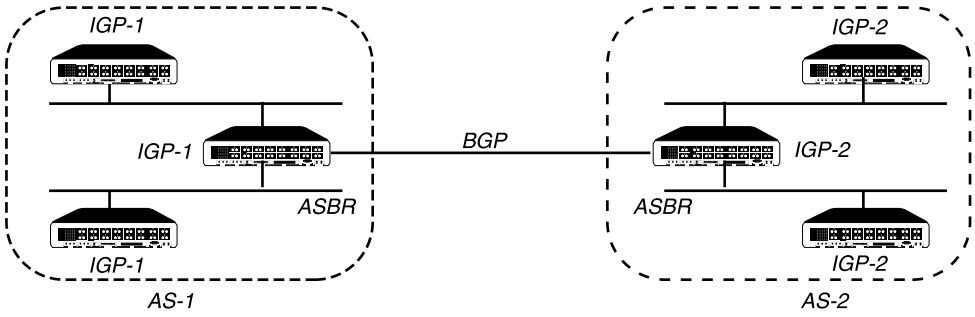


Figure 11-1. Autonomous system border routers

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 the ASBR calculations are always performed.

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, as shown in Figure 11-2.

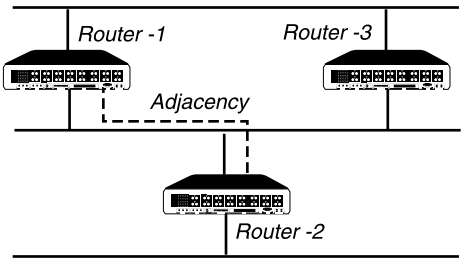


Figure 11-2. Adjacency between neighboring routers

An OSPF router dynamically detects its neighboring routers by sending its Hello packets to the multicast address All SPFRouters. It 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 become 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. This results in 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 supports the capability to address a single physical message to all of the attached routers.

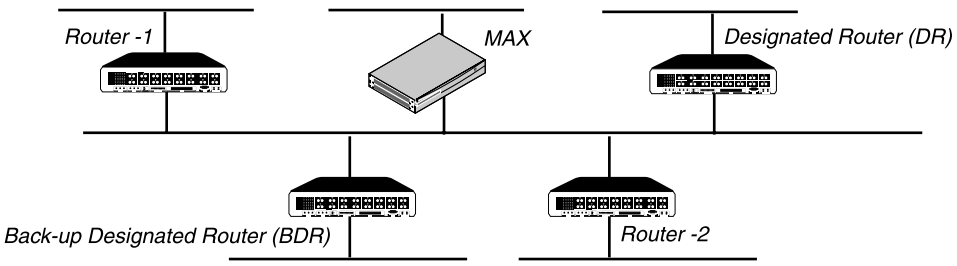


Figure 11-3. Designated and backup designated routers

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. The administrator chooses a DR and BDR based on the device's processing power and reliability.

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 plays other important roles as well to 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 224.0.0.6.

To prevent the designated router from becoming a serious liability to the network if it fails, OSPF also 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 based on 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.

The OSPF cost can also be used 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 are used to direct traffic over high-speed links. For example, if Router-2 in Figure 11-4 receives packets destined for Host B, it will route them through Router-1 across two T1 links (Cost=20) rather than across one 56kbps B-channel to Router-3 (Cost=240).

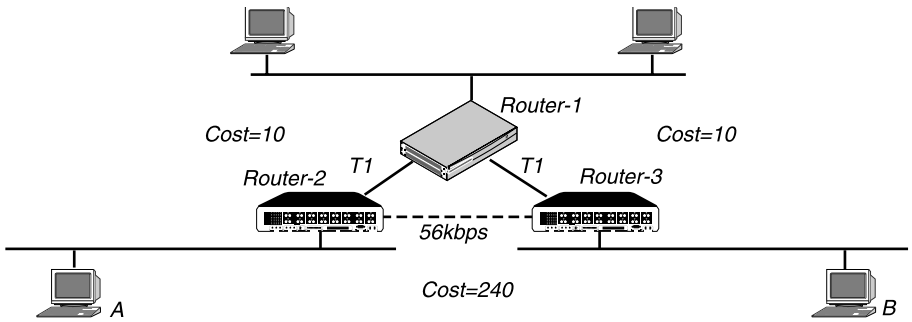


Figure 11-4. OSPF costs for different types of links

The MAX has a default cost of 1 for a connected route (Ethernet) and 10 for a WAN link. If you have two paths to the same destination, the one with the lower cost will be used. You may

want to reflect the bandwidth of a connection when assigning costs; for example, for a single B-channel connection, the cost would be 24 times greater than 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 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 an area and to the backbone area. These routers are area border routers (ABRs). In Figure 11-5, all of the routers are ABRs.If the ABRs and area boundaries are set up correctly, link-state databases are unique to an area.

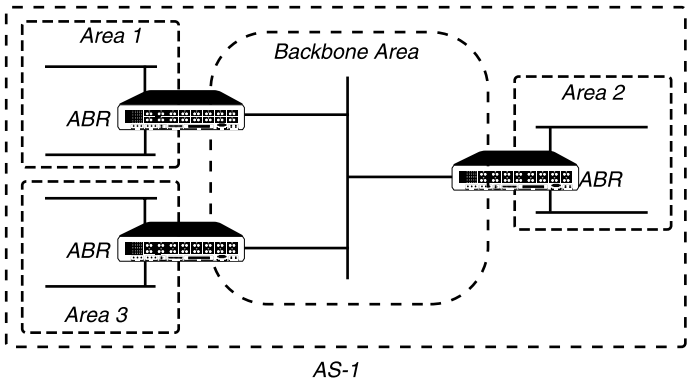


Figure 11-5. Dividing an AS into areas

Note: At this release, we recommend that you do not configure the MAX as an ABR. We currently recommend that you use the same area number for the Ethernet interface of the MAX and each of its WAN links. That are number does not have to be the backbone; 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 when there is a single exit point from the area, or when 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 RRC 1587. NSSAs allow you to treat complex networks similar to stub areas. This can simplify your networks topology and reduce OSPF-related traffic.

NSSAs and type-7 LSAs

NSSAs are similar to stub areas, except that they allow limited importing of Autonomous System (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.

Refer to RFC 1587 for complete information on NSSAs.

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.

Refer to the documentation that came with your MAX for complete information on configuring OSPF on the MAX.

To configure the MAX as 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.

6 Refer to the documentation that came with your MAX.

7 In this static route profile, specify whether you want to advertise this route outside the NSSA:

   – To advertise this route outside the NSSA, set NSSA-Type to Advertise.

   – To not advertise this route outside the NSSA, set NSSA-Type to DoNotAdvertise.

8 Exit and save the Static Rtes profile.

9 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 may 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.

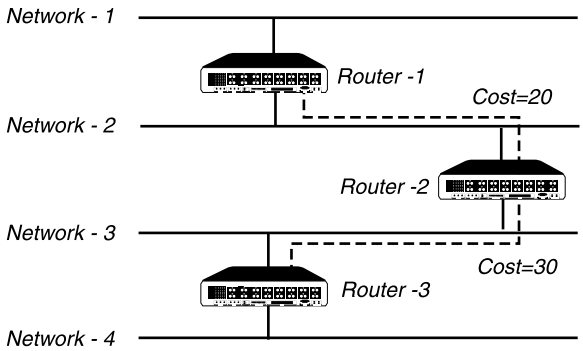


Figure 11-6. Sample network topology

The routers then use the trees to build their routing tables, as shown in Table 11-1.

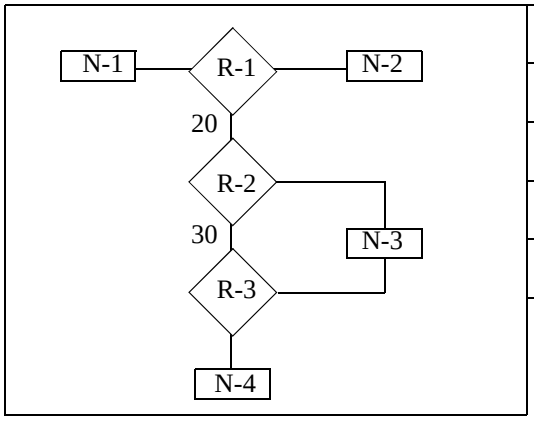
Table 11-1.Link state databases for network topology in Figure 11-6

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

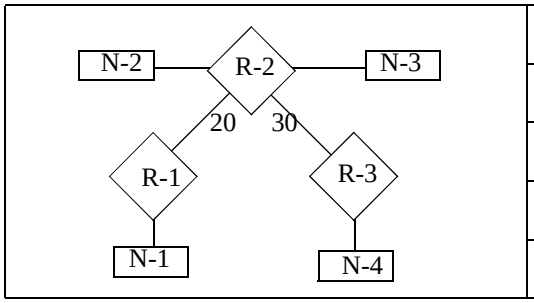
contain externally derived routing data, which is advertised throughout the AS but kept separate from the Link-state data. Also, each external route can be tagged by the advertising router, enabling the passing of additional information between routers on the boundary of the AS.

Table 11-2.Shortest-path tree and resulting routing table for Router-1



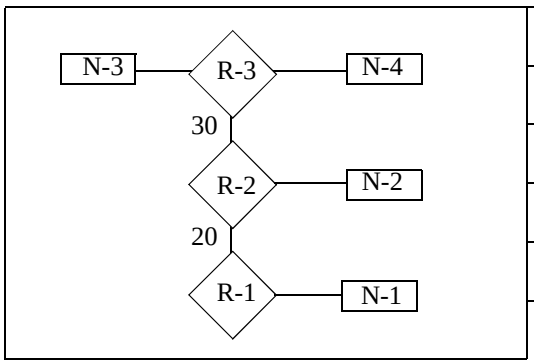
Destination	*Next Hop*	*Metric*
Network-1	Direct	0
Network-2	Direct	0
Network-3	Router-2	20
Network-4	Router-2	50

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

These are the parameters related to OSPF routing in the MAX:

```
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
         LSA-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
         LSA-type=N/A
         ASE-tag=N/A
         TransitDelay=5
         RetransmitInterval=20
```

For more information on each parameter, see the *MAX Reference Guide*.

Understanding the OSPF routing parameters

This section provides some background information about the OSPF parameters. 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 settings:

Setting	Description
Enabling OSPF on an interface	OSPF is turned off by default. To enable it on an interface, set RunOSPF to Yes.

Setting	Description
Specifying an area number and type	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	The routers in the network use the Priority value 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.)
Authentication type and key	You can specify that the MAX supports OSPF router authentication, and the key it looks for in packets to support that authentication. See “Security” on page 11-3.
Cost of the route on this interface	This parameter 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. See “Configurable metrics” on page 11-5.
Autonomous System External route (ASE) type and tag	ASEs are used only when OSPF is turned off on a particular interface. When OSPF is enabled, the ASE parameters are not applicable. ASE-type specifies he 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.

Setting	Description
LSA Type	LSAType is used only when OSPF is turned off on a particular interface. When OSPF is enabled, the LSA type is not applicable. LSA 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. You can also select Internal, which indicates that the static route be advertised in an internal LSA.
Transit delay	Specify 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.
Retransmit interval	Specify the number of seconds between retransmissions of Link-State Advertisements, Database Description, and Link State Request Packets.
OSPF global option for disabling ASBR calculations	Autonomous ASBRs (autonomous system border routers) 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 the ASBR calculations are always performed. If you must prevent the MAX from performing ASBR calculations, you can disable them in Ethernet > Mod Config > OSPF Global Options.

Example configurations adding the MAX to an OSPF network

This section describes 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. Configuring the unit labeled MAX-1 in Figure 11-7. To apply one or more of the procedures to your network, enter the appropriate settings instead of the ones shown.

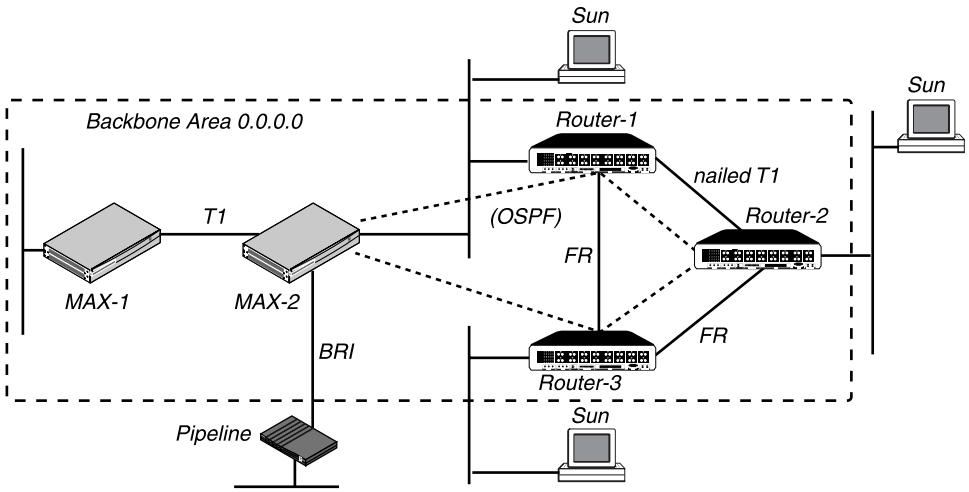


Figure 11-7. An example OSPF setup

In Figure 11-7, all OSPF routers are in the same area (the backbone area), so the units will 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 the example network diagram is in the OSPF backbone area. Although there is no limitation stated in the RFC about the number of routers in the backbone area, it is recommended that you 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 the MAX to that area. You can 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 the MAX as an IP host on that interface, you can configure it as an OSPF router in the backbone area in the Ethernet profile. To configure the MAX 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. It is not necessary to run both RIP and OSPF, and it reduces processor overhead to turn RIP off. OSPF can learn routes from RIP, incorporate them in

the routing table, assign them an external metric, and tag them as external routes. 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. See “Stub areas” on page 11-6 for background information.

4 Leave the Hello interval, Dead interval, and Priority values set to their defaults.

```
HelloInterval=10
DeadInterval=40
Priority=5
```

5 If authentication is required to get into the backbone area, 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 a 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.

```
RetransmitInterval=5
```

This 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. These 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 10. You can assign higher costs to reflect a slower connection or lower costs to set up a preferred route to a certain destination. If the cost of one route is lower than another to the same destination, the higher-cost route will not be used unless route preferences change that equation (see “Route preferences” on page 11-19).

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 (see 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
```

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
```

At this release, we recommend that you 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 uses this format.

5 Leave the Hello interval, Dead interval, and Priority values set to their defaults.

```
HelloInterval=40
DeadInterval=120
Priority=5
```

The Priority value is used to configure the MAX as a DR or BDR.

6 If authentication is required to get into the backbone area, specify the password.

For example:

```
AuthType=Simple
AuthKey=ascend0
```

If authentication is not required, 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 10.

```
Cost=10
```

8 Close the Connection profile.

Note: 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 (see Figure 11-7 on page 11-13). The remote Pipeline is an IP router that transmits routes using RIP-v2. The route to this network, as well as 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 will import 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
      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
```

See Chapter 10, “Configuring IP Routing.” Note that Connections > OSPF Options includes two ASE parameters that are active only when OSPF is *not* running on a link. When you configure these parameters, the Connection profile route will be 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, for a single-channel BRI link could have a cost approximately 24 times the cost of a dedicated T1 link:

```
         Cost=240
```

6 Specify the LSA type for this route.

```
         LSA-type=Type 2
```

`LSA-type=Type 2`

This 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 may also be used by border routers to filter this record. For example:

```
ASE-tag=cfff8000
```

8 Close the Connection profile.

Note: Of course, the remote MAX unit must also have a comparable Connection profile to connect to MAX-1.

Administering OSPF

This section describes how to work with OSPF information in the routing table and how to monitor OSPF activity in the terminal server command-line interface.

To invoke the terminal-server interface, select System > Sys Diag > Term Serv and press Enter.

Working with the routing table

The OSPF routing table includes routes built from the router's link-state database as well as those added by external routing protocols such as RIP. You can also add routes statically, for example, to direct traffic destined for a remote site through one of several possible border routers. For details on adding static routes, for example, if you want to force the use of one route over those learned from OSPF, see Chapter 10, "Configuring IP Routing.".

To view the IP routing table with added OSPF information, invoke the terminal-server (System > Sys Diag > Term Serv) and use the Iproute Show command with the –l option:

```
ascend% iproute show -l
```

In addition to the standard routing-table fields, which are described in Chapter 10, "Configuring IP Routing," the following three columns are specific to OSPF and are displayed only when you use the –l option. These OSPF-specific columns are displayed on the far right of each entry in the routing table:

```
...     Cost        T        Tag
...     1           0        0xc0000000
...     9           1        0xc8000000
...     10          0        0xc0000000
...     9           1        0xc8000000
...     1           1        0xc0000000
...     3           1        0xc8000000
...     9           1        0xc8000000
...     4           1        0xc8000000
...     5           1        0xc8000000
...     3           1        0xc8000000
...     3           1        0xc8000000
...     3           1        0xc8000000
```

- Cost

  The cost of an OSPF route. The interpretation of this cost depends on type of external metric type, displayed in the next column. If the MAX is advertising Type 1 metrics, OSPF can use the specified number as the cost of the route. Type 2 external metrics are an order of magnitude larger.

- T

  The LSA-type of metric to be advertised for an external route. 0 in this column means that it is an external-type-1 or an OSPF internal route. If this column shows a 1, it means that the route is an external-type-2 route.

- Tag

  This column specifies a 32-bit hexadecimal number attached to each external route to "tag" it as external to the AS. This number may be used by border routers to filter this record.

Multipath routing

A MAX running OSPF can alternate between two equal cost gateways. When OSPF detects more than one equally good gateway, in terms of routing costs, each equal-cost gateway is put on an equal-cost list. The router will alternate between all the gateways on the list. This is called equal-cost multipath routing.

For example, if a router A has two equal-cost routes to example.com, one via router B and the other via router C, the routing table could look like this:

```
Destination        Gateway         IF       Flg   Pref Met     Use
Age
10.174.88.0/25    10.174.88.12    wan2     OGM     10  10      52      19
10.174.88.0/25    10.174.88.13    wan3     OGM     10  10      52      19
10.174.88.12/32   10.174.88.12    wan2     OG      10  10       0      28
10.174.88.13/32   10.174.88.13    wan3     OG      10  10       0      28
192.168.253.0/24   -              ie0      C        0   0       1      49
192.168.253.6/32   -              lo0      CP       0   0      53      49
223.1.1.0/24       10.174.88.12   wan2     OG      10  10       0      19
223.5.1.0/24       10.174.88.12   wan2     OG      10  10       0      19
223.12.9.0/24      10.174.88.12   wan2     OG      10  10       0      19
255.255.255.255/32 -              ie0      CP       0   0       0      49
```

Note that the "M" in the Flags column indicates an equal-cost multipath. A Traceroute from A to example.com would look like this:

```
ascend% traceroute -q 10 example.com

traceroute to example.com (10.174.88.1), 30 hops max, 0 byte pack-
ets

1  C.example.com (10.174.88.13)  20 ms B .example.com
(10.174.88.12)  20 ms C.example.com (10.174.88.13)  20 ms B .exam-
ple.com (10.174.88.12)  20 ms  20 ms C.example.com (10.174.88.13)
60 ms  20 ms B .example.com (10.174.88.12)  20 ms C.example.com
(10.174.88.13)  20 ms B .example.com (10.174.88.12)  20 ms

2  example.com (10.174.88.1)  20 ms  20 ms  20 ms  20 ms  30 ms  20
ms  20 ms  30 ms  20 ms  30 ms
```

Note: Notice the alternating replies. The replies are statistically dispatched to B and C, with roughly 50% of the packets sent through each gateway. For background information on the routing table and on the Traceroute command, see Chapter 10, "Configuring IP Routing."

Third-party routing

A MAX running OSPF can advertise routes to external destinations on behalf of another gateway (a “third-party”). This is commonly known as advertising a forwarding address. Depending on the exact topology of the network, it may be possible for other routers to use this type of LSA and route directly to the forwarding address without involving the advertising MAX, increasing the total network throughput.

Third-party routing requires that all OSPF routers know how to route to the forwarding address. This will usually mean that the forwarding address must be on an Ethernet that has an OSPF router acting as the forwarding router, or that designated router is sending LSAs for that Ethernet to any area that sees the static route's forwarding address LSAs. To configure a static route for OSPF to advertise a third-party gateway:

1. Open a static route in Ethernet > Static Rtes.
2. Set Third-Party to Yes.
3. Set the Gateway to the forwarding address.

```
Ethernet
   Static Rtes
      Name=third-party
      Silent=No
      Active=Yes
      Dest=10.212.65.0/24
      Gateway=101.2.3.4
      Metric=3
      Preference=100
      Private=No
      Ospf-Cost=1
      LSA-Type=Type1
      ASE-tag=c00000000
      Third-Party=Yes
```

4. Close the static route.

How OSPF adds RIP routes

When the MAX establishes an IP routing connection with a caller that does not support OSPF, it imports the AS-external route from the Connection profile and adds it to the routing table. The MAX does not have to run RIP to learn these routes. RIP should be turned off when the MAX is running OSPF.

To enable OSPF to add the RIP-v2 routes to its routing table, configure RIP-v2 normally in this Connection profile. OSPF will import all RIP routes as Type-2 ASEs. The reason why RIP routes are imported with Type-2 metrics by default is that RIP metrics are not directly comparable to OSPF metrics. To prevent OSPF from interpreting RIP metrics, we assign the imported ASE route a Type-2 metric, which means that it is so large compared to OSPF costs that the metric can be ignored.

Route preferences

Route preferences provide additional control over which types of routes take precedence over others. They are necessary in a router which speaks multiple routing protocols, largely because RIP metrics are not comparable with OSPF metrics.

For each IP address and netmask pair, the routing table holds one route per protocol, where the protocols are defined as follows:

- Connected routes, such as Ethernet, have a Preference=0.
- Routes learned from ICMP Redirects have a Preference=30.
- Routes placed in the table by SNMP MIB II have a Preference=100.
- Routes learned from OSPF have a default Preference=10.
  You can modify the default in Ethernet > Mod Config > Route Pref.
- Routes learned from RIP have a default Preference=100.
  You can modify the default in Ethernet > Mod Config > Route Pref.
- A statically configured IP Route or Connection profile has a default Preference=100.
  You can modify the default in the Connection or IP Route profile.

When choosing which routes should be put in the routing table, the router first compares the Preference value, preferring the lower number. If the Preference values are equal, the router then compares the Metric field, using the route with the lower Metric.

If multiple routes exist for a given address and netmask pair, the route with the lower Preference is better. If two routes have the same Preference, then the lower Metric is better. The best route by these criteria is actually used by the router. The others remain latent or *hidden*, and are used in case the best route was removed.

To assign a WAN link the same preference as a route learned from OSPF:

1 Open Connections > IP Options.

2 Specify a preference value of 10 (the default value for OSPF routes). For example:

```
Ethernet
   Connections
      IP options…
         LAN Adrs=10.9.8.10/22
         WAN Alias=0.0.0.0
         IF Adrs=0.0.0.0
         Metric=5
         Preference=10
         Private=No
         RIP=Off
         Pool=0
```

3 Close the Connection profile.

On Ethernet, the route preferences also include ASE type and ASE tag information for routes learned from RIP. These values affect all RIP information learned across the Ethernet. To change the route preferences on Ethernet:

1 Open Ethernet > Mod Config > Route Pref.

2 Modify the parameters to adjust preference values. For example, to assign static routes the same preference value as those learned from OSPF:

```
Ethernet
   Mod Config
      Route prefs...
         Static Preference=10
         Rip Preference=100
         RipAseType=Type2
```

```
            Rip Tag=c8000000
            OSPF Preference=10
```

Or, to change RIP metrics to Type 1:

```
Ethernet
   Mod Config
      Route prefs...
         Static Preference=100
         Rip Preference=100
         RipAseType=Type1
         Rip Tag=c8000000
         OSPF Preference=10
```

3 Close the Ethernet profile.

Monitoring OSPF

The terminal server command-line interface provides commands for monitoring OSPF in the MAX. To see the options, invoke the terminal server interface (System > Sys Diag > Term Serv) and use the Show OSPF command; for example:

```
ascend% show ospf ?

show ospf ?              Display help information
show ospf errors         Display OSPF errors
show ospf areas          Display OSPF areas
show ospf general        Display OSPF general info
show ospf interfaces     Display OSPF interfaces
show ospf lsdb           Display OSPF link-state DB
show ospf lsa            Display OSPF link-state advertisements
show ospf nbrs           Display OSPF neighbors
show ospf rtab           Display OSPF routing tab
show ospf io             Display OSPF io
```

Viewing OSPF errors

To see OSPF errors, type:

```
ascend% show ospf errors

ERRORS from:                          boot
   0: IP: Bad OSPF pkt type            0: IP: Bad IP Dest
   0: IP: Bad IP proto id              1: IP: Pkt src = my IP addr
   0: OSPF: Bad OSPF version           0: OSPF: Bad OSPF checksum
   0: OSPF: Bad intf area id           0: OSPF: Area mismatch
   0: OSPF: Bad virt link info        0: OSPF: Auth type != area type
   0: OSPF: Auth key != area key       0: OSPF: Packet is too small
   0: OSPF: Packet size > IP length    0: OSPF: Transmit bad
   0: OSPF: Received on down IF        0: Hello: IF mask mismatch
    0: Hello: IF hello timer mismatch    0: Hello: IF dead timer mis-
match
    0: Hello: Extern option mismatch     0: Hello: Nbr Id/IP addr confu-
sion
   0: Hello: Unknown Virt nbr          0: Hello: Unknown NBMA nbr
   0: DD: Unknown nbr                  0: DD: Nbr state low
   0: DD: Nbr's rtr = my rtrid        0: DD: Extern option mismatch
   0: Ack: Unknown nbr                 0: Ack: Nbr state low
```

```
0: Ls Req: Nbr state low          0: Ls Req: Unknown nbr
0: Ls Req: Empty request          0: LS Req: Bad pkt
0: LS Update: Nbr state low       0: Ls Update: Unknown nbr
0: Ls Update: Newer self-gen LSA  0: Ls Update: Bad LS chksum
0: Ls Update: less recent rx      0: Ls Update: Unknown type
```

The output lists all error messages related to OSPF, with each message preceded by the number of times it has been generated since the MAX powered up. Immediately following the number is a field indicating the packet type:

- IP (IP packets)
- OSPF (OSPF packets)
- Hello (Hello packets)
- DD (Database Description packets, which are exchanged periodically between neighbors)
- Ack (every DD packet must be acknowledged)
- LS Req (Link-state request— a request for an updated database)
- LS Update (An exchange to update databases)

Viewing OSPF areas

To view information about OSPF areas, type:

```
ascend% show ospf areas

Area ID: 0.0.0.0
Auth Type: Simple Passwd  Import ASE: On  Spf Runs: 23
Local ABRs: 0  Local ASBRs: 5  Inter LSAs: 7  Inter Cksum sum:
0x2ee0e
```

- Area ID specifies the area number in dotted-decimal format.
- The Auth Type field states the type of authentication, simple or null.
- Import ASE relates to the way routes are calculated, in effect, it specifies whether the router is an ABR or not. This functionality is always ON in the MAX.
- Spf Runs show how many times the SPF calculation was run. The calculation is performed every time the router notes a topology change or receives an update from another router.
- Local ABRs shows the number of ABRs the router knows about and the number of areas. The number 0 means that the router knows about the backbone area only.
- Local ASBRs shows the number of ASBRs the router knows about.
- Inter LSAs shows the number of entries in the link-state database.
- Inter Cksum sum shows the checksum that is used to note that a database has changed.

Viewing OSPF general info

To see general information about OSPF, type:

```
ascend% show ospf general

Rtr ID: 10.5.2.154
    Status: Enabled Version: 2 ABR: Off ASBR: On
    LS ASE Count: 8 ASE Cksum sum: 0x4c303 Tos Support: TOS 0 Only
    New LSA Originate Count: 13  Rx New LSA Count: 498
```

- The Rtr ID field contains the MAX IP address (the IP address assigned to the MAX Ethernet interface).
- Status shows whether OSPF is enabled or disabled.
- Version is the version of the OSPF protocols running.
- ABR can be on or off, depending on where the MAX is situated on the network. If ABR is on, the MAX performs additional calculations related to external routes.
- ASBR is always on in the MAX. Although the MAX cannot function as an IGP gateway, it does import external routes— for example, when it establishes a WAN link with a caller that does not support OSPF—and the ASBR calculations are always performed.
- LS ASE count specifies the number of link-state database entries that are external.
- ASE Cksum sum specifies a checksum that is used to note that ASE routes in the database have changed.
- TOS Support shows the level of TOS support in the router.
- New LSA Originate Count shows the number of LSAs this router created.
- Rx New LSA Count shows the number of LSAs this router received from other OSPF routers.

To display the OSPF interfaces, type:

```
ascend% show ospf interfaces
Area      IP Address   Type   State   Cost   Pri  DR           BDR
-------------------------------------------------------------------------
-----
0.0.0.0   10.5.2.154   Bcast  BackupDR   1    5   10.5.2.155
10.5.2.154
0.0.0.0   10.5.2.154   PtoP   P To P     10   5   None         None
0.0.0.0   10.5.2.154   PtoP   P To P     10   5   None         None
```

- The Area field shows the area ID (0.0.0.0 is the backbone).
- IP Address shows the address assigned to the interface. In the MAX, the IP address is always the address assigned to the Ethernet interface. To identify WAN links, use the Type and Cost fields.
- Type can be broadcast or point-to-point. WAN links are point-to-point.
- State shows how far along the router is in the election process of a DR or BDR. The state may be 1-way (indicating that the election process has begun), 2-way (indicating that the router has received notification), BackupDR, or DR.
- Cost is the metric assigned to the link. The default cost for Ethernet is 1.
- Pri shows the designated router election priority assigned to the MAX.
- DR identifies the designated router.
- BDR identifies the backup designated router.

Viewing the OSPF link-state database

To view the router's link-state database, type:

```
ascend% show ospf lsdb
```

Note: You can expand each entry in the link-state database to view additional information about a particular LSA. See "Viewing OSPF link-state advertisements" on page 11-24.

```
LS Data Base:
Area        LS Type Link ID      Adv Rtr      Age  Len Seq #    Metric
---------------------------------------------------------------------------
-
0.0.0.0     STUB    10.5.2.146   10.5.2.146   3600 24  0        0
0.0.0.0     STUB    10.5.2.154   10.5.2.154   3600 24  0        0
0.0.0.0     STUB    10.5.2.155   10.5.2.155   3600 24  0        0
0.0.0.0     STUB    10.5.2.162   10.5.2.162   3600 24  0        0
0.0.0.0     STUB    10.5.2.163   10.5.2.163   3600 24  0        0
0.0.0.0     RTR     10.5.2.146   10.5.2.146   659  72  8000003e 0
0.0.0.0     RTR     10.5.2.154   10.5.2.154   950  84  8000000a 0
0.0.0.0     RTR     10.5.2.155   10.5.2.155   940  60  80000005 0
0.0.0.0     RTR     10.5.2.162   10.5.2.162   980  84  8000003b 0
0.0.0.0     RTR     10.5.2.163   10.5.2.163   961  60  80000005 0
0.0.0.0     NET     10.5.2.155   10.5.2.155   940  32  80000003 0
0.0.0.0     NET     10.5.2.163   10.5.2.163   961  32  80000003 0
0.0.0.0     ASE     10.5.2.16    10.5.2.163   18   36  80000098 3
0.0.0.0     ASE     10.5.2.18    10.5.2.163   546  36  80000004 10
0.0.0.0     ASE     10.5.2.144   10.5.2.146   245  36  80000037 1
0.0.0.0     ASE     10.5.2.152   10.5.2.154   536  36  80000006 1
0.0.0.0     ASE     10.5.2.152   10.5.2.155   526  36  80000004 1
0.0.0.0     ASE     10.5.2.152   10.5.2.163   18   36  80000097 9
0.0.0.0     ASE     10.5.2.155   10.5.2.163   17   36  80000097 9
0.0.0.0      ASE     10.5.2.160    10.5.2.162    568  36  80000037 1
```

- The Area field shows the area ID.
- The LS Type shows the type of link as defined in RFC 1583:

  Type 1 (RTR) are router-LSAs that describe the collected states of the router's interfaces.

  Type 2 (NET) are network-LSAs that describe the set of routers attached to the network.

  Types 3 and 4 (STUB) are summary-LSAs that describe point-to-point routes to networks or AS boundary routers.

  Type 5 (ASE) are AS-external-LSAs that describe routes to destinations external to the Autonomous System. A default route for the Autonomous System can also be described by an AS-external-LSA.
- Link ID is the target address of the route.
- Adv Rtr is the address of the advertising router.
- Age is the age of the route in seconds.
- Len is the length of the LSA.
- Seq # is a number that begins with 80000000 and increments by one for each LSA received.
- Metric is the cost of the link, not of a route. The cost of a route is the sum of all intervening links, including the cost of the connected route.

Viewing OSPF link-state advertisements

To view additional information about an LSA in the link-state database, first display the database as described in the preceding section. You can specify an LSA to expand using this format:

`show ospf lsa area ls-type ls-id adv-rtr`

This command requires that you include the first four fields of the LSA as listed in the database. You can select the first four fields and paste them in after typing the command, for example, to see an expanded view of the last entry in the link-state database shown in the previous section:

```
ascend% show ospf lsa 0.0.0.0 ase 10.5.2.160 10.5.2.162

LSA  type: ASE ls id: 10.5.2.160 adv rtr: 110.5.2.162 age: 568
           len: 36 seq #: 80000037 cksum: 0xfffa
           Net mask: 255.255.255.255 Tos 0 metric: 10 E type: 1
           Forwarding Address: 0.0.0.0 Tag: c0000000
```

Viewing OSPF neighbors

To view adjacencies, type:

```
ascend% show ospf nbrs
Area       Interface     Router Id     Nbr IP Addr   State      Mode
Pri
-------------------------------------------------------------------------
-----
0.0.0.0   10.5.2.154   10.5.2.155   10.5.2.155   Full      Slave  5
0.0.0.0   10.5.2.154   10.5.2.146   10.5.2.146   Full      Master 5
0.0.0.0   10.5.2.154   10.5.2.162   10.5.2.162   Full      Slave  5
```

- Area is the area ID.
- Interface shows the address assigned to the interface. In the MAX, the IP address is always the address assigned to the Ethernet interface.
- Router Id is the IP address of the router used to reach a neighbor. This is often the same address as the neighbor itself.
- Nbr IP Addr is the IP address of the neighbor.
- State indicates the state of the link-state database exchange. Full means that the databases are fully aligned between the MAX and its neighbor.
- Mode indicates whether the neighbor is functioning in master or slave mode. The master sends Database Description packets (polls) which are acknowledged by Database Description packets sent by the slave (responses).
- Pri shows the designated router election priority assigned to the MAX.

Viewing the OSPF routing table

To view the OSPF routing table, type:

```
ascend% show ospf rtab
SPF algorithm run 24 times since                        boot
Dest          D_mask          Area    Cost E Path Nexthop AdvRtr      L
-------------------------------------------------------------------------
-----
Nets:
10.5.2.163   255.255.255.248  0.0.0.0  10  3 EXT  10.5.2.163 10.5.2.163
0
10.5.2.163   255.255.255.255  0.0.0.0  20  0 EXT  10.5.2.163 10.5.2.163
0
10.5.2.146   255.255.255.248  0.0.0.0  20  1 EXT  10.5.2.154 10.5.2.146
```

```
0
10.5.2.146   255.255.255.255  0.0.0.0  20  0 STUB 10.5.2.154 10.5.2.146
0
10.5.2.155   255.255.255.248  0.0.0.0  10  0 INT  10.5.2.154 10.5.2.155
1
10.5.2.154   255.255.255.255  0.0.0.0  21  0 STUB 10.5.2.163 10.5.2.154
0
10.5.2.155   255.255.255.255  0.0.0.0  20  9 STUB 10.5.2.155 10.5.2.155
1
10.5.2.163   255.255.255.248  0.0.0.0  11  1 INT  10.5.2.163 10.5.2.163
0
10.5.2.162   255.255.255.255  0.0.0.0  20  0 STUB 10.5.2.163 10.5.2.162
0
10.5.2.163   255.255.255.255  0.0.0.0  10  0 STUB 10.5.2.163 10.5.2.163
0
```

- The Dest field shows the destination address.
- D_mask is the destination netmask.
- Area is the area ID.
- Cost is the cost of the route.
- E is the cost of the link. (The cost of a route is the sum of the cost of each intervening link, including the cost to the connected route.)
- Path specifies the type of link: EXT (exterior), INT (interior), or STUB (a default).
- Next hop specifies the target address from this router.
- Adv Rtr is the advertising router. Sometimes a router will advertise routes for which it is not the gateway.

Viewing OSPF protocol i/o

To display information about packets sent and received by the OSPF protocol, type:

```
ascend% show ospf io

IO stats from:                        boot
>> RECEIVED:
       0: Monitor request
     785: Hello
      13: DB Description
       6: Link-State Req
    1387: Link-State Update
      64: Link-State Ack
>> SENT:
     794: Hello
      15: DB Description
       6: Link-State Req
    1017: Link-State Update
     212: Link-State Ack
```

Setting Up IP Multicast Forwarding

12

This chapter covers these topics:

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 for transmitting audio and video on the Internet in real-time, because multicasting is a much cheaper and faster way to communicate the same information to multiple hosts.

When using the MBONE, the MAX looks like a multicast client. It responds as a client to IGMP (Internet Group Membership Protocol) packets it receives from MBONE routers, which may be IGMP version-1 or version-2, including IGMP MTRACE (multicast trace) 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.

These are the parameters for configuring multicast forwarding:

```
Ethernet
   Mod Config
      Multicast...
         Forwarding=Yes
         Membership Timeout=60
         Mbone Profile=
         Client=No
         Rate Limit=5
         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
       Ip options...
```

```
Multicast Client=No
Multicast Rate Limit=5
```

Understanding the multicast parameters

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

Enabling multicast 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. If you modify a multicast value in the Ethernet profile, you must set this parameter to No and then set it to Yes again to force a read of the new value.

Setting the Membership Timeout value

When the Ascend unit is configured as a multicast forwarder, it forwards polling messages generated by the multicast router and keeps track of active memberships from its client interfaces. You can configure the timeout value by specifying a value between 60 seconds and 65535 seconds. The factory default is still six minutes.

Specifying the MBONE interface

The MBONE interface is where the multicast router resides. 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 turned on, the MAX assumes that its Ethernet is the MBONE interface.

Monitoring the multicast heartbeat

When it is running as a multicast forwarder, the MAX is continually receiving 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 if there is a traffic breakdown. This 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 what packets will 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
Which packets will be monitored	HeartBeat Address specifies a multicast address. If the parameter is specified, the MAX listens for packets to and from this group. HeartBeat UDP Port specifies a UDP port number. If it is specified, the MAX listens only to packets received through that port. Source Addr and Source Mask specify an IP address and subnet mask. If they are specified, 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, and then polls again. HeartBeat Slot Count specifies how many times to poll before comparing the number of heartbeat packets received to the Alarm Threshold.
The threshold for generating an alarm	Heartbeat Alarm Threshold specifies a number. If the number of monitored packets falls below this number, the SNMP alarm trap is sent.

Configuring multicast forwarding on a client interface

Each local or WAN interface that supports multicast clients must set the Client (or Multicast Client) parameter to Yes. With this setting, the MAX begins handling IGMP requests and responses on the interface. It does not begin forwarding multicast traffic until the rate limit is set.

The Rate Limit specifies the rate at which the MAX accepts multicast packets from its clients. It does not affect the MBONE interface. By default, the Rate Limit parameter is set to 100. This 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 every 5 seconds. Any subsequent packets received in that 5-second window are discarded.

An implicit priority setting for dropping multicast packets

For high-bandwidth data, voice, and audio multicast applications, the MAX supports both multicast rate limiting (described immediately above) and prioritized packet dropping. If the MAX is the receiving device under extremely high loads, it drops packets according to a priority ranking, which is determined by these UDP port ranges:

- 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:

- mcast—Specified with destination address 224.0.0.0/4. All multicast addresses, except for special addresses discussed in this section, are directed to the mcast interface.
- local—Specified with destination address 224.0.0.1/32. This local address is the multicast address for all systems on the local subnet, and the MAX does not forward packets sent to this address.
- local—Specified with destination address 224.0.0.2/32. This local address is the multicast address for all routers on the local subnet, and the MAX does not forward packets sent to this address.
- local—Specified with destination address 224.0.0.5/32. This local address is the multicast address for all OSPF routers on the network, and the MAX does not forward packets sent to this address.

  If you disable OSPF routing, this route is changed from local to a black-hole interface.
- local—Specified with destination address 224.0.0.6/32. This local address is the multicast address for all OSPF designated routers on the network, and the MAX does not forward packets sent to this address.

  If you disable OSPF routing, this route is changed from local to a black-hole interface.

Forwarding from a 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.

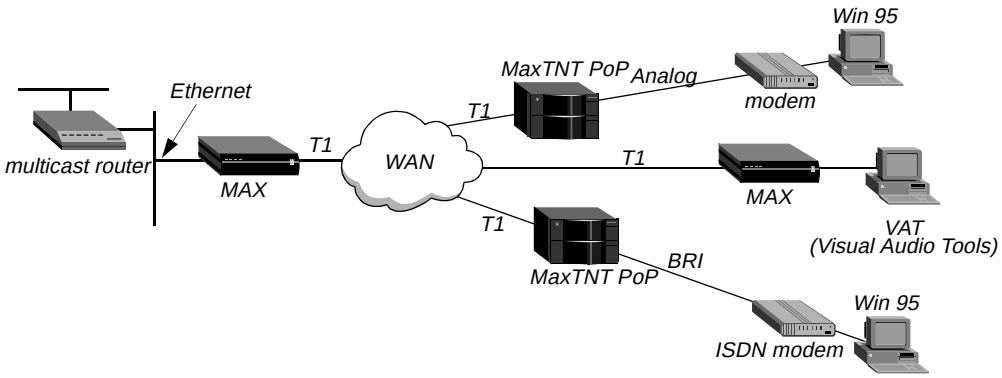


Figure 12-1. MAX forwarding multicast traffic to dial-in multicast clients

Note: Heartbeat monitoring is an optional feature. You can operate multicast forwarding without it if you prefer.

This sample profile 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.

```
        HeartBeat Addr=224.1.1.1
         HeartBeat Udp Port=16387
```

4. Specify the time, count, and alarm threshold parameters.

```
         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 5.

```
Ethernet
   Connections
      Ip options...
         Multicast Client=Yes
         Multicast Rate Limit=5
```

3. Close the Connection profile.

Forwarding from a MBONE router on a WAN link

Figure 12-2 shows a multicast router on the WAN with local and dial-in multicast clients.

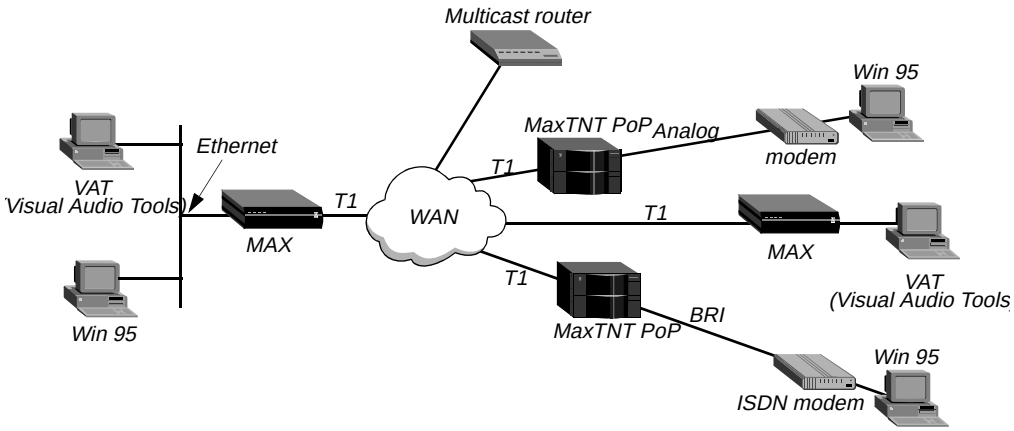


Figure 12-2. MAX acting as a multicast forwarder on Ethernet and WAN interfaces

Note: This example does not use heartbeat monitoring. If you want to configure the MAX for heartbeat monitoring, see the example settings in "Forwarding from a MBONE router on Ethernet" on page 12-4.

This sample profile specifies the MBONE interface as a WAN link accessed through a Connection profile #20.

Configuring the MAX for 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.
3. Set Multicast Rate Limit to a number lower than the default 100.

```
Ethernet
   Mod Config
      Multicast...
         Forwarding=Yes
         Membership Timeout=60
         Mbone Profile=20
         Client=Yes
         Rate Limit=5
```

4. Close the Ethernet profile.

Configuring the MBONE interface

To configure the MBONE interface:

1. Open the Connection profile for a 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 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 and set Multicast Client to Yes.

3 Set Multicast Rate Limit to a number lower than the default 100.

```
Ethernet
   Connections
      Ip options...
         Multicast Client=Yes
         Multicast Rate Limit=5
```

4 Close the Connection profile.

Administering multicast interfaces

The terminal server command-line interface provides commands to support IP multicast functionality. To see the options, invoke the terminal server interface (System > Sys Diag > Term Serv) and type:

```
ascend% show igmp ?
```

```
show igmp ?         Display help information
show igmp stats     Display IGMP Statistics
show igmp groups    Display IGMP groups Table
show igmp clients   Display IGMP clients
```

and:

```
ascend% show mrouting ?
```

```
show mrouting ?     Display help information
show mrouting stats Display MROUTING Statistics
```

Displaying the multicast forwarding table

To display active multicast group addresses and clients (interfaces) registered for each group:

```
ascend% show igmp groups
```

```
IGMP Group address Routing Table Up Time: 0:0:22:17
Hash      Group Address    Members    Expire time   Counts
N/A      Default route      *(Mbone)    ......     2224862
10       224.0.2.250
                             2           0:3:24       3211 :: 0 S5
                             1           0:3:21       145 :: 0 S5
                             0(Mbone)    ......       31901 :: 0 S5
```

The output contains these fields:

- Hash is an index to a hash table that is displayed for debugging purposes only.
  The Default route is not an entry of the hash table.
- Group address is the IP multicast address used.
  The Default route is the interface on which the multicast router resides.

  Note: The IP multicast address being monitored is marked with an asterisk, meaning that this address is joined by local application.
- Members is the interface ID on which the membership resides. 0 represents the Ethernet interface. Other numbers represent WAN interfaces, numbered according to when they became active. The interface labeled *Mbone* is the interface on which the multicast router resides.
- Expire time indicates when this membership expires. The MAX sends out IGMP queries every 60 seconds, so the expiration time is usually renewed. If the expiration time is reached, the entry is removed from the table. When this field contains periods, it indicates that the membership never expires.
- Counts shows the number of packets forwarded to the client, the number of packets dropped due to lack of resources, and the state of the membership (the state is displayed for debugging purposes).

Listing multicast clients

To display a list of multicast clients, type:

```
ascend% show igmp clients

IGMP Clients

Client      Version  RecvCount  CLU      ALU
  0(Mbone)      1       0          0       0
  2             1      39         68       67
  1             1   33310         65       65
```

The output contains these fields:

Client	indicates the interface ID on which the client resides. 0 represents the Ethernet. Other numbers are WAN interfaces, numbered according to when they became active. The interface labeled *Mbone* is the interface on which the multicast router resides.
Version	indicates the version of IGMP being used.
RecvCount	indicates the number of IGMP messages received on that interface.
CLU (current line utilization) and ALU (average line utilization)	show the percentage of bandwidth utilized across this interface. If bandwidth utilization is high, some IGMP packet types will not be forwarded.

Displaying multicast activity

To display the number of IGMP packet types sent and received:

```
ascend% show igmp stats
       46 packets received.
        0 bad checksum packets received.
        0 bad version packets received.
        0 query packets received.
       46 response packets received.
        0 leave packets received.
       51 packets transmitted.
       47 query packets sent.
        4 response packets sent.
        0 leave packets sent.
```

To display the number of multicast packets received and forwarded:

```
ascend% show mrouting stats
34988 packets received.
    57040 packets forwarded.
        0 packets in error.
       91 packets dropped.
        0 packets transmitted.
```

In many cases, the number of packets forwarded will be greater than the number of packets received, because packets may be duplicated and forwarded across multiple links.

Setting Up Virtual Private Networks

13

This chapter covers these topics:

Introduction to virtual private networks

Virtual Private Networks 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 occurs between two Ascend units via UDP/IP. The MAX encapsulates all packets passing through the tunnel in standard GRE (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.

Point-to-Point-Tunneling Protocol (PPTP) was developed by Microsoft Corporation 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.

Layer 2 Tunneling Protocol (L2TP) is specified in version 8 of the Internet Engineering Task Force (IETF) draft titled *Layer Two Tunneling Protocol "L2TP,"* dated November, 1997. 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.

The MAX does not support dial-in users, so its support of PPTP consists of routing or forwarding PPTP traffic as appropriate. The MAX does not act as either a PPTP Access Concentrator (PAC) or a PPTP Network Server (PNS).

Configuring ATMP tunnels

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 terminating part of the tunnel is the home agent, where most of the ATMP intelligence takes place. 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.

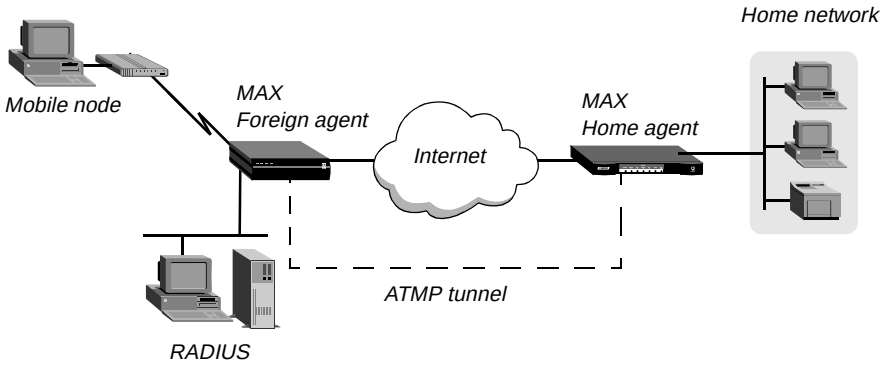


Figure 13-1. ATMP tunnel across the Internet

How the MAX creates ATMP tunnels

This is how the MAX establishes an ATMP tunnel connection:

1. A mobile node dials a connection to the foreign agent.
2. The foreign agent authenticates the mobile node using a RADIUS profile.

   The MAX requires RADIUS authentication of the mobile node, because RADIUS only 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. It sends up to 10 RegisterRequest messages at 2-second intervals, timing out and logging a message if it receives no response to those 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 down the tunnel.

The foreign agent can send its request a maximum of ten times, or until it receives a DeregisterReply. If the foreign agent receives packets for a mobile node whose connection has been terminated, the foreign agent silently discards the packets.

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

The parameters related to foreign agent configuration are:

```
Ethernet
   Mod Config
      ATMP options...
         ATMP Mode=Foreign
         Type=N/A
         Password=N/A
         SAP Reply=N/A
         UDP Port=5150
```

For the IP routing connection to the home agent:

```
Ethernet
   Mod Config
      Ether options...
         IP Adrs=10.65.212.226/24

Ethernet
   Connections
      Station=home-agent
      Active=Yes
      Dial #=555-1212
      Route IP=Yes
      IP options...
         LAN Adrs=10.1.2.3/24
```

To use RADIUS for 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
```

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
```

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"
```

For more information on each parameter, see the *MAX Reference Guide*. For details on attributes and configuring external authentication, see the MAX *RADIUS Configuration Guide*.

Understanding the foreign agent parameters and attributes

This section provides some background information on configuring a foreign agent to initiate an ATMP request to the home agent MAX.

Foreign agent parameters	Description
ATMP mode	For the foreign agent, the mode is Foreign, which makes the type, password, and SAP Reply fields 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.
IP configuration and Connection profile	The cross-Internet connection to the home agent is an IP routing connection, which the MAX authenticates and establishes in the usual way. For details, see Chapter 10, “Configuring IP Routing.”

Foreign agent parameters	Description
Configuring the foreign agent to authenticate using RADIUS	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*.
Creating a RADIUS user profile for a mobile node running TCP/IP	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.

The required attributes when the mobile node and home network are routing IP are:

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`

The required attributes when the mobile node and home network are routing IPX are:

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`

The foreign agent attributes and their descriptions are:

Attribute	Description
Ascend-Primary-Home-Agent	This is the IP address of the home agent, used to locate the Connection profile (or RADIUS profile) for the IP connection to the home agent.

Attribute	Description
Ascend-Home-Agent-Password	This is the password used to authenticate the ATMP tunnel itself, which must match the password specified in the home agent's Ethernet > Mod Config > ATMP Options. All mobile nodes use the *same* ATMP-Home-Agent-Password.
Ascend-Home-Agent-UDP-Port	This must match the UDP port configuration in Ethernet > Mod Config > ATMP Options. It is required only for a port number other than the default 5150.
Ascend-Home-Network-Name	This is the name of the home agent's local Connection profile to the home network. It is required only when the home agent is operating in gateway mode (when it has a nailed WAN link to the home network). See "Configuring a home agent in gateway mode" on page 13-12.
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	This is a virtual IPX network number. It is 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	This is a node address to represent the mobile node on the virtual IPX network. The node address is represented as a 12-digit string, which must be enclosed in double-quotes.

Example foreign agent configuration (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 using 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 details, see the MAX *RADIUS Configuration 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
      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 authenticates the mobile node using RADIUS. It then looks for a profile with an IP address that matches the Ascend-Home-Agent-IP-Addr value, so it can bring up an IP connection to the home agent.

Example foreign agent configuration (IPX)

The foreign agent configuration to support IPX connections via ATMP is the same as the one shown in the previous section. The only difference is in the mobile node's user profile. For 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 authenticates the mobile node using RADIUS. It then looks for a profile with an IP address that matches the Ascend-Home-Agent-IP-Addr value, so it can bring up an IP connection to the home agent.

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. It also adds a host route to the mobile node to its routing table.

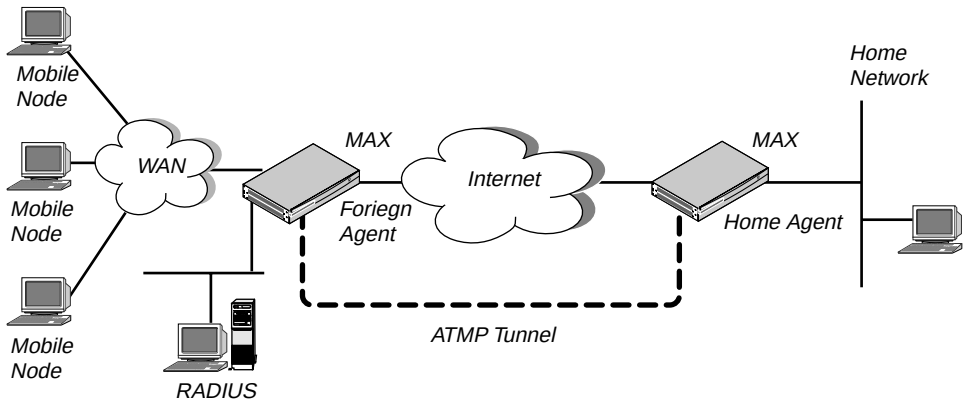


Figure 13-2. Home agent routing to the home network

The MAX requires the IPX routing parameters in the Ethernet profile only if the MAX is routing IPX. These are the parameters 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
```

For the IP routing connection to the foreign agent:

```
Ethernet
   Connections
      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 on configuring a home agent in router mode. For more information on each parameter, see the *MAX Reference Guide*.

ATMP mode and type

For the home agent, the mode is Home. 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

This is the password used to authenticate the ATMP tunnel itself, which must match the password specified in the Ascend-Home-Agent-Password attribute of mobile nodes' RADIUS profiles. (All mobile nodes use the same password for that attribute.)

SAP Reply

This 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 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.

IP configuration and Connection profile

The cross-Internet connection to the foreign agent is an IP routing connection, which the MAX authenticates and establishes in the usual way. For details, see Chapter 10, "Configuring IP Routing."

Notes about 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 based on 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 to enable local hosts to ARP for the mobile node.

For details on IP routes, see "Configuring IP Routing" on page 10-1. For information about IPX routes, see "Configuring IPX Routing" on page 9-1.

Example 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 may 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 ATMP Type to Router.
3. Specify the password used to authenticate the tunnel (Ascend-Home-Agent-Password).

```
      ATMP options...
         ATMP Mode=Home
         Type=Router
         Password=private
         SAP Reply=No
         UDP Port=5150
```

4. Close the Ethernet profile.
5. Open a Connection profile and configure an IP routing connection to the foreign agent. For example:

```
Ethernet
   Connections
      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 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 to communicate 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 Chapter 9, “Configuring IPX Routing.”

2 Open the ATMP Options subprofile and set ATMP Mode to Home and Type to Router.

3 Specify the password used to authenticate the tunnel (Ascend-Home-Agent-Password).

4 Set SAP Reply to Yes.

```
ATMP options...
   ATMP Mode=Home
   Type=Gateway
   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
      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 configured 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.

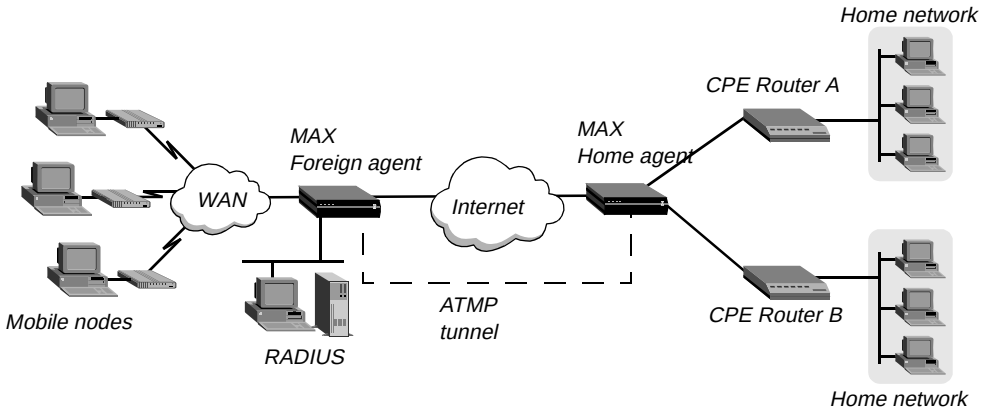


Figure 13-3. Home agent in gateway mode

Note: To enable hosts and routers on the home network to reach the mobile node, you must configure a static route in the CPE (customer premise equipment) 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.

These are the parameters for configuring a home agent in gateway 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=Gateway
         Password=private
         SAP Reply=No
         UDP Port=5150
```

For the IP routing connection to the foreign agent:

```
Ethernet
   Connections
      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
```

For the nailed connection to the home network:

```
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
```

The IPX routing parameters are required only if the MAX is routing IPX. For more information on each parameter, see the *MAX Reference Guide*.

Understanding the ATMP gateway mode parameters

This section provides some background information on configuring a home agent in gateway mode.

ATMP mode and type

For the home agent, the mode is Home. When you set the ATMP Type to Gateway, the home agent forwards packets received through the tunnel to the home network across a nailed WAN connection.

Password

This is the password used to authenticate the ATMP tunnel itself, which must match the password specified in the Ascend-Home-Agent-Password attribute of mobile nodes' RADIUS profiles. (All mobile nodes use the same password for that attribute.)

SAP Reply

This 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 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.

IP configuration and Connection profile

The cross-Internet connection to the foreign agent is an IP routing connection, which 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 in the Ascend-Home-Network-Name attribute in the mobile node's RADIUS profile. In addition, the Connection profile to the home network must specify these values:

- Nailed call type. The home agent must have a nailed connection to the home network, because it does dial the WAN connection based on packets received through the tunnel.
- ATMP Gateway session option. The ATMP Gateway parameter must be set to Yes. This parameter instructs the home agent to send data it receives back from the home network on this connection to the mobile node.
- MAX ATMP Tunnels session option. The MAX ATMP Tunnels parameter allows an administrator of the MAX to limit the number of ATMP tunnels that can be established from a home agent gateway to a home network. The MAX acts as the home agent gateway. On a home agent, the maximum number of ATMP tunnels can be specified individually for each home network.

Example 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 and set ATMP Mode to Home and Type to Gateway.

3 Specify the password used to authenticate the tunnel. This must match the Ascend-Home-Agent-Password attribute of mobile nodes' RADIUS profiles.

```
      ATMP options...
         ATMP Mode=Home
         Type=Gateway
         Password=private
         SAP Reply=No
         UDP Port=5150
```

4 Close the Ethernet profile.

5 Open a Connection profile and configure an IP routing connection to the foreign agent. For example:

```
Ethernet
   Connections
      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.

```
Ethernet
   Connections
      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
```

7 Close the Connection profile.

Example 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 to communicate 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 9, “Configuring IPX Routing.”

2 Open the ATMP Options subprofile and set ATMP Mode to Home and Type to Gateway.

3 Specify the password used to authenticate the tunnel. This must match the Ascend-Home-Agent-Password attribute of mobile nodes’ RADIUS profiles.

4 Set SAP Reply to Yes.

```
      ATMP options...
         ATMP Mode=Home
         Type=Gateway
         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
      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.

```
Ethernet
   Connections
      profile 5...
         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
```

8 Close the Connection profile.

Configuring the MAX as an ATMP multi-mode agent

You can configure the MAX to act as both a home agent and foreign agent on a tunnel-by-tunnel basis. Figure 13-4 shows an example network topology with a MAX acting as a home agent for Network B and a foreign agent for Network A.

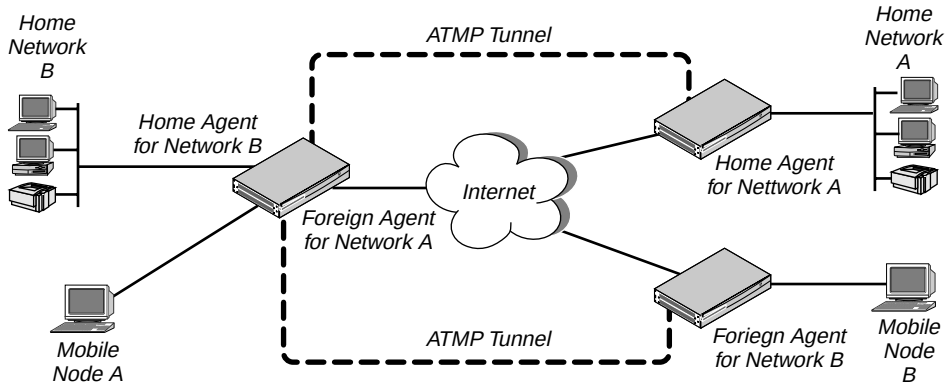


Figure 13-4. MAX acting as both home agent and foreign agent

To configure the MAX as a multi-mode agent, set ATMP Mode to Both and complete both the foreign and home agent requirements. 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:

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
```

To configure the foreign-agent aspect of the multi-mode configuration:

4 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 more information on each parameter, see the *MAX RADIUS Configuration Guide*.

5 Close the Ethernet profile.

6 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
```

7 Close the user profile.

8 Open a Connection profile and configure an IP routing connection to the Network A home agent. For example:

```
Ethernet
   Connections
      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
```

9 Close the Connection profile.

To configure the home-agent aspect of the multi-mode configuration:

10 Open a Connection profile and configure an IP routing connection to the Network B foreign agent. For example:

```
Ethernet
   Connections
      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
```

11 Open a Connection profile and configure a nailed WAN link to the Network B home network.

```
Ethernet
   Connections
      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
```

12 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 netmask as the home network*. For example, to connect to a home network whose router has this address:

```
10.1.2.3/28
```

The foreign agent's RADIUS entry for the remote router would contain lines like this:

```
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 this Framed-Address for the mobile node router (10.168.6.21/28), the connecting LAN can support up to 14 hosts.

- 10.168.6.16

  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.

- 10.168.6.31

The broadcast address for this subnet is 10.168.6.31. The broadcast address of any subnet is specified by setting the host portion of the IP address to all ones.

- 10.168.6.17—10.168.6.30

  This is the valid host address range (14 host addresses) for the LAN.

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 is directly connected to the home network, it should be configured to respond to ARP requests for the mobile node by setting Proxy ARP=Always.

  If the home agent is not directly connected 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 is passed on 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 example RADIUS entry shown above, the mobile node could support two subnets with a netmask 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 can connect 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 between a direct connection or a tunneled connection through the foreign agent.

For example, the following RADIUS entry authenticates a mobile NetWare client that will connect directly to the home agent. In this example, the home agent is configured in 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 the home agent is configured in router mode (in which it 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

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, which may support TCP/IP, IPX, or other protocols.

The MAX acts as a PAC (PPTP Access Controller), 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 PNS (PPTP Network Server). All authentication is negotiated between the Windows 95 or NT client and the PNS. The NT server's account information remain the same as if the client dialed in directly; no changes 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 called number or calling number. The following section describes how to dedicate an entire WAN access line for each destination PNS address. For details on configuring WAN lines and assigning phone numbers, see Chapter 2, "Configuring the MAX for WAN Access." For details on 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 via IP routing.

Note: The MAX handles PPTP calls differently than regular calls. No Connection profiles are used for these calls, and the Answer profile is not consulted. They are routed through the PPTP tunnel based solely upon the phone number dialed.

These are the parameters related to a PPTP PAC configuration:

```
Ethernet
   Mod Config
      L2 Tunneling Options...
         PPTP Enabled=Yes
         Line 1 tunnel type=PPTP
         Route line 1=10.65.212.11
         Line 2tunnel type=None
         Route line 2=0.0.0.0
         Line 3tunnel type=None
         Route line 3=0.0.0.0
```

```
Line 4tunnel type=None
Route line 4=0.0.0.0
```

For more information on each parameter, see the *MAX Reference Guide*.

Understanding the PPTP PAC parameters

This section provides some background information about configuring PPTP.

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 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.

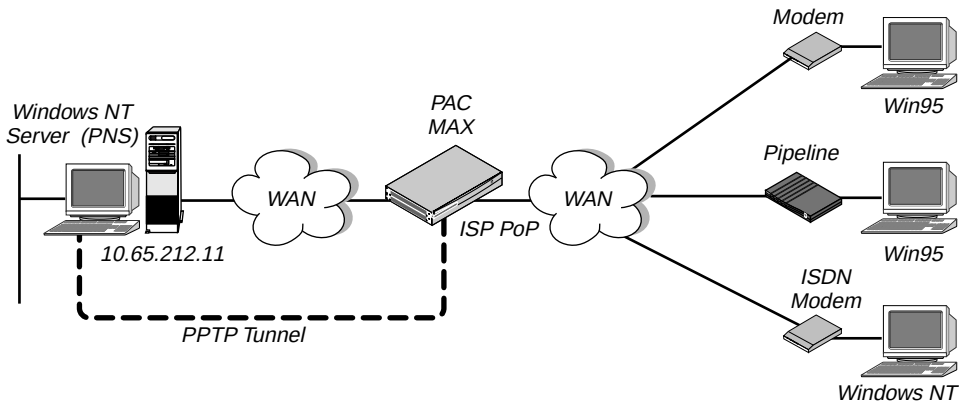


Figure 13-5. PPTP tunnel

To configure this MAX for PPTP:

1 Open Ethernet > Mod Config > PPTP Options.

2 Turn on PPTP, and specify the PNS IP address next to Route Line 4.

```
Ethernet
   Mod Config
      L2 Tunneling Options...
         PPTP Enabled=Yes
         Line 1 tunnel type=None
         Route line 1=0.0.0.0
         Line 2tunnel type=None
         Route line 2=0.0.0.0
         Line 3tunnel type=None
         Route line 3=0.0.0.0
         Line 4tunnel type=PPTP
         Route line 4=10.65.212.11
```

3 Close the Ethernet Profile.

Example PPTP tunnel across multiple POPs

Figure 13-5 shows an ISP POP MAX communicating through an intervening router to the PNS that is the end-point of its PPTP tunnel. The MAX route the packets in the usual way to reach the end-point IP address.

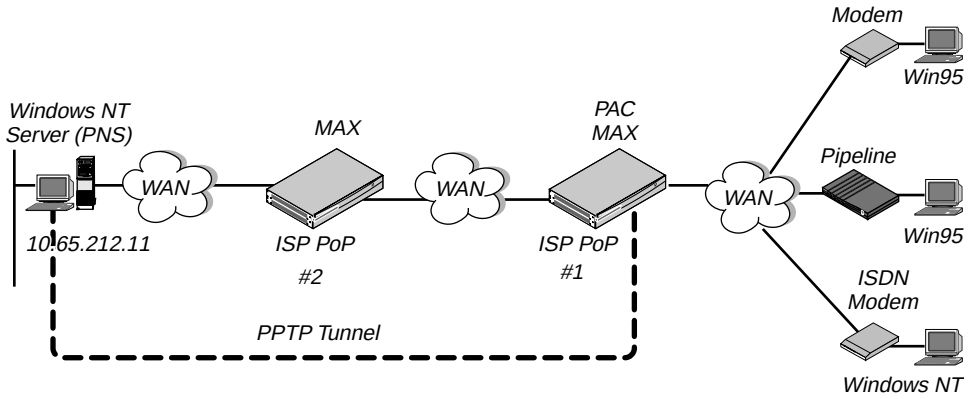


Figure 13-6. PPTP tunnel across multiple POPs

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 next to 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 2tunnel type=PPTP
         Route line 2=10.65.212.11
         Line 3tunnel type=None
         Route line 3=0.0.0.0
         Line 4tunnel 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. This does not have to be a static route, it can be learned dynamically via routing protocols. This example shows a static route to ISP POP #2:

4 Open an unused IP Route profile and activate it.

```
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 via the terminal-server interface, which 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.

To use the command, enter the following at the terminal-server prompt:

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, establish an L2TP tunnel. The LAC contacts the L2TP Network Server (LNS), which is connected 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 on the basis of expiration of the value you set for a user profile's MAX-Connect-Time attribute. You can also manually disconnect tunnels from the LNS via SNMP, the terminal-server Kill command, or the DO Hangup command (which you access by pressing <control> 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.

Configuring 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 13-7 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.

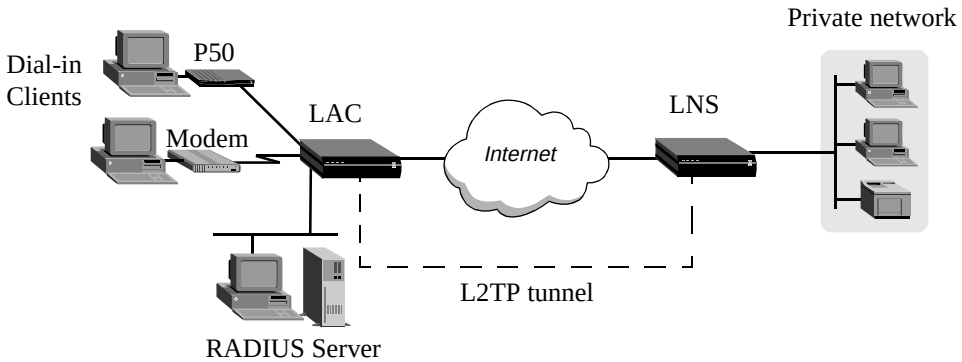


Figure 13-7. L2TP tunnel across the Internet

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. Via 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 completed, 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 acts an LAC on the basis of the dial-in client configuration. The MAX acts as an LNS when it receives an Inbound Call Request from an LAC.

Note: The MAX can support several simultaneous connections, some where it acts an LAC, and some where it acts as an LNS. For any single connection, however, the MAX can operate as either an LAC or LNS, but not both.

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 that it receives on that line.

If you use RADIUS to configure L2TP on a per-user basis, and specify the Client-Port-DNIS attribute, the LAC does not perform PAP or CHAP authentication. When use specify Client-Port-DNIS, the tunnel is created as soon as the LAC receives the DNIS number and it 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.

Configuring 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 enabled	To enable the MAX unit's LAC functionality, you must set L2TP to LAC or Both.
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, using 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 as an LAC

To configure the MAX as an L2TP LAC, you must first enable L2TP LAC on the MAX, then configure how the MAX determines which connections are tunneled.

Configuring system-wide L2TP LAC parameters

To configure system-wide L2TP LAC parameters on the MAX:

1. Open the Ethernet > Mod Config > L2 Tunneling options menu.
2. Set L2TP Enabled to either LAC or Both.

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 (labelled WAN 1 on the MAX backpanel), set Line 1 tunnel type=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 these attributes.

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.
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.

Configuring the MAX as an LNS

When 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 the configuration of MAX is simple. Proceed as follows:

1 Open the Ethernet > Mod Config > L2 Tunneling options menu.

2 Set L2TP Enabled to either LNS or Both.

MAX System Administration

14

This chapter covers these topics:

Introduction to MAX administration

This chapter describes the following administration tasks:

- Administrative configurations

  Some system- or network-wide configurations are related to the unit itself. These are described in “System and Ethernet profile configurations” on page 13-3.
- Administrative commands

  The terminal server provides commands related to managing the system, its networks, and its calls. This chapter focuses on those related to the system itself, and tells you where to find information about the network and connection-oriented commands.
- SNMP administration

  MAX configurations control which classes of events will generate traps to be sent to an SNMP manager, which SNMP managers may access the unit, and community strings to protect that access. This chapter shows you how to set up the unit to work with SNMP.

Note: You can manage the MAX from your workstation by establishing a Telnet session and logging in with sufficient administrative privileges. You can also use Telnet to manage remote Ascend units, such as Pipeline or MAX units.

Where to find additional administrative information

The following administrative topics are documented in a separate guide or supplement.

- Security profiles

  For details on Security profiles, see the *MAX Security Supplement.*
- RADIUS authentication and accounting

  For details, see the *MAX RADIUS Configuration Guide.*
- MIF (Machine Interface Format) interface

  MIF is an Ascend-specific language that provides an alternative configuration interface for Ascend units. You can use a command-line or write a MIF program that sets Ascend

parameters rather than use the configuration menus to change one parameter after another. MIF programs provide a batch-processing method of changing a configuration or performing a series of actions. For details on using it, see the *MAX MIF Supplement.*

- Sys Diag and Line Diag commands

  The Sys Diag commands enable you to reset the device, save or restore configuration information, and perform other administrative functions. The Line Diag commands enable loopbacks and other diagnostics on WAN lines. For details, see the *MAX Reference Guide*.

  You can also reset the MAX, set the configuration state of a T1 line, and obtain configuration information information from RADIUS using SNMP. For details, see the Ascend Enterprise MIB. You can download the most up-to-date verson of the Ascend Enterprise MIB by logging in as *anonymous* to ftp.ascend.com. (No password is required.)

- DO commands

  Pressing Ctrl-D in the vt100 interface displays the DO menu, which contains commands for changing security levels in the MAX, or manually dialing or clearing a call. For details, see the *MAX Reference Guide*.

- Status windows

  The status windows in the vt100 interface provide information about what is currently happening in the MAX. You can also perform DO commands, for example, clear an active connection, using the status windows. For details, see the *MAX Reference Guide*.

- Troubleshooting

  For troubleshooting tips, see Appendix A, “Troubleshooting.”

Activating administrative permissions

Before you can use the administrative commands and profiles, you must login as super-user by activating a Security profile that has sufficient permissions, such as the Full Access profile. To do so:

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

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

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

The MAX prompts you for the Full Access password:

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

 Press > to accept
```

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

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

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

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

Note: The default password for the Full Access login is *Ascend*. The first task you should perform after logging in as the super-user is to assign a new password to the profile. See the *MAX Security Supplement* for details.

System and Ethernet profile configurations

This section describes the following system administration configurations:

```
System
   Sys Config
      Name=gateway-1
      Location=east-bay
      Contact=thf
      Date=2/20/97
      Time=10:00:29
      Term Rate=9600
      Console=Standard
      Remote Mgmt=Yes
      Parallel Dial=5
      Single Answer=Yes
      Auto Logout=No
      Idle Logout=0
      DS0 Min Rst=Off
      Max DS0 Mins=N/A
      High BER=10 ** -3
      High BER Alarm=No
      No Trunk Alarm=No
      Edit=00-000
      Status 1=10-100
      Status 2=10-200
      Status 3=90-100
      Status 4=00-200
      Status 5=90-300
      Status 6=90-400
      Status 7=20-100
      Status 8=20-200

Ethernet
   Mod Config
      Log...
         Syslog=Yes
         Log Host=10.65.212.12
         Log Port=514
         Log Facility=Local0
```

For details on these parameters, see the *MAX Reference Guide.* For background information on additional parameters that appear in the System profile, see Chapter 2, “Configuring the MAX for WAN Access.”

Understanding the administrative parameters

This section provides some background information on the administration options.

The system name

The system name can contain up to 16 characters. It is a good idea to keep the name simple (do not include special characters), because it is used in negotiating bridged PPP, AIM, and BONDING connections.

Specifying who to contact about problems and the location of the unit

The contact and location fields are SNMP readable and settable, and should indicate the person to contact about this unit, and its location. You can enter up to 80 characters.

Setting the system date and time

The date and time parameters set the system date and time. If you are using SNTP (Simple Network Time Protocol), the MAX can maintain its date and time by accessing the SNTP server. See Chapter 10, “Configuring IP Routing.”

Console and term rate

The Console parameter lets you change the configuration interface, for example, you can change it from Standard to MIF. If you set it to MIF, the Machine Interface Format interface comes up when you power up the MAX. “Limited” brings up simplified menus for operation with the serial host ports (but not for bridging and routing). See the *MAX MIF Supplement* for details.

You should also verify that the data rate of your terminal emulation program is set to 9600 baud or lower and that the term-rate parameter in the System profile is also set to 9600. Higher speeds might cause transmission errors.

Allowing remote management

You can set Remote Mgmt to Yes to enable management of the MAX from a WAN link.

Dial-in and dial-out parameters

The Parallel Dial parameter specifies the number of channels that the MAX can dial simultaneously over the T1 PRI line, or that the MAX can disconnect simultaneously. Although you can specify any number of channels, the initial number of channels in a connection never exceeds the value of the Base Ch Count parameter.

The Single Answer parameter specifies whether the MAX completes the answering and routing of one call before answering and routing the next call.

Logging out the console port

The Auto Logout parameter specifies whether to log out and go back to default privileges on loss of DTR from the serial port. Idle Logout specifies the number of minutes an administrative login can remain inactive before the MAX logs out and hangs up.

DS0 minimum and maximum resets

A DS0 minute is the online usage of a single 56-kbps or 64-kbps switched channel for one minute. For example, a 5-minute, 6-channel call uses 30 DS0 minutes.

The DS0 Min Rst parameter specifies when the MAX should reset accumulated DS0 minutes to 0 (zero). You can also use this parameter to specify that the MAX should disable the timer altogether.

The Max DS0 Mins parameter specifies the maximum number of DS0 minutes a call can be online. When the usage exceeds the maximum specified by the Max DS0 Mins parameter, the MAX cannot place any more calls, and takes any existing calls offline.

Setting a high-bit-error alarm

High BER specifies the maximum bit-error rate for any PRI line. The bit-error rate consists of the number of bit errors that occur per second. The number that comes after the double asterisks specifies the power of 10 for the current ratio of error bits to total bits.

High BER alarm specifies whether the back panel alarm relay closes when the bit-error rate exceeds the value specified by the High BER parameter.

Setting an alarm when no trunks are available

No Trunk Alarm specifies whether the back panel alarm relay closes when all T1 PRI lines (or trunks) go out of service.

Customizing the vt100 interface

The Edit and Status parameters customize the status windows in the vt100 interface so that particular screens appear at startup. For details, see the *MAX Reference Guide*.

Interacting with the syslog daemon to save ASCII log files

The sylog-enabled, host, and facility parameters relate to the sending of log messages to syslogd running on a UNIX host. To maintain a permanent log of MAX system events and send Call Detail Reporting (CDR) reports to a host that can record and process them, configure the MAX to report events to a syslog host on the local IP network. The host running a syslog daemon is typically a UNIX host, but it may also be a Windows system. If the log host is not on the same subnet as the MAX, the MAX must have a route to that host, either via RIP or a static route.

Note: Do not configure the MAX to send reports to a syslog host that can only be reached by a dial-up connection. That would cause the MAX to dial the log host for every logged action, including hang ups.

The facility parameter is used to flag messages from the MAX. After you set a log facility number, you need to configure the syslog daemon to write all messages containing that facility number to a particular log file. (That will be the MAX log file.)

Responding to Finger requests (RFC 1288)

The MAX supports Finger remote user information protocol (RFC 1288). You can use Finger to get information about users currently logged into the MAX. This includes the host address, name, port, and channel. For security reasons, the MAX does not forward Finger requests. Refer to RFC 1288 for complete details of the Finger protocol.

Example administrative configurations

This section shows some sample configurations.

Setting basic system parameters

To configure the system name and other basic parameters in the System profile:

1. Open the System profile.
2. Specify a system name up to 16 characters long, enter the physical location of the MAX unit, and indicate a person to contact in case of problems.

```
System
   Sys Config
      Name=gateway-1
      Location=east-bay
      Contact=thf
```

3. If necessary, set the system date and time.

```
      Date=2/20/97
      Time=10:00:29
```

4. Specify the data transfer rate of the MAX Control port.

```
      Term Rate=9600
```

5. Close the System profile.

Configuring the MAX to interact with syslog

To maintain a permanent log of MAX system events and send Call Detail Reporting (CDR) reports to a host that can record and process them, configure the MAX to report events to a syslog host on the local IP network. Note that the Ethernet interface sends out the syslog reports. To configure the MAX to send messages to a Syslog daemon:

1. Open Ethernet > Mod Config > Log.
2. Turn on Syslog.
3. Specify the IP address of the host running the Syslog daemon.
4. Specify the port at which the Syslog daemon listens for syslog messages from this MAX.
5. Set the log facility level.

```
Ethernet
   Mod Config
      Log...
         Syslog=Yes
         Log Host=10.65.212.12
         Log Port=514
         Log Facility=Local0
```

6 Close the Ethernet profile.

To configure the Syslog daemon, you need to modify /etc/syslog.conf on the log host. This file specifies which action the daemon will perform when it receives messages from a particular log facility number (which represents the MAX). For example, if you set Log Facility to Local5 in the MAX, and you want to log its messages in /var/log/MAX, add this line to /etc/syslog.conf:

```
local5.info<tab>/var/log/MAX
```

Note: The Syslog daemon must reread /etc/syslog.conf after it has been changed.

Configuring Finger support

You can configure the MAX to respond to Finger reqests, as specified in RFC 1288—*The Finger User Informtion Protocol*.

To enable the MAX to respond to Finger requests:

1 Open the Ethernet > Mod Config menu.

2 Set Finger to Yes.

3 Exit and save the changes.

Terminal server commands

This section describes the commands available in the terminal server command-line interface. To invoke the terminal server command-line interface, you must have administrative privileges. See “Activating administrative permissions” on page 14-2.

You can open the terminal server command-line interface using any of these methods:

- Select System > Sys Diag > Term Serv, and press Enter.
- Press Ctrl-D to open the DO menu in the Main Edit menu and select E=Termsrv.
- Enter the following keystroke sequence (Escape key, left square bracket, Escape key, zero) in rapid succession:

  ```
  <Esc> [ <Esc> 0
  ```

If you have sufficient privileges to invoke the command line, you’ll see the command-line prompt; for example:

```
** Ascend Terminal Server **

ascend%
```

Note: If you have a MAX running Multiband Simulation, you cannot use the following terminal server commands: close, ipxping, open, resume, rlogin, telnet.

Displaying terminal-server commands

To display the list of terminal server commands:

```
ascend% ?
```

Or:

```
   ascend% help

?            Displays help information
help         Displays help information
quit         Closes terminal server session
hangup       Closes terminal server session
test         test <number> frame-count.] [ <optional
             fields>]
local        Go to local mode
remote       remote <station>
set          Set various items. Type ‘set ?’ for help
show         Show various tables. Type ‘show ?’ for help
iproute      Manage IP routes. Type ‘iproute ?’ for help
dnstab       Displays help information about the DNS table.
             Type 'dnstab ?' for help
slip         SLIP command
cslip        Compressed SLIP command
ppp          PPP command
menu         Host menu interface
telnet       telnet [ -a|-b|-t ] <host-name> [
             <port-number> ]
tcp          tcp <host-name> <port-number>
ping         ping <host-name>
ipxping      ipxping <host-name>
traceroute   Trace route to host.  Type 'traceroute -?' for
             help
rlogin       rlogin [ -l user -ec ] <host-name> [ -l user ]
open         open < modem-number | slot:modem-on-slot >
resume       resume virtual connect session
close        close virtual connect session
kill         terminate session
```

Returning to the vt100 menus

The following commands close the terminal server command-line interface and return the cursor to the vt100 menus.

```
quit               Closes terminal server session
hangup                "      "       "       "
local              Go to local mode
For example:

   ascend% quit
```

When a dial-in user enters the Local command, a Telnet session begins.

Commands for monitoring networks

The following commands are specific to IP or IPX routing connections, and are described in the chapter that explains those connections:

```
iproute             Manage IP routes.  Type 'iproute ?' for help
ping                ping <host-name>
ipxping             ipxping <host-name>
traceroute          Trace route to host.  Type 'traceroute -?' for help
```

For information about IPXping, see Chapter 9, "Configuring IPX Routing."

For details on IProute, Ping, and Traceroute, see Chapter 10, "Configuring IP Routing."

Commands for use by terminal-server users

The following commands must be enabled for use in Ethernet > Mod Config > TServ Options. If they are enabled, login users can initiate a session by invoking the commands in the terminal-server interface.

```
slip                SLIP command
cslip               Compressed SLIP command
ppp                 PPP command
menu                Host menu interface
telnet              telnet [ -a|-b|-t ] <host-name> [ <port-number> ]
rlogin              rlogin [ -l user -ec ] <host-name> [ -l user ]
tcp                 tcp <hostname> <port-number>
open                open < modem-number | slot:modem-on-slot >
resume              resume virtual connect session
close               close virtual connect session
```

These commands initiate a session with a host or modem, or toggle to a different interface that displays a menu selection of Telnet hosts. For details on enabling these commands, see Chapter 3, "Configuring WAN Links."

SLIP, CSLIP, and PPP commands

These commands initiate SLIP (Serial Line IP), CSLIP (Compressed SLIP), and PPP sessions from the terminal-server command line.

Menu command

You can use the Menu command to invoke the terminal-server menu mode which lists up to four hosts, which can be either Telnet hosts or raw TCP hosts. You can mix Telnet and raw TCP hosts in a menu.

Specifying Telnet hosts

The Menu command invokes the terminal-server menu mode, which lists up to four Telnet hosts as configured in Ethernet > Mod Config > TServ Options. For example:

```
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)
```

To return to the command-line, press 0. Terminal-server security must be set up to allow the operator to *toggle* between the command line and menu mode, or the Menu command has no effect.

Specifying raw TCP hosts

To specify IP addresses or DNS names of hosts to which you establish a raw TCP connection, proceed as follows:

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

2 Select one of the Host # Addr fields and enter the following:

`rawTcp` `hostaddress portnumber`

rawTcp is the required string that causes the MAX to establish a raw TCP connection when the user chooses this host number. This entry is case-sensitive and must be entered exactly as shown.

`hostname` can be the DNS name of the host or the IP address of the host. The total number of characters, including the rawTcp string, must not exceed 31.

`portnumber` is the number of the port on which the connection for this host is to be established.

3 Enter a description of the host on the Host # Text field.

Note: You cannot configure raw TCP hosts if you are using a RADIUS server to provide the list of hosts.

Example configuration combining Telnet hosts and raw TCP hosts

For example, suppose you configure the following values in the TServ Options menu:

```
Remote Conf=No
Host #1 Addr=10.10.10.1
Host #1 Text=Cleveland
Host #2 Addr=
Host #2 Text=
Host #3 Addr=
Host #3 Text=
Host #4 Addr=rawTcp corp-host 7
Host #4 Text=The Office - port 7
Immed Service=None
Immed Host=N/A
```

```
Immed Port=N/A
Telnet Host Auth=No
```

The Terminal Server menu displays the following:

```
** Ascend Pipeline Terminal Server **

     1. Cleveland
     2. The Office - port 7

     Enter Selection (1-2,q)
```

If you select 2, the a raw TCP connection is established to the host corp-host on port 7.

If a you select 1, the MAX establishes a Telnet connection to the host 10.10.10.1 on port 23, the default Telnet port.

Telnet command

The Telnet command initiates a login session to a remote host. It uses this format:

```
telnet [-a|-b|–t] <hostname> [<port-number>]
```

If DNS is configured in the Ethernet profile, you can specify a hostname:

```
ascend% telnet myhost
```

If you do not configure DNS, you must specify the host's IP address instead. There are also several options in Ethernet > Mod Config > TServ Options that affect Telnet; for example, if you set Def Telnet to Yes, you can just type a hostname to open a Telnet session to that host.

```
ascend% myhost
```

Another way to open a session is to invoke Telnet first, followed by the Open command at the Telnet prompt, for example:

```
ascend% telnet
telnet> open myhost
```

The Telnet prompt is *telnet*>. When you see that prompt, you can enter any of the Telnet commands described in "Telnet session commands" on page 14-12. You can quit the Telnet session at any time by typing quit at the Telnet prompt:

```
telnet> quit
```

Note: During an open Telnet connection, type Ctrl-] to display the *telnet*> prompt and the Telnet command-line interface. Any valid Telnet command returns you to the open session. Note that Ctrl-] does not function in binary mode Telnet. If you log into the MAX by Telnet, you might want to change its escape sequence from Ctrl-] to a different setting.

Telnet command arguments

The arguments to the Telnet command are:

- <hostname>
  If you conigureDNS, you can specify the remote system's hostname. Otherwise, hostname must be the IP address of the remote station.
- –a | –b | –t

(Optional.) You can specify -a, -b, or -t on the Telnet command line to indicate ASCII, Binary, or Transparent mode. A specification on the command line overrides the setting of the Telnet Mode parameter.

  – In ASCII mode, the MAX uses standard 7-bit mode.

  – In Binary mode, the MAX tries to negotiate 8-bit Binary mode with the server at the remote end of the connection.

  – In Transparent mode, the user can send and receive binary files, and use 8-bit file transfer protocols, without having to be in Binary mode.

- <port-number>

  (Optional.) You can specifies the port to use for the session. The default is 23, the well-known port for Telnet.

Telnet session commands

The commands in this section can be typed at the Telnet prompt during an open session. To display the Telnet prompt during an active login to the specified host, press Ctrl-] (hold down the Control key and type a right-bracket). To display information about Telnet session commands, use the Help or ? command. For example:

```
telnet> ?
```

To open a Telnet connection after invoking Telnet, use the Open command; for example:

```
telnet> open myhost
```

To send standard Telnet commands such as *Are You There* or *Suspend Process*, use the Send command. For example:

```
telnet> send susp
```

For a list of Send commands and their syntax, type:

```
telnet> send ?
```

To set special characters for use during the Telnet session, use the SET command. For example:

```
telnet> set eof ^D
```

To display current settings, type:

```
telnet> set all
```

To see a list of Set commands, type:

```
telnet> set ?
```

To quit the Telnet session and close the connection, use the Close or Quit command. For example:

```
telnet> close
```

Telnet error messages

The MAX generates an error message for any condition that causes the Telnet session to fail or terminate abnormally. These error messages may appear:

- no connection: host reset (The destination host reset the connection.)
- no connection: host unreachable (The destination host is unreachable.)
- no connection: net unreachable (The destination network is unreachable.)
- Unit busy. Try again later. (The host already has open the maximum number of concurrent Telnet sessions.)

Rlogin command

The Rlogin command initiates a login session to a remote host. It uses this format:

```
rlogin              rlogin [ -l user -ec ] <host-name> [ -l user ]
```

If you configure DNS, you can specify a hostname such as:

```
ascend% rlogin myhost
```

If DNS has not been configured, you must specify the host's IP address instead. Rlogin must also be enabled in Ethernet > Mod Config > TServ Options. The arguments to the Rlogin command are:

- <hostname>

  If you configure DNS, you can specify the remote system's hostname. Otherwise, hostname must be the IP address of the remote station.
- -e<char>

  (Optional.) This argument sets the escape character to <char>; for example:

  ```
  rlogin -e$ 10.2.3.4
  ```

  The default for <char> is a tilde (~).
- -l <username>

  (Optional.) This argument specifies that you log into the remote host as <username>, rather than as the name you used to log into the terminal server. You can specify the -l option before or after <host-name>. For example, the following two lines perform identical functions:

  ```
  rlogin -l jim 10.2.3.4
  rlogin 10.2.3.4 -l jim
  ```

  If you did not log into the terminal server using RADIUS or TACACS, you can use this option on the command-line instead of being prompted for it by the remote host.

To terminate the remote login, use the Exit command at the remote system's prompt. Or, you can use the following escape sequence:

```
<CR><ESC-CHAR><PERIOD>
```

For example, to terminate a remote login that was initiated with the default escape character (a tilde), press Return and then type a tilde followed by a period.

```
~.
```

TCP command

The TCP command initiates a login session to a remote host. It uses this format:

```
tcp <hostname> <port-number>
```

For example:

```
ascend% tcp myhost
```

The arguments to the TCP command are:

- <hostname>
  If you configure DNS, you can specify the remote system's hostname. Otherwise, hostname must be the IP address of the remote station.
- [<port-number>]
  (Optional.) You can specifies the port to use for the session. The port number typically indicates a custom application that runs on top of the TCP session. For example, port number 23 starts a Telnet session. However, terminating the Telnet session does not terminate the raw TCP session.

When the raw TCP session starts running, the MAX displays the word *connected*. You can now use the TCP session to transport data by running an application on top of TCP. You can hang up the device at either end to terminate the raw TCP session. If you are using a remote terminal server session, ending the connection also terminates raw TCP.

If a raw TCP connection fails, the MAX returns one of the following error messages:

Cannot open session: <hostname> <port-number>

You entered an invalid or unknown value for <hostname>, you entered an invalid value for <port-number>, or you failed to enter a port number.

- no connection: host reset (The destination host reset the connection.)
- no connection: host unreachable (The destination host is unreachable.)
- no connection: net unreachable (The destination network is unreachable.)

Open, Resume, and Close commands

If the MAX has V.34 digital modems installed and Modem Dialout is enabled in the TServ Options submenu, a local user can issue AT commands to the modem as if connected locally to the modem's asynchronous port. To set up a virtual connection to a V.34 mode, a user can enter the Open command in this format:

```
open [<modem number> | <slot>:<modemOnSlot>]
```

For example:

```
ascend% open 7:1
```

If the user is not sure which slot or item number to specify, the Show Modems command displays the possible choices. If the user enters the Open command without specifying any of the optional arguments, the MAX opens a virtual connection to the first available V.34 modem.

Once the user is connected to the V.34 modem, he or she can issue AT commands to the modem and receive responses from it.

To temporarily suspend a virtual connection, the user can press Ctrl-C three times. This control sequence causes the MAX to display the terminals server interface again. To resume a virtual connection suspended with Ctrl-C, the user can enter this command at the terminal server prompt:

```
ascend% resume
```

To terminate a virtual connection, the user enters this command at the terminal server prompt:

```
ascend% close
```

Administrative commands

The following commands are related to system administration:

```
test                test <number> frame-count> ] [ <optional fields> ]
remote              remote <station>
set                 Set various items. Type 'set ?' for help
show                Show various tables. Type 'show ?' for help
kill                terminate session
```

Test command

To run a self-test in which the MAX calls itself, the MAX must have two open channels: one for the placing the call, and the other for receiving it. The TEST command has this format:

```
test <phonenumber> [<frame-count>] [<optional fields>]
```

- <phonenumber>
  The phone number of the channel receiving the test call. This can include the numbers 0 through 9 and the characters ()[]-, but cannot include spaces.
- [<frame-count>]
  (Optional.) The number of frames to send during the test (a number from 1 to 65535.) The default is 100.
- [data-svc=<data-svc>]
  For data-svc, enter a data service identical to any of the values available for the Data Svc parameter of the Connection profile. For a list of valid values, see the *MAX Reference Guide*. If you do not specify a value, the default value is the one specified for the Data Svc parameter.
- [call-by-call=<T1-PRI-service>]
  For PRI-service, enter any value available to the Call-by-Call parameter of the Connection profile. The Call-by-Call parameter specifies the PRI service that the MAX uses when placing a PPP call. For a list of valid values, see the *MAX Reference Guide*. If you do not specify a value, the default is as specified for the Call-by-Call parameter.
- [primary-number-type=<AT&T-switch>]
  For AT&T-switch, specify any value available to the PRI # Type parameter of the Connection profile. The PRI # Type parameter specifies an AT&T switch. For a list of valid values, see the *MAX Reference Guide*. If you do not specify a value, the default value is the one specified for the PRI # Type parameter.
- [transit-number=<IEC>]
  For IEC, specify any value available to the Transit # parameter of the Connection profile. The Transit # parameter specifies the U.S. Interexchange Carrier (IEC) you use for long distance calls over a PRI line. For a list of valid values, see the *MAX Reference Guide*. If you do not specify a value, the default is as specified for the Transit # parameter.

For example:

```
ascend% test 555-1212
```

You can enter Ctrl-C at any time to terminate the test. While the test is running, the MAX displays the status, for example:

```
calling...answering...testing...end
200 packets sent, 200 packets received
```

If you enable trunk groups on the MAX, you can specify the outgoing lines used in the self test; if you do not, the MAX uses the first available T1 (or E1) line. For example, if you assign the trunk group 7 to line 1 on a Net/BRI module and a preceding "9" is required by your PBX to make an outgoing call, the following command places the outgoing call on line 1 of the Net/BRI module:

```
ascend% test 7-9-555-1212
```

The MAX generates an error message for any condition that causes the test to terminate before sending the full number of packets. These error messages may appear:

- bad digits in phone number

  The phone number you specified contained a character other than the numbers 0 through 9 and the characters ()[]-.

- call failed

  The MAX did not answer the outgoing call. This error can indicate a wrong phone number or a busy phone number. Use the Show ISDN command to determine the nature of the failure.

- call terminated <N1> packets sent <N2> packets received

  This message indicates the number of packets sent (<N1>) and received (<N2>).

- cannot handshake

  The MAX answered the outgoing call, but the two sides did not properly identify themselves. This error can indicate that the call was routed to the wrong MAX module, or that the phone number was incorrect.

- frame-count must be in the range 1-65535

  The number of frames requested exceeded 65535.

- no phone number

  You did not specify a phone number on the command-line.

- test aborted

  The test was terminated (Ctrl-C).

- unit busy

  You attempted to start another self-test when one was already in progress. You can run only a single self-test at a time.

- unknown items on command-line

  The command-line contained unknown items. Inserting one or more spaces in the telephone number can generate this error.

- unknown option <option>

  The command-line contained the option specified by <option>, which is invalid.

- unknown value <value>

  The command-line contained the value specified by <value>, which is invalid.

- wrong phone number

  A device other than the MAX answered the call; therefore, the phone number you specified was incorrect.

Remote command

After an MP+ connection has been established with a remote station (for example, by using the DO DIAL command), you can start a remote management session with that station by entering the Remote command in this format:

```
remote <station>
```

For example:

```
ascend% remote lab17gw
```

During the remote management session, the user interface of the remote device replaces your local user interface, as if you had opened a Telnet connection to the device. You can enter Ctrl-\ at any time to terminate the Remote session. Note that either end of an MP+ link can terminate the session by hanging up all channels of the connection.

The argument to the Remote command is the name of the remote station, which must match the value of a Station parameter in a Connection profile that allows outgoing MP+ calls, or the user-id at the start of a RADIUS profile set up for outgoing calls.

Note: A remote management session can time out because the traffic it generates does not reset the idle timer. Therefore, the Idle parameter in the Connection profile at both the calling and answering ends of the connection should be disabled during a remote management session, and restored just before exiting. Remote management works best at higher terminal speeds.

At the beginning of a remote management session, you have privileges set by the default Security profile at the remote end of the connection. To activate administrative privileges on the remote station, activate the appropriate remote Security profile by using the DO Password command (see “Activating administrative permissions” on page 14-2.)

The MAX generates an error message for any condition that causes the test to terminate before sending the full number of packets. These error messages may appear:

- not authorized

  Your current security privileges are insufficient for beginning a remote management session. To assign yourself the required privileges, log in with the DO PASSWORD command to a Security profile whose Edit System parameter is set to Yes.

- cannot find profile for <station>

  The MAX could not locate a local Connection profile containing a Station parameter whose value matched <station>.

- profile for <station> does not specify MPP

  The local Connection profile containing a Station value equal to <station> did not contain Encaps=MPP.

- cannot establish connection for <station>

  The MAX located a local Connection profile containing the proper Station and Encaps settings, but it could not complete the connection to the remote station.

- <station> did not negotiate MPP

  The remote station did not negotiate an MP+ connection. This error occurs most often when the remote station does not support MP+, but does support PPP.

- far end does not support remote management

  The remote station is running a version of MP+ that does not support remote management.

- management session failed

  A temporary condition, such as premature termination of the connection, caused the management session to fail.

- far end rejected session

  The remote station was configured to reject remote management; its Remote Mgmt parameter was set to No in the System profile.

Set command

The Set command takes several arguments. To see the Set commands:

```
ascend% set ?

set ?               Display help information
set all             Display current settings
set term            Sets the telnet/rlogin terminal type
set password        Enable dynamic password serving
set fr              Frame Relay datalink control
set circuit         Frame Relay Circuit control
```

The Set All command displays current settings.

```
ascend% set all

term = vt100
dynamic password serving = disabled
```

To specify a terminal type other than the default vt100, use the Set Term command.

The Set Password command puts the terminal server in password mode, where a third-party ACE or SAFEWORD server at a secure site can display password challenges dynamically in the terminal server interface. When the terminal server is in password mode, it passively waits for password challenges from a remote ACE or SAFEWORD server. This command applies only when using security card authentication. To enter password mode:

```
ascend% set password

Entering Password Mode...

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

To return to normal terminal server operations and thereby disable password mode, press Ctrl-C.

Note: Note that each channel of a connection to a secure site requires a separate password challenge, so for multichannel connections to a secure site, you must leave the terminal server in password mode until all channels have been established. The APP Server utility is an alternative way to allow users to respond to dynamic password challenges obtained from hand-held security cards. For details on dynamic password serving, see the *MAX Security Supplement*.

The Set FR commands enable you to bring down the nailed connection specified in the named Frame Relay profile. The connection will be reestablished within a few seconds. The Set Circuit commands let you activate or deactivate a frame relay circuit. For details, see Chapter 4, “Configuring Frame Relay.”

Show command

The Show command takes several arguments. To see the Show commands:

```
ascend% show ?
```

```
show ?          Display help information
show arp        Display the arp cache
show icmp       Display ICMP information
show if         Display Interface info. Type ‘show if ?’ for help
show ip         Display IP information. Type 'show ip ?' for help.
show udp        Display UDP information. Type 'show udp ?' for help
show igmp       Display IGMP information. Type 'show igmp ?' for help.
show mrouting   Display MROUTING information. Type 'show mrouting ?' f
                ?’
show ospf       Display OSPF information. Type 'show ospf ?' for help.
show tcp        Display TCP information. Type 'show tcp ?' for help
show dnstab     Display local DNS table. Type ‘show dnstab ?’ for help
show netware    Display IPX information. Type 'show netware ? ' for
                help
show isdn       Display ISDN events.  Type 'show isdn <line number’
                for help
show fr         Display Frame relay info. Type 'show fr ?' for help
show pools      Display the assign address pools
show modems     Display status of all modems
show calls      Display status of calls
show pad        Display X25/PAD information
show uptime     Display system uptime
show revision   Display system revision
show v.110s     Display status of all v.110 cards
show users      Display concise list of active users
show x25        Display status of X.25 stack
```

Note: Many of the Show commands are specific to a particular type of usage, for example, IP routing or OSPF. The chapters of this guide that relate to these types of connection and routing describe the relevant Show commands.

Show commands related to network information

The following Show commands are related to monitoring protocols and other network-specific information:

Table 14-1.Network-specific Show commands

Show command	Where described
`show arp`	See Chapter 10, “Configuring IP Routing.”
`show icmp`	See Chapter 10, “Configuring IP Routing.”
`show if`	See Chapter 10, “Configuring IP Routing.”
`show ip`	See Chapter 10, “Configuring IP Routing.”
`show udp`	See Chapter 10, “Configuring IP Routing.”
`show igmp`	See Chapter 12, “Setting Up IP Multicast Forwarding.”
`show mrouting`	See Chapter 12, “Setting Up IP Multicast Forwarding.”
`show ospf`	See Chapter 11, “Configuring OSPF Routing.”
`show tcp`	See Chapter 10, “Configuring IP Routing.”
`show dnstab`	See Chapter 10, “Configuring IP Routing.”
`show netware`	See Chapter 9, “Configuring IPX Routing.”
`show fr`	See Chapter 4, “Configuring Frame Relay.”
`show pools`	See Chapter 10, “Configuring IP Routing.”
`show pad`	See Chapter 6, “Configuring X.25.”
`show x25`	See Chapter 6, “Configuring X.25.”

Show ISDN

The Show ISDN command enables the MAX to display the last 20 events that have occurred on the specified ISDN line. Enter the command in this format:

```
show isdn <line-number>
```

where <line-number> is the number of the ISDN line. For details on how lines are numbered, see Chapter 2, “Configuring the MAX for WAN Access.” For example, to display information about the leftmost built-in WAN port:

```
ascend% show isdn 0
```

The MAX responds with one or more of these messages:

```
PH: ACTIVATED
PH: DEACTIVATED
DL: TEI ASSIGNED (BRI interfaces only)
```

```
DL: TEI REMOVED (BRI interfaces only)
NL: CALL REQUEST
NL: CLEAR REQUEST
NL: ANSWER REQUEST
NL: CALL CONNECTED
NL: CALL FAILED/T303 EXPIRY
NL: CALL CLEARED/L1 CHANGE
NL: CALL REJECTED/OTHER DEST
NL: CALL REJECTED/BAD CALL REF
NL: CALL REJECTED/NO VOICE CALLS
NL: CALL REJECTED/INVALID CONTENTS
NL: CALL REJECTED/BAD CHANNEL ID
NL: CALL FAILED/BAD PROGRESS IE
NL: CALL CLEARED WITH CAUSE
```

In some cases, the message can include a phone number (prefixed by #), a data service (suffixed by K for kbps), a channel number, TEI assignment, and cause code. For example, this information might display:

```
PH: ACTIVATED
NL: CALL REQUEST: 64K, #442
NL: CALL CONNECTED: B2, #442
NL: CLEAR REQUEST: B1
NL: CALL CLEARED WITH CAUSE 16 B1 #442
```

For information on each of the messages that can display, see the CCITTT Blue Book Q.931 or other ISDN specifications.

Show Modems

To display the status of the MAX unit's digital modems, enter the Show Modems command. For example, the following is output from a MAX with a V.34 modem slot card in slot 8::

```
ascend% show modems

slot:item    modem    status
   8:1         1       online
   8:2         2       online
   8:3         3       online
   8:4         4       idle
   8:5         5       idle
   8:6         6       idle
   8:7         7       idle
   8:8         8       idle
```

8-MOD and 12-MOD K56Flex modem slot cards are not numbered sequentially. This numbering does not affect functionality.

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

```
ascend% show modems

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

```
8:7         6      idle
8:10        7      idle
8:11        8      idle
```

As another example, if you have an 12-MOD modem card in slot 8 in a MAX, the Show Modems command in the Terminal Server displays the following output:

```
ascend% show modems

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

The output contains these fields:

Field	Description
slot item	The slot and port number of the modem. For example, 8:1 indicates the first port on the digital modem card installed in slot 8.
modem	The SNMP interface number of each modem.
status	Modem status, which may be one of the following strings: – idle: The modem is not in use. – awaiting DCD: The call is up and waiting for DCD. – awaiting codes: DCD is up, and the call is waiting for modem result codes. – online: The call is up. The modem can now send and receive data. – initializing: The modem is being reset.

Show Calls

The Show Calls commands displays information about active calls on a German 1TR6 or Japan NTT switch type.

```
ascend% show calls

Call ID  Called Party ID Calling Party ID InOctets OutOctets

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

The output includes these fields:

Field	Description
CallID	An identifier for the call
CalledPartyID	The telephone number of the answering device (that is, this unit). This ID is obtained from layer 3 protocol messages during call setup.
CallingPartyID	The telephone number of the caller. This ID is obtained from layer 3 protocol messages during call setup.
InOctets	The total number of octets received by the user from the moment the call begins until it is cleared.
OutOctets	The total number of octets sent by the user from the moment the call begins until it is cleared.

Show Uptime

To see how long the MAX has been running:

```
ascend% show uptime
system uptime: up 2 days, 4 hours, 38 minutes, 43 seconds
```

If the MAX stays up 1000 consecutive days with no power cycles, the number of days displayed *turns over* to 0 and begins to increment again.

Show Revision

The Show Revision command displays the software load and version number currently running in the MAX.

```
ascend% show revision
techpubs-lab-17 system revision: ebiom.m40 5.0A
```

Show V.110s

To display the status of the MAX unit's v.110 cards:

```
ascend% show v.110s
slot:item    v.110s    status
   4:1         1       in use
   4:2         2       in use
   4:3         3       in use
   4:4         4       open issued
   4:5         5       carrier detected
   4:6         6       session closed
   4:7         7       idle
   4:8         8       in use
```

The output contains these fields:

Field	Description
slot item	The slot and port number of the V110 port. For example, 8:1 indicates the first port on the V110 card installed in slot 8

Field	Description
v.110s	The SNMP interface number of each V110 card.
status	V.110 port status, which may be one of the following strings: – idle: The V.110 port is not in use. – open issued: An open was issued, but the MAX has not synced up with the far end. – carrier detected: A carrier was detected from the remote end. – in use: A V.110 session is up.

Show Users

To display the number of active sessions:

```
   ascend% show users
I Session    Line: Slot: Tx    Rx    Service    Host         User
O ID         Chan  Port  Data  Rate  Type[mpID] Address      Name
O 231849873  1:1   9:1   56K   56K   MPP[1]     10.10.68.2   jdoe
I 231849874  1:3   3:1   28800 33600 Termsrv    N/A          Modem 3:1
O 214933581  1:2   9:2   56K   56K   MPP[1]     10.10.4.9    arwp50
O 214933582  1:6   9:3   56K   56K   MPP[1]     MPP Bundle   arwp50
```

The output contains these fields:

Field	Description
IO	specify I (incoming call) or O (outgoing call)
Session ID	shows the unique session-ID. This is the same as Acct-Session-ID in RADIUS.
Line	Channel shows the line and channel on which the session is established.
Slot	Port shows the slot and port of the service being used by the session, which may be the number of a slot containing a modem card and the modem on that card, or the virtual slot of the MAX unit's bridge/router, with port giving the virtual interfaces to bridge/router starting with 1 for the first session of a multichannel session.
Tx Data Rate	shows the transmit data rate in bits per second.
Rx Data Rate	shows the receive data rate in bits per second.
Service Type	shows the type of session, which may be Termsrv or a protocol name. For MP and MPP, this shows the bundle ID shared by the calls in a multichannel session. The special values Initial and Login document the progress of a session. Initial identifies sessions that do not yet have a protocol assigned. Login identifies Termsrv sessions during the login process.

Field	Description
Host Address	shows the network address of the host originating the session. For some sessions this field is N/A. For outgoing MPP sessions only the first connection has a valid network address associated with it. All other connections in the bundle have the network address as listed as MPP Bundle
User Name	The station name associated with the session. Initially, this value is Answer. This is usually replaced with the name of the remote host. For terminal server sessions this is the login name. Prior to login completion this field will show the string “modem x:y” where x and y are the slot and port of them modem servicing the session.

Kill command

The Kill command enables you to disconnect a user who establishes a connection with the Ascend unit via Telnet. You can disconnect the user by session ID. The disconnect code that results is identical to the RADIUS disconnect code, allowing you to track all administrative disconnects. To terminate a Telnet session, use this format:

```
kill <session ID>
```

where <session ID> is the session ID as displayed by the Show Users command described in the preceding section. The reported disconnect cause is DIS_LOCAL_ADMIN. The active Security profile must have Edit All Calls=Yes. If Edit All Calls=No, this message displays when you issue the kill command:

```
Insufficient security level for that operation.
```

When the session is properly terminated, a message like this one displays:

```
Session 216747095 killed.
```

When the session is not terminated, a caution like this one displays:

```
Unable to kill session 216747095.
```

Dirdo commands to support Deutsche Telekom’s ZGR

The following Dirdo commands enable you to show, add, or delete entries from the answer list or the subaddress list. The following table lists the new commands.To use them, you must have administrative authorization.

Command	Description
Dirdo show ans | sub	Lists all the answer numbers (when you specify ans) or all the subaddresses (when you specify sub) on the RADIUS bootup server.

Command	Description
Dirdo add ans *num* | sub *num*	Adds the answer number (when you specify ans) or subaddress (when you specify sub) that you enter as the *num* argument. For example, to add the subaddress 1234 to the list, enter the following command: **Dirdo add sub 1234**
Dirdo del ans *num* | sub *num*	Deletes the answer number (when you specify ans) or subaddress (when you specify sub) that you enter as the *num* argument. For example, to delete the subaddress 1234 from the list, enter the following command: **Dirdo del sub 1234**

SNMP administration support

The MAX supports SNMP on a TCP/IP network. An SNMP management station that uses the Ascend Enterprise MIB can query the MAX, set some parameters, sound alarms when certain conditions appear in the MAX, and so forth. An SNMP manager must be running on a host on the local IP network, and the MAX must be able to find that host, either via static route or RIP.

SNMP has its own password security, which you should set up to protect the MAX from being reconfigured from an SNMP station.

Configuring SNMP access security

There are two levels of SNMP security: community strings, which must be known by a community of SNMP managers to access the box, and address security, which excludes SNMP access unless it is initiated from a specified IP address. These are the relevant parameters:

```
Ethernet
   Mod Config
      SNMP options...
         Read Comm=Ascend
         R/W Comm Enable=No
         R/W Comm=Secret
         Security=Yes
         RD Mgr1=10.0.0.1
         RD Mgr2=10.0.0.2
         RD Mgr3=10.0.0.3
         RD Mgr4=10.0.0.4
         RD Mgr5=10.0.0.5
         WR Mgr1=10.0.0.11
         WR Mgr2=10.0.0.12
         WR Mgr3=10.0.0.13
         WR Mgr4=10.0.0.14
         WR Mgr5=10.0.0.15
```

For complete information on each parameter, see the *MAX Reference Guide*.

Understanding the SNMP options

This section provides some background information on the SNMP profile settings.

- enabling SNMP set commands

  R/W Comm Enable disables SNMP set commands by default. Before you can use an SNMP set command, you must set R/W Comm Enable to Yes.

  Note: Even you enable R/W Comm, you must still know the read-write community string to use a set command.

- Setting community strings

  The Read Comm parameter specifies the SNMP community name for read access (up to 32 characters), and the R/W Comm parameter specifies SNMP community name for read/write access.

- Setting up and enforcing address security

  If the Security parameter is set to No (its default value), any SNMP manager that presents the right community name will be allowed access. If you set this parameter to Yes, the MAX checks the source IP address of the SNMP manager and allows access only to those IP addresses listed in the RD MgrN and WR MgrN parameters, each of which specify up to five host addresses.

- resetting the MAX and determining whether the MAX has reset

  You can use SNMP (sysReset object) to reset a MAX from an SNMP manager. A one-minute timeout (not modifiable) after the reset command is issued permits the MAX to confirm the set rquest before the unit is reset.

  Information held in the Ascend Events Group is erased and its values are initialized when the MAX is reset by software or by toggling the power off and on. sysAbsoluteStartupTime is the time in seconds since January 1, 1990, and is not modified. To determine whether the MAX has actually reset, you can retrieve the SNMP object sysAbsoluteStartupTime and compare this value against the previous poll's value for Ascend Events Group variables.

Example SNMP security configuration

This example sets the community strings, enforces address security, and prevents write access:

1. Open Ethernet > Mod Config > SNMP Options.
2. Set R/W Comm Enable to Yes.
3. Specify the Read Comm and R/W comm parameter strings.
4. Set Security to Yes.
5. Specify up to five host addresses in the RD MgrN parameters. Leave the WR MgrN parameters set to zero to prevent write access.

```
Ethernet
   Mod Config
      SNMP options...
         Read Comm=Secret-1
         R/W Comm Enable=Yes
         R/W Comm=Secret-2
         Security=Yes
         RD Mgr1=10.0.0.1
         RD Mgr2=10.0.0.2
         RD Mgr3=10.0.0.3
```

```
RD Mgr4=10.0.0.4
RD Mgr5=10.0.0.5
WR Mgr1=0.0.0.0
WR Mgr2=0.0.0.0
WR Mgr3=0.0.0.0
WR Mgr4=0.0.0.0
WR Mgr5=0.0.0.0
```

6 Close the Ethernet profile.

Setting SNMP traps

A trap is a mechanism for reporting system change in real time, for example, reporting an incoming call to a serial host port. When a trap is generated by some condition, a traps-PDU (protocol data unit) is sent across the Ethernet to the SNMP manager.

These are the parameters related to setting SNMP traps:

```
Ethernet
   SNMP Traps
      Name=
      Alarm=Yes
      Port=Yes
      Security=Yes
      Comm=
      Dest=10.2.3.4
```

For details on each parameter and the events that generate traps in the various classes, see the *MAX Reference Guide*.

Understanding the SNMP trap parameters

This section provides some background information about setting traps.

- The community string for communicating with the SNMP manager

  The Comm field must contain the community name associated with the SNMP PDU.
- Classes of traps to be sent to the specified host

  The next three fields specify whether the MAX traps alarm events, security events, and port events and sends a trap-PDU to the SNMP manager.
- Specifying the destination address for the trap-status report.

  If DNS or YP/NIS is supported, the Dest field can contain the hostname of a system running an SNMP manager. The DNS or YP/NIS is not supported, the Dest field must contain the host's address.

  Note: To turn off SNMP traps, set Dest=0.0.0.0 and delete the value for Comm.

Example SNMP trap configuration

In this example profile, a community name is specified and the host's IP address is specified in the Dest parameter.

1 Open an SNMP Traps profile and assign it a name.

2 Specify the community name (for example, Ascend).

3 Set the trap types to Yes.

4 Specify the IP address of the host to which the trap-PDUs will be sent.

```
Ethernet
   SNMP Traps
      Name=security-traps
      Alarm=Yes
      Port=Yes
      Security=Yes
      Comm=Ascend
      Dest=10.2.3.4
```

5 Close the SNMP Traps profile.

Ascend enterprise traps

This section gives a brief summary of the traps generated by alarm, port, and security events. For details, see the Ascend Enterprise MIB. For details on obtaining the Ascend MIB, see "Supported MIBs" on page 14-31.

Alarm events

Alarm events (also called "error events") use trap types defined in RFC 1215 and 1315, as well as an Ascend enterprise trap type. The following trap types from RFC 1215 are supported:

- coldStart (RFC-1215 trap-type 0)

  A coldStart trap signifies that the MAX sending the trap is reinitializing itself so that the configuration of the SNMP manager or the unit might be altered.
- warmStart (RFC-1215 trap-type 1)

  A warmStart trap signifies that the MAX sending the trap is reinitializing itself so that neither the configuration of SNMP manager or the unit is altered.
- linkDown (RFC-1215 trap-type 2)

  A linkDown trap signifies that the MAX sending the trap recognizes a failure in one of the communication links represented in the SNMP manager's configuration.
- linkUp (RFC-1215 trap-type 3)

  A linkUp trap signifies that the MAX sending the trap recognizes that one of the communication links represented in the SNMP manager's configuration has come up.
- frDLCIStatusChange (RFC-1315 trap-type 1)

  A DLCIStatusChange trap signifies that the MAX sending the trap recognizes that one of the virtual circuits (to which a DLCI number has been assigned) has changed state; that is, the link has either been created, invalidated, or it has toggled between the active and inactive states.
- eventTableOverwrite (ascend trap-type 16)

  A new event has overwritten an unread event. This trap is sent only for systems that support Ascend's accounting MIB. Once sent, additional overwrites will not cause another trap to be sent until at least one table's worth of new events have occurred.

Port state change events

These traps are effective on a port-by-port basis for each port pointed to by ifIndex. The hostPort objects are used to associate a change with ifIndex objects.

- portInactive (ascend trap-type 0)

AIM port associated with the passed index has become inactive.

- portDualDelay (ascend trap-type 1)
  AIM port associated with the passed index is delaying the dialing of a second to avoid overloading devices that cannot handle two calls in close succession.
- portWaitSerial (ascend trap-type 2)
  AIM port associated with the passed index has detected DTR and is waiting for an HDLC controller to come online. CTS is off (V.25 bis dialing only).
- portHaveSerial (ascend trap-type 3)
  AIM port associated with the passed index is waiting for V.25 bis commands. CTS is on.
- portRinging (ascend trap-type 4)
  AIM port associated with the passed index has been notified of an incoming call.
- portCollectDigits (ascend trap-type 5)
  AIM port associated with the passed index is receiving digits from an RS366 interface (RS-366 dialing only).
- portWaiting (ascend trap-type 6)
  AIM port associated with the passed index is waiting for connect notification from the WAN after dialing or answer notification has been issued.
- portConnected (ascend trap-type 7)
  AIM port associated with the passed index has changed state. This change of state can be from connected to unconnected or vice versa. If connected to the far end, end-to-end data can flow but has not yet been enabled.
  The following trap report sequence shows a link is up:
  portWaiting (6)
  portConnected (7)
  portCarrier (8)
  The following trap report sequence shows a link is down:
  portConnected (7)
  portInactive (0)
- portCarrier (ascend trap-type 8)
  AIM port associated with the passed index has end-to-end data flow enabled.
- portLoopback (ascend trap-type 9)
  AIM port associated with the passed index has been placed in local loopback mode.
- portAcrPending (ascend trap-type 10)
  AIM port associated with the passed index has set ACR on the RS366 interface, and is waiting for the host device (RS-366 dialing only).
- portDTENotReady (ascend trap-type 11)
  AIM port associated with the passed index is waiting for DTE to signal a ready condition when performing X.21 dialing.

Security events

Security events are used to notify users of security problems and track access to the unit from the console. The MIB-II event *authenticationError* is a security event. The other security events are Ascend-specific.

- authenticationFailure (RFC-1215 trap-type 4)

An authenticationFailure trap signifies that the MAX sending the trap is the addressee of a protocol message that is not properly authenticated.

- consoleStateChange (ascend trap-type 12)
  The console associated with the passed console index has changed state. To read the console's state get ConsoleEntry from the Ascend enterprise MIB.
- portUseExceeded (ascend trap-type 13)
  The serial host port's use exceeds maximum set by Max DS0 Mins Port parameter associated with the passed index (namely, the interface number).
- systemUseExceeded (ascend trap-type 14)
  The serial host port's use exceeds maximum set by Max DS0 Mins System parameter associated with the passed index (namely, the interface number).
- maxTelnetAttempts (ascend trap-type 15)
  There have been three consecutive failed attempts to login onto this MAX via Telnet.

Supported MIBs

You can download the most up-to-date verson of the Ascend Enterprise MIB by logging in as *anonymous* to ftp.ascend.com. (No password is required.) In addition to the Ascend MIB, the MAX also supports objects related to Ascend functionality in the following Internet standard MIBs:

- MIB-II implementation (RFC 1213)
- DS1 MIB implementation (RFC 1406)
- RS232 MIB implementation (RFC-1317)
- Frame Relay MIB implementation (RFC-1315)
- Modem MIB implementation (RFC 1696)

You can download the most recent version of these RFCs by logging in as *anonymous* to ftp.ds.internic.net. (No password is required.)

Troubleshooting

A

This appendix explores the types of problems that might interrupt or prevent call transmission, and suggests some procedures for addressing those problems. This appendix covers these topics:

LEDs

This section describes the types of LEDs available on different MAX models, and explains the information they display.

MAX front panel

The MAX front panel includes this set of LEDs:

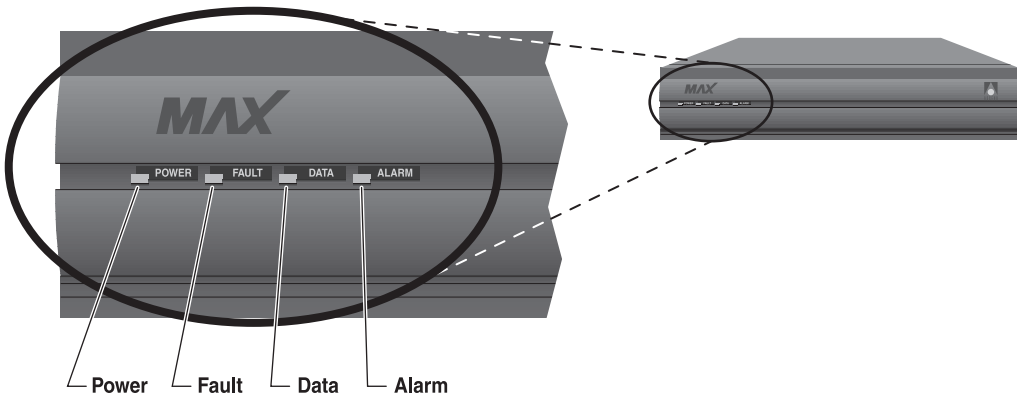


Figure A-1. MAX front panel LEDs

The front-panel LEDs report on the status of the system, the PRI interface, and the data transfer in active sessions.

Table A-1 lists and describes each LED.

Table A-1. MAX LEDs

LED	Description
Power	This LED is on when the MAX power is on.
Fault	This LED is on in one of two cases—either a hardware self-test is in progress or there is a hardware failure. When a hardware self-test is in progress, the LED is on. If any type of hardware failure occurs, the LED flashes. If the failure is isolated to a expansion card, the MAX may continue functioning without the expansion card.
Data	This LED is on when calls are active.
Alarm	This LED is on when there is a WAN alarm or a trunk is out of service, such as during line loopback diagnostics. WAN alarms include Loss of Sync, Red Alarm, Yellow Alarm, and All Ones (or AIS).

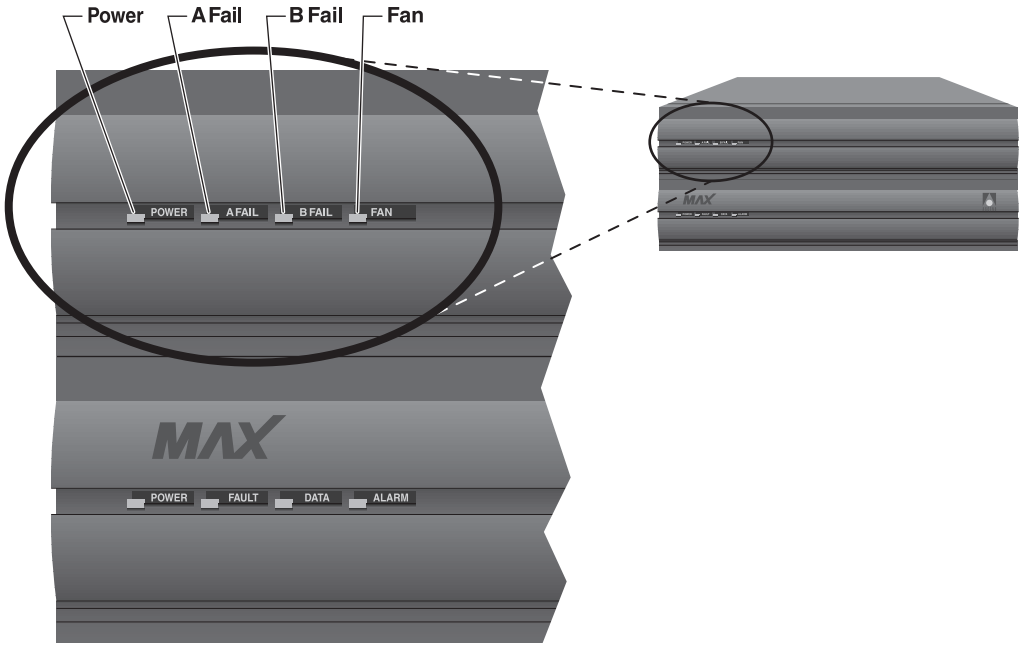


Figure A-2. Location of LEDs on the Redundant MAX

Table A-2 lists and describes each LED.

Table A-2. Redundant MAX LEDs

LED	Description
Power	This LED is on when the Redundant MAX power supply is on.
A Fail	This LED is on only when there is a failure on power supply A, (if one or more of the voltages on the A side has failed: +5, +3.3, +12, -12, -5.)
B Fail	This LED is on only when there is a failure on power supply B, (if one or more of the voltages on the B side has failed: +5, +3.3, +12, -12, -5.)
Fan	This LED is on when the fans are functioning properly (if +12 VDC from either A or B is good.) This LED is off when there is a fan failure.

MAX back panel

The MAX back panel includes the following LEDs that display the status of the Ethernet interface:

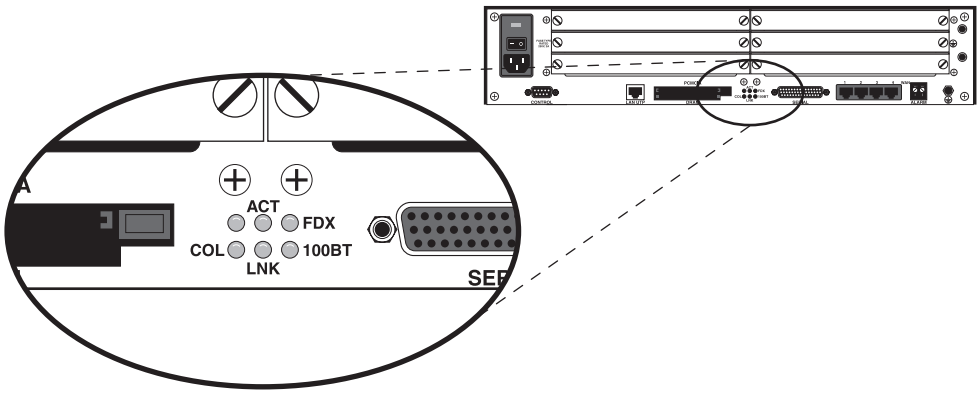


Figure A-3. Ethernet interface LEDs on MAX back panel

Note: The Classic MAX back panel shows similar LEDs on the Ethernet expansion card if one is installed. On the Classic MAX, there is one LED for each possible Ethernet interface (10BaseT, and COAX (10Base2), which are lit when the interface is in use. The ACT and COL LEDs are the same as those on the MAX 6000 (Table A-3).

The Ethernet interface LEDs are described in Table A-3.

Table A-3. Ethernet interface LEDs on back panel

LED	Description
ACT (Activity)	This LED is on when the MAX is detecting activity (network traffic) on its Ethernet interface.
COL (Collisions)	This LED is on when the MAX detects packet collisions on the Ethernet.

Table A-3. Ethernet interface LEDs on back panel (continued)

LED	Description
FDX	When this LED is on it indicates full duplex on the Ethernet.
100ST	When this LED is on, it indicates 100BT; when it is off, it indicates 10BT.
LINK (Link integrity)	This LED is on when the Ethernet interface is functional.

ISDN cause codes

ISDN cause codes are numerical diagnostic codes sent from an ISDN switch to a DTE; these codes provide an indication of why a call failed to be established or why a call terminated. The cause codes are part of the ISDN D-channel signaling communications supported by the Signaling System 7 supervisory network (WAN). When you dial a call from the MAX using ISDN access, the MAX reports the cause codes in the Message Log status menu. When the MAX clears the call, a cause code is reported even when inband signaling is in use. If the PRI or BRI switch type is 1TR6 (Germany), see Table A-5.

Table A-4 lists the numerical cause codes and provides a description of each.

Table A-4. ISDN cause codes

Code	Cause
0	Valid cause code not yet received
1	Unallocated (unassigned) number
2	No route to specified transit network (WAN)
3	No route to destination
4	Send special information tone
5	Misdialed trunk prefix
6	Channel unacceptable
7	Call awarded and being delivered in an established channel
8	Prefix 0 dialed but not allowed
9	Prefix 1 dialed but not allowed
10	Prefix 1 dialed but not required
11	More digits received than allowed, but the call is proceeding
16	Normal clearing

Table A-4. ISDN cause codes (continued)

Code	Cause
17	User busy
18	No user responding
19	No answer from user (user alerted)
21	Call rejected
22	Number changed
23	Reverse charging rejected
24	Call suspended
25	Call resumed
26	Non-selected user clearing
27	Destination out of order
28	Invalid number format (incomplete number)
29	Facility rejected
30	Response to STATUS ENQUIRY
31	Normal, unspecified
33	Circuit out of order
34	No circuit/channel available
35	Destination unattainable
37	Degraded service
38	Network (WAN) out of order
39	Transit delay range cannot be achieved
40	Throughput range cannot be achieved
41	Temporary failure
42	Switching equipment congestion
43	Access information discarded
44	Requested circuit channel not available
45	Pre-empted

Table A-4. ISDN cause codes (continued)

Code	Cause
46	Precedence call blocked
47	Resource unavailable, unspecified
49	Quality of service unavailable
50	Requested facility not subscribed
51	Reverse charging not allowed
52	Outgoing calls barred
53	Outgoing calls barred within CUG
54	Incoming calls barred
55	Incoming calls barred within CUG
56	Call waiting not subscribed
57	Bearer capability not authorized
58	Bearer capability not presently available
63	Service or option not available, unspecified
65	Bearer service not implemented
66	Channel type not implemented
67	Transit network selection not implemented
68	Message not implemented
69	Requested facility not implemented
70	Only restricted digital information bearer capability is available
79	Service or option not implemented, unspecified
81	Invalid call reference value
82	Identified channel does not exist
83	A suspended call exists, but this call identity does not
84	Call identity in use
85	No call suspended
86	Call having the requested call identity has been cleared

Table A-4. ISDN cause codes (continued)

Code	Cause
87	Called user not member of CUG
88	Incompatible destination
89	Nonexistent abbreviated address entry
90	Destination address missing, and direct call not subscribed
91	Invalid transit network selection (national use)
92	Invalid facility parameter
93	Mandatory information element is missing
95	Invalid message, unspecified
96	Mandatory information element is missing
97	Message type non-existent or not implemented
98	Message not compatible with call state or message type non-existent or not implemented
99	Information element nonexistent or not implemented
100	Invalid information element contents
101	Message not compatible with call state
102	Recovery on timer expiry
103	Parameter nonexistent or not implemented, passed on?
111	Protocol error, unspecified
127	Internetworking, unspecified

Table A-5 lists the cause codes for the 1TR6 switch type.

Table A-5. ISDN cause codes for 1TR6 switch type

1TR6 Code	Cause
1	Invalid call reference value
3	Bearer service not implemented. (Service not available in the A-exchange or at another position in the network, or no application has been made for the specified service.)
7	Call identity does not exist. (Unknown call identity)

Table A-5. ISDN cause codes for 1TR6 switch type (continued)

1TR6 Code	Cause
8	Call identity in use. (Call identity has already been assigned to a suspended link.)
10	No channel available. (No useful channel available on the subscriber access line—only local significance.)
16	Requested facility not implemented. (The specified FAC code is unknown in the A-exchange or at another point in the network.)
17	Request facility no subscribed. (Request facility rejected because the initiating or remote user does not have appropriate authorization.)
32	Outgoing calls barred. (Outgoing call not possible due to access restriction which has been installed.)
33	User access busy . (If the total made up of the number of free B-channels and the number of calling procedures without any defined B-channel is equal to four, then any new incoming calls will be cleared down from within the network. The calling party receives a DISC with cause “user access busy” (= 1st busy instance) and engaged tone.)
34	Negative CUG comparison. (Link not possible due to negative CUG comparison.)
37	Communication as semi-permanent link not permitted
48 - 50	Not used. (Link not possible, e.g. because RFNR check is negative.)
53	Destination not obtainable. (Link cannot be established in the network due to incorrect destination address, services or facilities)
56	Number changed. (Number of B-subscriber has changed.)
57	Out of order. (Remote TE not ready)
58	No user responding. (No TE has responded to the incoming SETUP or call has been interrupted, absence assumed—expiry of call timeout T3AA.)
59	User busy. (B-subscriber busy)
61	Incoming calls barred. (B-subscriber has installed restricted access against incoming link or the service which has been requested is not supported by the B-subscriber)

Table A-5. ISDN cause codes for 1TR6 switch type (continued)

1TR6 Code	Cause
62	Call rejected. (To A-subscriber: Link request actively rejected by B-subscriber —by sending a DISC in response to an incoming SETUP. To a TE during the phase in which an incoming call is being established: The call has already been accepted by another TE on the bus.)
89	Network congestion. (Bottleneck situation in the network; e.g. all-trunks-busy, no conference set free)
90	Remote user initiated. (Rejected or cleared down by remote user or exchange.)
112	Local procedure error. (In REL: Call cleared down due to local errors; e.g. invalid messages or parameters, expiry of timeout, etc. In SUS REJ: The link must not be suspended because another facility is already active. In RES REJ: No suspended call available. In FAC REJ: No further facility can be requested because one facility is already being processed, or the specified facility may not be requested in the present call status.)
113	Remote procedure error. (Call cleared down due to error at remote end.)
114	Remote user suspended. (The call has been placed on hold or suspended at the remote end.)
115	Remote user resumed. (Call at remote end is no longer on hold, suspended or in the conference status.)
127	User Info discarded locally. (The USER INFO message is rejected locally. This cause is specified in the CON message.)
35	Non existent CUG. (This CUG does not exist.)

Common problems and their solutions

This section lists problems you might encounter and describes ways to resolve them.

General problems

Calls fail between AIM ports

.The following first-level diagnostic commands can help in troubleshooting calls between AIM ports:

- For a local loopback toward an application at its AIM port interface, use the Local LB command in the Port Diag menu.

- For a loopback toward an application at its remote-end AIM interface, use the DO Beg/End Rem LB command.
- For a channel-by-channel error measurement, use the DO Beg/End BERT command.
- To resynchronize a multichannel call, use the DO Resynchronize command.

You must be in a profile or status window specific to an AIM port with a call online to use each DO command. For information on the Local LB command and on each DO command, see the *MAX Reference Guide*

DO menus do not allow most operations

When the list of DO commands appears, many operations may not be not available if the right profile is not selected. Because the MAX can manage a number of calls simultaneously, you might need to select a specific Connection profile, Port profile, or a Call profile in order to see certain DO commands. For example, to dial a Call profile or a Connection profile, you must move to the Call profile (Host/6>Port N Menu > Directory) or the Connection profile, and then type Ctrl-D 1.

Note that you cannot dial if Operations=No for the control port. If a call is already active, DO 2 (Hang Up) appears instead of DO 1 (Dial). If the T1 or E1 line is not available, Trunk Down appears in the message log and you cannot dial.

POST takes more than 30 seconds to complete

The MAX downloads 12MOD modem code, waits for the modems to checksum the downloaded code, and then verifies the checksum matches before continuing with AT POST. Previously, the MAX downloaded the modem code and immediately commence with AT POST. This feature helps to reduce the POST failure rates for the MOD12 cards.

The 12MOD digital modem slot card boots every time the MAX power-cycles, and requires boot-up configuration data from the MAX. This means the MAX makes two further attempts to download the code for the MAX unit's MOD12 digital 12-modem slot card if the first boot-up fails.

Previously, the MAX downloaded the required code and immediately commenced with `AT POST` (which sends the string `AT` to each modem and waits for the modem to respond with "OK"). Now the MAX downloads the modem code, waits for the modems to checksum the downloaded code, and then verifies that the checksum matches before continuing. If the checksum does not match, the MAX will download the code again, up to 2 more times. If the checksum still doesn't match after three download attempts, the MAX will fail the entire slot card.

Configuration problems

The most common problems result from improperly configured profiles.

The MAX cannot dial out on a T1 or E1 line

To verify that the configured profile is correctly configured:

1 Make certain that you have entered the correct phone number to dial.

2 Check that the Data Svc parameter specifies a WAN service available on your line.

   If you request a WAN service that is not available on your line, the WAN rejects your request to place a call.

3 Check whether the channels using the requested WAN service are busy.

   If these channels are busy, an outgoing call might be routed to channels for which you did not request the specified WAN service. Check the Data Svc, Call-by-Call, and PRI # Type parameter values in the profile.

4 Determine whether you have correctly set the parameters controlling Dynamic Bandwidth Allocation.

   For detailed information, see Chapter 2, "Configuring the MAX for WAN Access," and Chapter 3, "Configuring WAN Links."

Some channels do not connect

You may encounter a problem where the Line Status menu shows that the MAX is calling multiple channels simultaneously, but only some of the channels connect.

An international MAX placed the call or the call was from the U.S. to another country. In some countries, setting the Parallel Dial parameter in the System profile above 1 or 2 violates certain dialing rules, and only some of the channels can connect during call setup. Try reducing the Parallel Dial parameter to the value 2. If the problem persists, try reducing it to 1.

Data is corrupted on some international calls

You may notice that the data appears to be corrupted on single- or multichannel calls dialed in the U.S. to another country. On some international calls, the data service per channel is not conveyed by the WAN to the MAX answering the call. You must therefore set Force 56=Yes in the Call profile. If you do not, the MAX incorrectly thinks that the call uses 64-kbps channels.

Only the base channel connects

You may encounter a problem where the first channel of an inverse multiplexing or MP+ call connects, but then the call clears or does not connect on the remaining channels.

The most common error in defining Line profiles is specifying incorrect phone numbers. The MAX cannot successfully build inverse multiplexing or MP+ calls if the phone numbers in the Line profile of the called unit are incorrect. The phone numbers that you specify in the Line profile are the numbers local to your unit. Do not enter the phone numbers of the MAX you are calling in the Line profile. The numbers you are calling belong in the Call profile, Destination profile, or Connection profile.

In addition, when you are using E1 or T1 lines, any phone numbers you specify must correspond to those channels within the circuit that are available for data transmission. For example, if channels 13-21 are allocated to a particular slot, you must specify the phone numbers for channels 13-21 in the Line profile. Switched data channels do not have to be contiguous within the circuit.

No Channel Avail error message

When the MAX tries to place a call, if the error message No Channel Avail appears in the Message Log display, check the Line profile configuration. This message can also indicate that the lines' cables have been disconnected or were installed incorrectly.

Restored configuration has incorrect RADIUS parameters

The RADIUS Server submenu used to consist of 3 clients (specific host addresses) and 1 Server Key for all 3 clients. If the MAX supports the new RADIUS Server, the restoration of the MAX configuration will cause a problem because the new RADIUS Server allows up to 9 addresses (host or net) and a Server Key for each address. When you restore configurations with the old Client Address list, the netmask assigned to the clients will be the default netmask of the address type given (for example, 128.50.1.1 will get a netmask of 16) and not the previous 32-bit (single host) address. In addition, the Server Key will not automatically be set. You must set the Server Key manually for each client in the RADIUS Server submenu.

Hardware configuration problems

If you cannot communicate with the MAX through the vt100 control terminal, you might have a terminal configuration, control port cable, or MAX hardware problem.

Cannot access the vt100

If no data is displayed on the vt100, verify that the unit completes all of the power-on self tests successfully by following these steps:

1 Verify that the MAX and your terminal are set at the same speed.

2 Locate the LED labeled FAULT.

3 Switch on the MAX.

The FAULT LED should remain off except during the power-on self tests. If you are using the vt100 interface, type Ctrl-L to refresh the screen.

If the FAULT LED remains on longer than a minute, there is a MAX hardware failure. A blinking FAULT LED also indicates a hardware failure. Should these situations arise, contact Ascend Customer Support.

FAULT LED is off but no menus are displayed

If the unit passed its power-on self tests and you still cannot communicate with the vt100 interface, type Ctrl-L to refresh the screen. If you still do not see any data, check the cabling between the MAX and your terminal as follows:

1 Check the pin-out carefully on the 9-pin cable.

The control terminal plugs into the HHT-vt100 cable or 9-pin connector labeled Control on the back of the MAX. If you are connecting to an IBM PC-like 9-pin serial connector, a straight-through cable is appropriate. Otherwise, you might need a 9-to-25 pin conversion cable.

2 Check the flow control settings on your vt100 terminal.

If you are not communicating at all with the MAX, see whether you can establish communications after you have turned off all transmit and receive flow control at your terminal or terminal emulator.

3 Determine whether you need a null-modem cable converter.

In general, these are not required for communications to the MAX. However, so many different cable and terminal configurations are available that occasionally a null-modem cable converter might be required.

Random characters appear in the vt100 interface

If random or illegible characters appear on your display, there is probably a communications settings problem. You must make these settings:

- 9600 bits per second data rate
- 8 data bits
- 1 stop bit
- No flow control
- No parity

If you have changed the data rate through the Port profile, make certain that your vt100 terminal matches that rate.

A power-on self test fails

If the start-up display indicates a failure in any of its tests, an internal hardware failure has occurred with the unit. In this case, contact Ascend Customer Support.

AIM port interface problems

There are two ways to test the AIM port interface:

- A local loopback test
- Through true end-to-end communications

Many codecs or other AIM devices support some knowledge of loopback. For example, when the MAX is in loopback mode and is connected to a codec, users see their own images through the codec. Likewise, most bridge/router devices recognize and report a diagnostic message when a packet is sent out and received by the same module. More often than not, the codec must be configured explicitly to accept the loopback from the communications device.

Local loopback testing is the best aid when troubleshooting the AIM port interface—the interface between the codec and the MAX. All of the symptoms and operations described in this section assume you are working from the local loopback diagnostics menu. Unless otherwise specified, the AIM port interfaces in this section can include the Ascend Remote Port Modules (RPMs).

The first and most critical aspect of the AIM port interface is the cable or cables connecting the codec to the MAX. If you are unsure about the cabling required, contact Ascend Customer Support.

The MAX reports data errors on all calls

This problem can indicate that you have installed faulty host interface cables or cables not suited to the application. Information on host interface cabling requirements is found in *MAX Getting Started*

Calls cannot be made, answered, or cleared using control leads

If you have purchased or built your own cables, verify the pin-out against the MAX pin-out for compatibility. *MAX Getting Started* lists the host interface pin-outs.

Frequently, a DB-25 breakout box is useful for monitoring control leads and for making quick changes to the cabling. However, because the host interface is running V.35 or RS-422 signal levels, you must verify that the breakout box is passive; that is, you must verify that the breakout box is not regenerating RS-232 level signals.

The codec indicates that there is no connection

The codec expects one or more of its control lines to be active. If no lines are active, toggle the various outputs available on the local loopback diagnostics menu. If there is still no connection, verify that you have installed the host cables correctly as described in *MAX Getting Started.* If the cabling is installed correctly, examine the host interface cable pin-outs as described in *MAX Getting Started*.

The codec does not receive data

To resolve this problem:

1. Verify that the codec is configured to accept a loopback at the communications device. Frequently, a codec requires certain control lines to be active during data transfer. Therefore, you might want to toggle the various host interface output lines, especially DSR and CD, to ensure that they are active.
2. If there is still no data transfer, your cable might not provide one or more control lines required by the host; refer to the documentation of your equipment for a description of what pins it requires to be active. These control lines are generally the most important ones:
   - Carrier Detect (CD)
   - Clear To Send (CTS)
   - Data Set Ready (DSR)
3. If you are convinced that the control lines are in their correct states, but there is still no data transfer, you might have a clocking problem. The MAX provides both the transmit data clocks and the receive data clocks to your equipment through the host interface.The codec must be configured to accept the clocks from the MAX.
4. Check your cable length.
   If the cable length exceeds the recommended distances, you should be using terminal timing. Alternately, you might need to install RPMs.
5. Check the data rate.
   You can adjust the data rate from the local loopback diagnostics menu by choosing the number of channels. Some applications cannot work above or below a certain data rate;

for example, some high performance codecs cannot operate at data rates less than 384 kbps. In such cases, adjust the number of channels of data being looped back.

The codec cannot establish a call when DTR is active

You may notice that the Port profile is set to establish calls when DTR is active, but the codec cannot establish a call. If the codec is going to originate the calls directly by using control-lead dialing, the call origination and clearing mechanisms must be configured for compatibility between the MAX and the codec. To verify a compatible configuration from the local loopback diagnostics menu:

1 Disable each of the MAX output control lines except DSR.

To disable an output control line, toggle it to be Inactive (-). At this time, the codec should indicate that there is no connection.

2 Request an outgoing call from your equipment and monitor the Port Leads status menu of the ports active in the call.

One or more of the control line inputs should go active and remain active for some period of time. If the DTR input is not one of the leads that changes state, your cable is not properly configured. In this case, you must change the cable to route the appropriate host output signal to the DTR input of the MAX. The MAX must use the DTR lead to establish outgoing calls.

3 Once you have made any changes required to verify that the DTR lead becomes active when the MAX requests the call, configure the Port profile to expect the DTR input.

In the Port profile, set the Dial Call = DTR Active.

Calls initiated by control-lead toggling are cleared too soon

You may encounter a problem where the MAX clears a call initiated by control-lead toggling before it completely establishes the call. If the call is cleared almost immediately, the Port profile most likely has a configuration error. To find the source of the problem:

1 Place an outgoing call from the codec while monitoring the Port Leads status menu of the AIM ports used in the call.

2 Watch the DTR input carefully while the MAX is establishing the call.

If the DTR input indicates Active (+) and then shortly thereafter returns to Inactive (-), the MAX is using DTR as a pulse to place the call. Make sure that the Clear parameter in the Port profile does not have the value DTR Inactive. (DTR Inactive should be selected for Clear only when the application maintains DTR positive during the call.)

3 While your equipment is still dialing the call, toggle the value of the CD output to indicate to your equipment that the call completed. At this time, watch the control leads very carefully. Make certain that any control leads that toggle while the call is being established are not used in the Clear parameter to clear the call. This type of configuration error is the most likely cause of a call being cleared almost immediately.

The codec cannot clear a call

You may encounter a problem where a codec-initiated call cannot be cleared. If the call cannot be cleared from the codec, the Port profile most likely has a configuration error. To verify the source of the problem:

1 Place an outgoing call from your equipment while monitoring the Port Leads status menu of the AIM ports used in the call.

2 Toggle the CD output to Active (+) once the host has requested the outgoing call. The codec should recognize that the call is online.

3 Make a request to clear the call from the codec.

4 Watch the control leads very carefully as one or more of the input control lines toggle. Generally, either DTR or RTS is the line that toggles. Record whether the control lead input goes to Active (+) or Inactive (-) when the call is cleared; then, check that the value of the Clear parameter in the Port profile matches the action that the codec takes when the call is cleared.

ISDN PRI and BRI interface problems

Calls are not dialed or answered reliably

To resolve this problem:

1 Check your cabling.

The first and most critical aspect of the interface is the physical cable connecting the MAX to the line or terminating equipment. Typically, WAN interface cabling problems appear immediately after installation. If you are unsure about the cabling required, contact Ascend Customer Support. *MAX Getting Started* describes the general PRI and BRI interface requirements, and lists cabling pin-outs.

2 If the cabling is not the problem and the MAX is a T1 unit, check that the value of the Buildout parameter or the Length parameter in the Line profile matches the actual distance in your configuration.

- The MAX displays the Buildout parameter if its interface to the T1 line is equipped with an internal CSU. Its enumerated values can be 0 db, 7.5 db, 15 db, and 22.5 db. Contact your carrier representative to determine which value to choose.
- If the line interface is not equipped with an internal CSU, the Length parameter is displayed. Its value can be 1-133, 134-266, 267-399, 400-533, or 534-655 feet, which should correspond to the distance between the MAX and the WAN interface equipment, typically a CSU or multiplexer.

Note: T1 PRI ports not equipped with internal CSUs require an external CSU or other equipment approved for the metallic interface between the MAX and the WAN facility.

The Net/BRI lines do not dial or answer calls

Do not connect the MAX unit's Net/BRI ports directly to U-interface BRI lines. The MAX unit's Net/BRI ports require carrier-approved NT1 (network terminating 1) equipment between the MAX and BRI lines. Note that Net/BRI outbound calls require the use of trunk groups.

No Logical Link status

You may notice that the status of a Net/BRI line in the Line Status display is No Logical Link.

In some countries outside the U.S., it is common for no logical link to exist before the MAX places a call. In the U.S., when you first plug a line into the MAX or switch power on, the central office switch can take as long as 15 minutes to recognize that the line is now available. You might have to wait that long for the line state to change to Active (A). The physical link can exist without a logical link up on the line.

If you wait longer than 15 minutes and the line is still not available:

1. Check whether all the ISDN telephone cables are wired straight through.

   If you are running multipoint (passive bus) on your switch, all of the ISDN telephone cables must be wired straight through. If any of the cables are wired to cross over, you will not be able to place calls.

2. Check that 100% termination is provided on each ISDN line.

3. Check whether you have correctly specified the SPIDs (Service profile Identifiers) in the Line profile for each line. If the SPIDs are not correctly specified, the line status might indicate No Logical Link. Check with your system manager or carrier representative to obtain the SPID or SPIDs for your line. You specify your SPIDs using the Pri SPID and Sec SPID parameters in the Line profile.

WAN calling errors occur in outbound Net/BRI calls

You may encounter a problem where the Call Status window immediately indicates a WAN calling error when the MAX places a call on a Net/BRI module. To resolve the problem:

1. Check the value of the Data Svc parameter in the Call or Connection profile.

   Try both the 64K and 56K options for Data Svc to see whether using a different value solves the problem.

2. Check whether you are using the correct dialing plan.

   Depending on how the BRI lines are configured, you might need to type four, seven, or ten digits to communicate with the remote end.

   Four-digit dialing involves the last four digits of your phone number. For example, if your phone number is (415) 555-9015, four-digit dialing requires that you type only the last four digits—9015. Seven-digit dialing specifies that you dial the digits 5559015, and ten-digit dialing requires 4155559015.

   If you are sending the incorrect number of digits, the MAX cannot route the call. Ask your carrier representative for the correct dialing plan, or simply try all of the possibilities.

3. Verify explicitly with your carrier representative that the line is capable of supporting the call types you are requesting.

ISDN PRI and BRI circuit-quality problems

Excessive data errors on calls to AIM ports

You may encounter a problem where the MAX reports excessive data errors on some calls to AIM ports. The MAX provides a BERT (byte error test) that counts data errors that occur on each channel during a call to a AIM port. The BERT checks the data integrity from the MAX at one end of the call to the MAX at the other end.

If you have verified that the MAX is correctly installed and configured, and you have previously placed calls without excessive errors, run the BERT using the command DO Beg/End BERT. Do not clear the call before running the BERT. You can run a BERT only under these conditions:

- A call is active.
- The Call Type parameter is set to AIM, FT1-B&O, or FT1-AIM.
- The Call Mgm parameter is set to Manual, Dynamic, or Delta.

You can also configure the Auto BERT parameter in the Call profile to run an automatic BERT. If the BERT indicates very high errors on some of the channels, clear the call and redial. When redialed, the call might take a different path, correcting the excessive error problem.

Excessive handshaking on calls to AIM ports

Handshaking is a normal and momentary occurrence during call setup and when the MAX increases or decreases bandwidth. If there is trouble in the circuits that carry the call, frequent handshaking can occur. If the trouble is serious enough to degrade the quality of the call, the MAX disconnects. If handshaking is continuous for over a minute, the problem is probably not due to the quality of the line, and you should call Ascend Customer Support.

Inbound data is scrambled during an AIM Static call

Because an AIM Static call does not have a management channel, it is possible for data scrambling to occur because of WAN slips, a type of timing error. Slips are a very infrequent occurrence. If you encounter such problems, clear the call and redial.

Problems indicated in LEDs

LEDs are not lit for the secondary E1 or T1 line

If no LEDs relating to the secondary line are lit, the line is disabled in the Line profile. You can enable the secondary line by modifying the Line profile.

The E1 or T1 line is in a Red Alarm state

If the ALARM LED and the Line Status menu indicate that the line is in a Red Alarm state, the MAX cannot establish proper synchronization and frame alignment with the WAN. This behavior is normal for as long as 30 seconds when an PRI line is first plugged into the MAX.

If the Red Alarm condition persists for longer than 30 seconds:

1 Check the value of the Framing Mode parameter in the Line profile.

Change the value to the other available option and check to see whether the Red Alarm condition goes away within 30 seconds.

2 If the Red Alarm state still persists, check the cabling.

You might have a crossover cable installed when a straight-through cable is required, or vice versa. If the MAX is connected through bantam plugs, reverse the transmit and receive plugs. Then, allow the MAX to attempt to establish synchronization for an additional 30 seconds.

3 You can eliminate the cabling as a possible cause by replacing the connection with a loopback plug. The LS LED should go off immediately, followed by the RA LED in about 30 seconds.

A PRI line is in use and the ALARM LED blinks

A blinking ALARM LED means that the physical configuration of the E1 or T1 line is correct, but that the D channel is not communicating with the WAN. To resolve this problem:

1 Verify with your carrier representative that the D channel is channel 16 (E1) or 24 (T1).

2 If the D channel number is correct, check the value of the Line Encoding parameter in the Line profile. When B8ZS encoding is in use, a non-inverted D channel is established. If AMI encoding is selected, an inverted D channel is established. Check the line translations provided by your carrier representative and set the line encoding to match the inversion requirements.

3 Determine whether your WAN interface or the MAX T1 unit is equipped with a CSU.

If the WAN interface or the MAX is not equipped with a CSU, the ALARM LED blinks. Check whether you have specified the proper Length or Buildout value in the Line profile.

4 Check whether the D channel is in service.

If no equipment has been plugged into the line for a short period of time (five to ten minutes), the D channel is taken out of service. You might need to contact your carrier to put the D channel back into service.

Problems accessing the WAN

Only some channels are dialed for AIM or BONDING calls

You may encounter a problem where whenever the MAX makes an AIM or BONDING call, it dials only some of the channels. To resolve this problem:

1 Verify that there are enough channels enabled for switched services in the Line profile to meet the requirements of the Parallel Dial parameter in the System profile.

Most WAN providers can place a limited number of calls simultaneously from a single E1 or T1 line. If more concurrent attempts are made than the WAN can support, the WAN applies a congestion tone—a fast busy signal.

2 Try adding bandwidth once the call is up.

If you can add bandwidth, the solution is to adjust the Parallel Dial parameter in the System profile. A value of 5 works for almost all WAN providers, while some support substantially more. If adding bandwidth does not work, the problem is most likely within the individual channel translations. In this case, call your carrier representative.

The MAX never uses some channels

To resolve this problem:

1 If you are making AIM or BONDING calls, verify that the affected channels are enabled for switched services in the Line profile.

2 If you have an E1 unit, check whether it has been connected recently to a device that does not support the full 31 channels. If so, the switch might take the unused channels out of service. This situation can arise on either the local or the remote end.

3 If you have a T1 unit, check whether it has been connected recently to a device that does not support the full 23 channels. If so, the switch might take the unused channels out of service. This situation can arise on either the local or the remote end.

4 Check whether the channels enabled in your Line profile correspond to the channels enabled in the circuit. If only some of the channels in the circuit are available for data calls, you must specifically enable those channels in your Line profile.

5 If you place a call and some channels are always skipped, call your carrier representative.

An outgoing call using fails to connect to the remote end

If the T1 or E1 line is configured for inband singaling and outbound calls fail to connect:

1. Make sure that your Line profile is properly configured for wink-start or idle-start.

   The Rob Ctl parameter in the Line profile determines which of these call-control mechanisms the MAX uses. Check with your carrier representative to find out which inband signaling your line supports.

2. If the Line profile is configured correctly and you still cannot place an outgoing call, check the service state of the line.

   Frequently, if a T1 or E1 line has been unplugged for an extended duration, the switched services available on the line are taken out of service. Once you install the MAX, you might need to call your carrier representative to have the line reactivated. If this is the case, leave the MAX on all the time, even when you are not using it; otherwise, you will have to call your carrier to reactivate the line each time the unit is switched off and on.

3. Ask your carrier representative whether the line is configured for DTMF dialing; the line must support this type of dialing in order to recognize digits being dialed.

Incoming call routing problems

Routing problems occur when a call is connected to the answering MAX but cannot be routed to one of its slots.

Call status drops back to IDLE

You may see a condition where after the Call Status window reports ANSWERING and HANDSHAKING, it drops back to IDLE. This condition might not indicate a problem. It can indicate that the call was initially answered and that when its routing was checked, the target AIM port was busy or disabled. Handshaking does not occur on calls to the MAX unit's internal router, but calls can initially be answered and then quickly cleared during normal operation, such as during the receipt of an incorrect password.

Dual-port call status drops back to IDLE

If when trying to make a dual-port call, the Call Status menu reports ANSWERING and HANDSHAKING, and then drops back to IDLE, check the status of both ports specified in the Dual Ports, Port 1/2 Dual, Port 3/4 Dual, or Port 5/6 Dual parameter of the answering MAX. If either port in the pair is busy, the call cannot be routed to that pair.

AIM or BONDING call status drops back to IDLE

If when trying to make an AIM or BONDING call, the Call Status window reports ANSWERING and HANDSHAKING, and then drops back to IDLE, check that the routing parameters are configured correctly. If the routing parameters are configured incorrectly, an AIM, BONDING, or AIM/DBA call might be routed to ports that cannot support these types of calls.

Bridge/router problems

The link is of uncertain quality

When running FTP (File Transfer Protocol), the data transfer rate appears in bytes per second. Multiply this rate times 8 to get the bits per second. For example, suppose that you are connected to Detroit on a 56-kbps B channel and that FTP indicates a 5.8 kbyte/s data rate; in this case, the link is running at 5.8x8=46.8 kbps, or approximately 83% efficiency. Many factors can affect efficiency, including the load on the FTP server, the round-trip delay, the overall traffic between endpoints, and the link quality.

You can check link quality in the WAN Stat status window, or by running a ping between the same endpoints. Dropped packets hurt the link's efficiency, as does round-trip delay. Random round-trip delay indicates heavy traffic, a condition that also drops the efficiency of the link.

The MAX hangs up after answering an IP call

To resolve this problem:

1. If you are running PPP, check that you have entered the proper passwords.
2. Check that Auth is set to PAP or CHAP.
3. If you are routing IP over PPP, check that the calling device gives its IP address
   Some calling devices supply their names, but not their IP addresses. However, you can derive an IP address if the calling device is listed in a local Connection profile or on a RADIUS authentication server. Try enabling PAP or CHAP for the Recv Auth parameter so that the MAX matches the caller's name to the Station parameter in a Connection profile and gets the corresponding LAN Adrs.

Upgrading System Software

B

Caution: You must use the new software loading procedure explained in ”Upgrading system software” to load this version of software onto your system. Read the instructions carefully before upgrading your system.

If you are upgrading your software using TFTP, you must use the `fsave` command immediately after executing the `tload` command. Failure to do so may cause your Ascend unit to lose its configuration.

Each incremental release contains new features and corrections. To use this release note:

1. Read through the table of contents to determine which software release and (new features) apply to your environment.
2. Obtain the file from Ascend anonymous FTP server (ftp.ascend.com). If you need Technical Assistance, contact Ascend in one of the following ways:

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

3. Upgrade to the new software by following the instructions in the next section, “Upgrading system software.” Then configure the features that apply to your site.

Upgrading system software

Caution: The procedure for uploading new software to Ascend units have changed significantly. Carefully read the new software loading procedures explained in this section before upgrading your system.

This section explains how to upgrade your system software. It contains the following sections:

- Definitions and terms
- Guidelines for upgrading system software
- Before you begin
- Upgrading system software
- Using TFTP to upgrade to a fat or thin load
- Upgrading software with an extended load
- Upgrading software from versions earlier than 4.6C to version 5.0A or above
- Using the serial port to upgrade to a standard or a thin load
- System messages

Definitions and terms

This document uses the following terms:

Build	The name of the software binary. For example, `ti.m40` is the MAX 4000 T1 IP-only software build. For the names of all the software builds and the features they provide see `/pub/Software-Releases/Max/SW-Filenames-Max.txt` or `/pub/Software-Releases/Pipeline/SW-Filenames-Pipeline.txt` on the Ascend FTP server. If possible, you should stay with the same build when upgrading. Loading a different build can cause your Ascend unit to lose its configuration. If this happens, you must restore your configuration from a backup.
Standard load	Software versions 4.6Ci18 or earlier and all 4.6Cp releases. You can load these versions of software through the serial port or by using TFTP. TFTP is the recommended upgrade method for standard loads.
Fat load	4.6Ci19 to 5.0Aix and all 5.0Ap releases with a file size greater than 960 KB (for MAX units) or 450K (for Pipeline units). Before upgrading to a fat load for the first time, you must upgrade to a thin load. You must use TFTP to upgrade to fat loads.
Thin load	4.6Ci19 to 5.0Aix and all 5.0Ap releases with a file size less than 960 KB (for MAX units) or 450 KB (for Pipeline units). TFTP is the recommended upgrade method for thin loads.

Restricted load	6.0.0 or later release denoted by an "r" preceding the build name. For example, `rti.m40` is the restricted load for the MAX 4000 T1 IP-only software build A restricted load is not meant for production environments. It is a special load that is required to upgrade to an extended load. Before upgrading to an extended load for the first time, you must upgrade to a restricted load. You must use TFTP to upgrade to restricted loads.
Extended load	6.0.0 or later release. You must use TFTP to upgrade to extended loads.

Guidelines for upgrading system software

Caution: Before upgrading, consider the following very important guidelines:

- Use TFTP to upgrade if possible. TFTP is more reliable and saves the Ascend unit configuration when you upgrade.
- You cannot load or a fat load, a restricted load, or an extended load through the serial port. You must use TFTP.
- If you are using TFTP to upgrade your software, use the `fsave` command immediately after executing the `tload` command. Failure to do so might cause your Ascend unit to lose its configuration.
- If possible, you should always stay with the same build of software when you upgrade. If you load a different version, your Ascend unit may lose its configuration. If this happens, you must restore your configuration from a backup.
- If you are upgrading to a software version 5.0A or 5.0Aix fat load for the first time, you must be on a load that supports the fat load format. All versions of software 5.0A or above support fat loads. You should perform the upgrade in two steps:
  - Upgrade to a thin load of the same build
  - Upgrade to the fat load
- If you are upgrading to a software version 6.0.0 or above, you must be on a load that supports the extended load format. All versions of software 6.0.0 or above support extended loads. You should perform the upgrade in two steps:
  - Upgrade to a restricted load of the same build
  - Upgrade to the extended load
- You can upgrade to a thin load or a restricted load from any version of software.
- If you are upgrading from software version 4.6C or earlier to software version 5.0A or later, see "Upgrading software from versions earlier than 4.6C to version 5.0A or above" on page B-10 for important information before you start.

Table B-1 explains where to find the information you need to upgrade your unit.

Table B-1. Ascend system software versions

Version you are upgrading to	Use the instructions in...
Standard load (4.6Ci18 or earlier and all 4.6Cp releases)	"Upgrading system software" on page B-5.
Fat or thin load (4.6Ci19 to 5.0Aix and all 5.0Ap releases)	"Using TFTP to upgrade to a fat or thin load" on page B-6.
Extended load (6.0.0 or later)	A restricted load is not meant for production environments. It is a special load that is required to upgrade to an extended load. "Upgrading software with an extended load" on page B-9.

Before you begin

Make sure you perform all the tasks explained in Table B-2 before upgrading your software.

Table B-2. Before upgrading

Task	Description
If necessary, activate a Security Profile that allows for field upgrade.	If you are not sure how, see the section about Security Profiles in your documentation.
Record all of the passwords you want to retain, and save your Ascend unit's current configuration to your computer's hard disk.	For security reasons, passwords are not written to configuration files created through the serial console. A configuration file created using the Tsave command, however, *does* contain the system passwords. You can restore the Tsave configuration file using the serial console. If you chose to save your configuration using the serial console, you will have to restore your passwords manually. Restoring passwords is explained in "Using the serial port to upgrade to a standard or a thin load" on page B-11.

Table B-2. Before upgrading (continued)

Task	Description
Obtain the correct file, either by downloading it from the FTP server or by requesting it from Ascend technical support.	To ensure that you load the correct software binary, you should check the load currently installed on your unit. To do so: **1** Tab over to the System status window. **2** Press Enter to open the Sys Options menu. **3** Using the Down-Arrow key (or Ctrl- N), scroll down until you see a line similar to the following: `Load: tb.m40` **4** When upgrading, obtain the file with same name from the Ascend FTP site. If your unit does not display the current load or you are unsure about which load to use, contact technical support.
If you are upgrading to a fat load or an extended load for the first time, you must also obtain a thin load or a restricted load of the same build.	For example, if you are upgrading a MAX 4000 to 5.0Ai13 fat load (such as `tbim.m40`), obtain a thin load of the same build (such as 5.0A `tbim.m40`). If you are upgrading to a 6.0.0 extended load, obtain a 6.0.0 restricted load. Restricted loads are designated with an "r" in the load name. (For example `rtbam.m40` is a restricted load). Newer Pipeline 50 or 75 units do not have fat or extended loads. Refer to the README file in `/pub/Software-Releases/Pipeline/software-version` to determine if you have a new Pipeline 50 or 75 unit.
If you are using TFTP, make sure you load the correct binaries into the TFTP home directory on the TFTP server.	You must use TFTP to upgrade to a fat load or an extended load.
If you are using the serial port, make sure you have a reliable terminal emulation program, such as Procomm Plus.	If you use the serial port, you can only upgrade to a standard or a thin load. Upgrading through the serial port is not recommended. If you use a Windows-based terminal emulator such as Windows Terminal or HyperTerminal, disable any screen savers or other programs or applications that could interrupt the file transfer. Failure to do so might cause the software upload to halt, and can render the Ascend unit unusable.

Upgrading system software

To upgrade system software with a standard load you can use either the serial port or TFTP. TFTP is the recommended method because it preserves your Ascend unit's configuration. If you want to use the serial port to upgrade, see "Using the serial port to upgrade to a standard or a thin load" on page B-11.

Using TFTP to upgrade to a standard load

To upgrade to a standard load using TFTP, you only have to enter a few commands. But you must enter them in the correct sequence, or you could lose the Ascend unit's configuration.

To upgrade to a standard load via TFTP:

1. Obtain the software version you want to upgrade to and place it in the TFTP server home directory.
2. From the Ascend unit's VT100 interface, access the diagnostics monitor by typing the following characters in rapid succession:

   `Esc [ Esc =`

   Or, press Ctrl-D to invoke the DO menu and select D=Diagnostics.
3. At the > prompt, use the Tsave command to save your configuration as in the following example:

   `> tsave tftp-server router1.cfg`

   This saves the configuration of your unit to the file named `router1.cfg` in the TFTP home directory of the server named `tftp-server`. This file must already exist and be writable. Normally, TFTP upgrades save the configuration. Tsave is a precaution.

Caution: The file you save with the Tsave command contains all the passwords in clear text. You should move this file from the TFTP directory to a secure location after the upgrade procedure is complete.

4. Enter the following command:

   `tloadcode` ***hostname filename***

   where *hostname* is the name or IP address of your TFTP server, and *filename* is the name of the system software on the server (relative to the TFTP home directory).

   For example, the command:

   `tloadcode tftp-server t.m40`

   loads `t.m40` into flash from the machine named `tftp-server`.

Caution: You must use the Fsave command immediately after executing the Tload command. Failure to do so can cause your Ascend unit to lose its configuration.

5. Enter the following command to save your configuration to flash memory:

   `fsave`
6. Enter the following command:

   `nvramclear`

   After the Ascend unit clears NVRAM memory, it automatically resets.

This completes the upgrade.

Using TFTP to upgrade to a fat or thin load

Upgrading to a fat or thin load is not difficult, but you must be careful to follow the correct sequence of tasks.

Caution: If you are upgrading from software version 4.6C or earlier, see "Upgrading software from versions earlier than 4.6C to version 5.0A or above" on page B-10 for important information before upgrading.

To upgrade your system:

1 Obtain the software version binary you want to upgrade to and place it in the TFTP server home directory. If you are upgrading to a fat load for the first time, also obtain a thin load of the same build and place it in the same directory.

Caution: If possible, you should stay with the same build when upgrading. Loading a different build can cause your Ascend unit to lose its configuration. If this happens, you must restore your configuration from a backup.

For example, if you are upgrading a MAX 4000 to 5.0Ai13 fat load (such as `tbim.m40`), obtain a thin load of the same build (such as 5.0A `tbim.m40`).

Note: Newer Pipeline 50 or 75 units do not have fat or thin loads, you only need to load a single software binary. Refer to the README file in `/pub/Software-Releases/Pipeline/`*`software-version`* on the Ascend FTP site to determine if you have a new Pipeline 50 or 75 unit.

2 From the Ascend unit's VT100 interface, access the diagnostics monitor by typing the following characters in rapid succession:

```
Esc [ Esc =
```

Or, press Ctrl-D to invoke the DO menu and select D=Diagnostics.

3 At the > prompt, use the Tsave command to save your configuration, as in the following example:

```
> tsave tftp-server router1.cfg
```

This saves the configuration of your unit to the file named `router1.cfg` in the TFTP home directory of the server named `tftp-server`. This file must already exist and be writable. Normally, TFTP upgrades save the configuration. Tsave is a precaution.

Caution: The file you save with the Tsave command contains all the passwords in clear text. You should move this file from the TFTP directory to a secure location after the upgrade procedure is complete.

4 At the > prompt, enter:

`tloadcode` ***hostname filename***

where *hostname* is the name or IP address of your TFTP server, and *filename* is the name of the system software on the server (relative to the TFTP home directory).

Caution: If you are upgrading from a standard load to a fat load, make sure you load a thin load first.

For example, the command:

```
tloadcode tftp-server t.m40
```

loads `t.m40` into flash from the machine named `tftp-server`.

Caution: You must use the Fsave command immediately after executing the Tload command. Failure to do so may cause your Ascend unit to lose its configuration.

5 Enter the following command to save your configuration to flash memory:

```
fsave
```

6 Enter the following command:

```
nvramclear
```

After the Ascend unit clears NVRAM memory, it automatically resets.

7 If you are upgrading to a thin load, you are done. If you are upgrading to a fat load, repeat the procedure, this time uploading the fat load binary.

After a successful upgrade, one of the following messages appears.

- If the load is thin:

```
UART initialized
thin load: inflate
.....................................................
starting system...
```

- If the load is fat:

```
UART initialized
fat load: inflate
.....................................................
starting system...
```

This completes the upgrade if you have no errors. If the upgrade is not successful, refer to ”Recovering from a failed fat load upgrade” next.

Recovering from a failed fat load upgrade

If a fat load has a CRC (cyclic redundancy check) error, the following message appears:

```
UART initialized
fat load: bad CRC!!
forcing serial download at 57600 bps
please download a "thin" system...
```

Immediately after this message appears, the serial console speed is switched to 57600 bps, and the Ascend unit initiates an Xmodem serial download. To recover from this error and load the fat system, you must first load a thin system that is fat-load aware. Proceed as follows:

1 Activate your Xmodem software.

2 After you have finished loading the fat-aware thin load, reboot the unit.

3 Use the Tload command to download the fat load.

When you download a fat load, messages similar to the following appear on the diagnostics monitor screen:

```
> tload 192.168.1.82 tbam.m40
saving config to flash
.....................................
loading code from 192.168.1.82:69
file tbam.m40..
fat load part 1:
.............................................................
```

```
......
fat load part 2:
................................................
```

The "fat load part *n*:" messages notify you when the first and second halves of the download begin.

Upgrading software with an extended load

Your first upgrade to an extended load requires a preliminary procedure. You must first upgrade to a restricted load. Restricted loads are not meant to be used in a working unit. They are a temporary load that are only used to prepare your Ascend unit for the extended load.

Caution: If you are upgrading from software version 4.6C or earlier, see "Upgrading software from versions earlier than 4.6C to version 5.0A or above" on page B-10 for important information before upgrading.

To upgrade your system:

1. Obtain the software-version binary you want to upgrade to and place it in the TFTP server home directory.
2. If this is the first time you have upgraded to an extended load, obtain a restricted load of the same build and place it in the directory.

   For example, if you are upgrading a MAX 4000 to an extended load (such as `tbam.m40`), obtain a MAX 4000 restricted load (such as `rtbam.m40`).

   Note: Newer Pipeline 50 or 75 units do not have restricted loads, you only need to load a single software binary. Refer to the README file in `/pub/Software-Releases/Pipeline/`*`software-version`* on the Ascend FTP site to determine if you have a new Pipeline 50 or 75 unit.
3. From the Ascend unit's VT100 interface, access the diagnostics monitor by typing the following characters in rapid succession:

   `Esc [ Esc =`

   Or, press Ctrl-D to invoke the DO menu, and select D=Diagnostics.
4. At the > prompt, use the Tsave command to save your configuration, as in the following example:

   `> tsave tftp-server router1.cfg`

   This saves the configuration of your unit to the file named `router1.cfg` in the TFTP home directory of the server named `tftp-server`. This file must already exist and be writable. Normally, TFTP upgrades save the configuration. Tsave is a precaution.

Caution: The file you save with the Tsave command contains all the passwords in clear text. You should move this file from the TFTP directory to a secure location after the upgrade procedure is complete.

5. At the > prompt, enter:

   `tloadcode` ***hostname filename***

   where *hostname* is the name or IP address of your TFTP server, and *filename* is the name of the system software on the server (relative to the TFTP home directory).

Caution: If you want to upgrade your system for the first time to a software version 6.0.0 or later, you must first upgrade your system to a restricted load. Failure to do so can cause your Ascend unit to lose its configuration.

For example, the command:

```
tloadcode tftp-server rtbam.m40
```

loads the restricted load `rtbam.m40` into flash from the machine named `tftp-server`.

Caution: You must use the Fsave command immediately after executing the Tload command. Failure to do so can cause your Ascend unit to lose its configuration.

6 Enter the following command to save your configuration to flash memory:

```
fsave
```

7 Enter the following command:

```
nvramclear
```

After the Ascend unit clears NVRAM memory, it automatically resets.

If you have downloaded the extended load, the upgrade is complete.

If you have loaded a restricted load, your system boots up in restricted mode. Restricted mode only allows you to load software. You cannot change or save profiles. While in restricted mode, the Edit menu displays the following banner:

* * RESTRICTED MODE * * * YOU MUST RERUN THE LAST tloadcode COMMAND * *

If your system boots up in restricted mode, repeat the step 5 through step 7 to download the extended load.

Upgrading software from versions earlier than 4.6C to version 5.0A or above

If you are upgrading from software version 4.6C or earlier to version 5.0A or later, perform the upgrade in the following order:

1 Load version 4.6Ci18, following the procedure in “Upgrading system software” on page B-5.

2 Load version 5.0A, following the procedure in “Using TFTP to upgrade to a fat or thin load” on page B-6.

3 Load version 5.0Aix or 6.0.0, following the procedure in “Using TFTP to upgrade to a fat or thin load” on page B-6 (for software versions 5.0Aix) or “Upgrading software with an extended load” on page B-9 (for software version 6.0.0).

Caution: Failure to follow this procedure might cause your Ascend unit to lose or corrupt its configuration, and could render the unit unusable.

Using the serial port to upgrade to a standard or a thin load

Caution: Uploading system software via the serial console overwrites all existing profiles. Save your current profiles settings to your hard disk before you begin upgrading system software. After the upgrade, restore your profiles from the backup file you created. Since the backup file is readable text, you can reenter the settings through the Ascend unit's user interface. To avoid having existing profiles overwritten, use TFTP to upgrade your unit.

Caution: You cannot upload a fat load or an extended load using the serial port; it must be done using TFTP.

Upgrading through the serial port consists of the following general steps:

- Saving your configuration
- Uploading the software
- Restoring the configuration

Before you begin

Before upgrading your system through the serial port, make sure you have the following equipment and software:

- An IBM compatible PC or Macintosh with a serial port capable of connecting to the Ascend unit's Console port.
- A straight-through serial cable.
- Data communications software for your PC or Mac with XModem CRC/1K support (for example, Procomm Plus, HyperTerminal for PCs or ZTerm for the Mac).

Caution: If you use a Windows-based terminal emulator such as Windows Terminal or HyperTerminal, disable any screen savers or other programs or applications that could interrupt the file transfer. Failure to do so might cause the software upload to halt, and can render the Ascend unit unusable.

Saving your configuration

Before you start, verify that your terminal emulation program has a disk capture feature. Disk capture allows your emulator to capture to disk the ASCII characters it receives at its serial port. You should also verify that the data rate of your terminal emulation program is set to the same rate as the Term Rate parameter in the System Profile (Sys Config menu).

You can cancel the backup process at any time by pressing Ctrl-C.

To save the Pipeline configuration (except passwords) to disk:

1. Open the Sys Diag menu.
2. Select Save Config, and press Enter.

   The following message appears:

   ```
   Ready to download - type any key to start....
   ```

3 Turn on the Capture feature of your communications program, and supply a filename for the saved profiles. (Consult the documentation for your communications program if you have any questions about how to turn on the Capture feature.)

4 Press any key to start saving your configured profiles.

Rows of configuration information appear on the screen as the configuration file is downloaded to your hard disk. When the file has been saved, your communications program displays a message indicating the download is complete.

5 Turn off the Capture feature of your communications program.

6 Print a copy of your configured profiles for later reference.

You should examine the saved configuration file. Notice that some of the lines begin with `START=` and other lines begin with `END=`. A pair of these START/STOP lines and the block of data between them constitute a profile. If a parameter in a profile is set to its default value, it does not appear. In fact, you can have profiles with all parameters at their defaults, in which case the corresponding START/STOP blocks are empty. Make sure that there are no extra lines of text or characters either before `START=` or after `END=`. If there are, delete them. They could cause problems when you try to upload the file to the Ascend unit.

Uploading the software

To upload the software:

1 Type the following four-key sequence in rapid succession (press each key in the sequence shown, one after the other, as quickly as possible):

`Esc [ Esc -`

(Press the escape key, the left bracket key, the escape key, and the minus key, in that order, in rapid succession.) The following string of Xmodem control characters appears:

`CKCKCKCK`

If you do not see these characters, you probably did not press the four-key sequence quickly enough. Try again. Most people use both hands and keep one finger on the escape key.

2 Use the Xmodem file-transfer protocol to send the system file to the Ascend unit.

Your communications program normally takes anywhere from 5 to 15 minutes to send the file to your Ascend unit. The time displayed on the screen does not represent real time. Do not worry if your communication program displays several “bad batch” messages. This is normal.

After the upload, the Ascend unit resets. Upon completion of the self-test, the Ascend unit’s initial menu appears in the Edit window with all parameters set to default values. This completes the upgrade.

If the upload fails during the transfer, try downloading another copy of the binary image from the Ascend FTP server and re-loading the code to the Ascend unit. If you still have problems, contact Ascend technical support for assistance.

Restoring the configuration

Under certain circumstances, the serial-port method might not completely restore your configuration. You should therefore verify that your configuration was properly restored every time you use this method. If you have many profiles and passwords, you should consider using

TFTP to upgrade your software. (See "Using TFTP to upgrade to a standard load" on page B-6.)

To restore the configuration, you must have administrative privileges that include Field Service (such as the Full Access Profile, for example). You use the Restore Cfg command to restore a full configuration that you saved by using the Save Cfg command, or to upload more specific configuration information obtained from Ascend (for example, a single filter stored in a special configuration file).

To load configuration information through the serial port

1. From the Ascend unit's VT100 interface, access the diagnostics monitor by typing the following characters in rapid succession:

   ```
   Esc [ Esc =
   ```

   Or, press Ctrl-D to invoke the DO menu, and select D=Diagnostics.

2. At the **>** prompt, enter the Fclear command:

   ```
   > fclear
   ```

3. At the **>** prompt, enter the NVRAMClear command:

   ```
   > nvramclear
   ```

   This causes the system to reset. When it comes back up, proceed with restoring your configuration.

4. Enter **quit** to exit the Diagnostic interface.

5. Open the Sys Diag menu.

6. Select Restore Cfg, and press Enter.

   The following message appears:

   ```
   Waiting for upload data...
   ```

7. Use the Send ASCII File feature of the communications software to send the configuration file to the unit. (If you have any questions about how to send an ASCII file, consult the documentation for your communications program.)

   When the restore has been completed, the following message appears:

   ```
   Restore complete - type any key to return to menu
   ```

8. Press any key to return to the configuration menus.

9. Reset the Ascend unit, by selecting System > Sys Diag > Sys Reset and confirming the reset.

Restoring passwords

For security reasons, passwords are not written to configuration files created through the serial console. A configuration file created using the Tsave command, however, *does* contain the system passwords. You can restore the Tsave configuration file using the serial console.

After upgrading you may have to re-enter all the passwords on your system. If you edit your saved configuration file, however, and enter passwords in the appropriate fields (by replacing the word *SECURE* in each instance), these passwords will be restored. But note that if you do choose to edit your configuration file, you must save it as text only or you will not be able to load it into your unit.

If you restored a complete configuration, the passwords used in your Security profiles have been wiped out. To reset them:

1. Press Ctrl-D to invoke the DO menu, select Password, and choose the Full Access profile.
2. When you are prompted to enter the password, press Enter (the null password).
   After you have restored your privileges by entering the null password, you should immediately open the Connection profiles, Security profiles, and Ethernet profile (Mod Config menu), and reset the passwords to their previous values.

System messages

Table B-3 explains the messages that can appear during your upgrade.

Table B-3. System software messages

Message	Explanation

`UART initialized`
`fat load: bad CRC!!`
`forcing serial download at 57600 bps`
`please download a "thin" system...`
	The fat load has a CRC (cyclic redundancy check) error. Immediately after this message appears, the serial console speed is switched to 57600 bps, and the Ascend unit initiates an Xmodem serial download. Load a thin load that understand the fat load format, as explained in “Using TFTP to upgrade to a fat or thin load” on page B-6.

`File tbam.m40`
`incompatible fat load`
`format--discarding downloaded data`
	You attempted to upgrade to a fat load from a version of system software that does not understand the fat load format. You must first load a thin load that is fat load aware, as explained in “Using TFTP to upgrade to a fat or thin load” on page B-6.

`This load has no platform identifier.` `Proceed with caution.`	This message can occur if you are running software version 5.0Ai11 or later and you load an earlier incremental or patch release onto your system. The message indicates that Tloadcode cannot determine which platform the code is intended for. If you are using the correct software version, you can ignore this message.
`This load appears not to support your network interface.` `Download aborted.  Use ‘tloadcode -f’ to force.`	Indicates you are attempting to load a version of code intended for a different network interface (for example, loading MAX 4000 T1 software onto a MAX 4000 E1 unit).
`This load appears to be for another platform.` `Download aborted.  Use ‘tloadcode -f’ to force.`	Indicates you are attempting to load a version of code onto a platform for which it is not intended (for example, loading MAX 4000 software onto a MAX 2000). This is not recommended

`UART initialized`
`fat load: inflate`
`.....`
`.....`
`starting system...`
	Indicates you have successfully loaded a fat load.

Table B-3. System software messages (continued)

Message	Explanation
UART initialized hybrid load: inflate essential .+.+..... . invalid CRC!! entering restricted mode starting system...	Indicates the extended load has failed and that your system is being brought up in restricted mode. You must reload the software as explained in “Upgrading software with an extended load” on page B-9.
UART initialized hybrid load: inflate essential .+.+..... . invalid length!! entering restricted mode starting system...	Indicates the extended load has failed and that your system is being brought up in restricted mode. You must reload the software as explained in “Upgrading software with an extended load” on page B-9.
UART initialized hybrid load: inflate essential .+.+..... . inflate expendable .....|..... starting system...	Indicates you have successfully loaded an extended load.
UART initialized thin load: inflate .... starting system...	Indicates you have successfully loaded a thin load.

Index

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z