MAX 200Plus
Administrator's Guide

Ascend Communications, Inc.

Part Number 7820-0427-002 June 4, 1997

FCC Part 15

Warning: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

The authority to operate this equipment is conditioned by the requirement that no modifications will be made to the equipment unless the changes or modifications are expressly approved by Ascend.

Canadian Notice

Note: The Canadian Department of Communications label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situation.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give

the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The *Load Number (LN)* assigned to each terminal device denotes the percentage of the total load to be connected to a telephone loop which is used by the device, to prevent overloading. The termination on a loop may consist of any combination of devices subject only to the requirement that the total of the Load Numbers of all the devices does not exceed 100.

This equipment does not support line loopbacks.

Warning: THE DIGITAL APPARATUS DOES NOT EXCEED THE CLASS A LIMITS FOR RADIO NOISE EMISSIONS FROM DIGITAL APPARATUS SET OUT IN THE RADIO INTERFERENCE REGULATIONS OF THE CANADIAN DEPARTMENT OF COMMUNICATIONS.

LE PRESENT APPAREIL NUMERIQUE N'EMET PAS DE BRUITS RADIOELECTRIQUES DEPASSANT LES LIMITES APPLICABLES AUX APPAREILS NUMERIQUES DE LA CLASSE A PRESCRITES DANS LE REGLEMENT SUR LE BROUILLAGE RADIOELECTRIQUE EDICTE PAR LE MINISTERE DES COMMUNICATIONS DU CANADA.

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

5 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).

6 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.

7 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.

8 Prior to 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.

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

10 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.

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

12 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.

13 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.

14 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.

15 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.

Product warranty

1 Ascend warrants that the MAX will be free from defects in material and workmanship for a period of twelve (12) months from date of shipment.

2 Ascend shall incur no liability under this warranty if

- the allegedly defective goods are not returned prepaid to Ascend within thirty (30) days of the discovery of the alleged defect and in accordance with Ascend's repair procedures; or
- Ascend's tests disclose that the alleged defect is not due to defects in material or workmanship.

3 Ascend's liability shall be limited to either repair or replacement of the defective goods, at Ascend's option.

4 Ascend MAKES NO EXPRESS OR IMPLIED WARRANTIES REGARDING THE QUALITY, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE BEYOND THOSE THAT APPEAR IN THE APPLICABLE Ascend USER'S DOCUMENTATION. Ascend SHALL NOT BE RESPONSIBLE FOR CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGE, INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR DAMAGES TO BUSINESS OR BUSINESS RELATIONS. THIS WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES.

Warranty repair

1 During the first three (3) months of ownership, Ascend will repair or replace a defective product covered under warranty within twenty-four (24) hours of receipt of the product. During the fourth (4th) through twelfth (12th) months of ownership, Ascend will repair or replace a defective product covered under warranty within ten (10) days of receipt of the product. The warranty period for the replaced product shall be ninety (90) days or the remainder of the warranty period of the original unit, whichever is greater. Ascend will ship surface freight. Expedited freight is at customer's expense.

2 The customer must return the defective product to Ascend within fourteen (14) days after the request for replacement. If the defective product is not returned within this time period, Ascend will bill the customer for the product at list price.

Out-of warranty repair

Ascend will either repair or, at its option, replace a defective product not covered under warranty within ten (10) working days of its receipt. Repair charges are available from the Repair Facility upon request. The warranty on a serviced product is thirty (30) days measured from date of service. Out-of-warranty repair charges are based upon the prices in effect at the time of return.

Ascend Customer Service

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

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

How to contact Ascend Customer Service

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

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, Inc.
1701 Harbor Bay Parkway
Alameda, CA 94502-3002

Need information on new features and products?

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

- For the latest information on the Ascend product line, visit our site on the World Wide Web: `http://www.ascend.com/`
- For software upgrades, release notes, and addenda to this manual, visit our FTP site: `ftp.ascend.com`

Contents

About this guide

This guide explains how to install, configure, and use the MAX 200Plus.

What is in this guide?

This guide contains these chapters:

Chapter 1, “Getting Acquainted with the MAX 200Plus,” provides an overview of what the MAX can do and explains some basic internetworking concepts.

Chapter 2, “Configuring the MAX 200Plus,” explains how to configure the MAX.

Chapter 3, “MAX 200Plus System Administration,” explains how to perform such system administration tasks as upgrading MAX system software, backing up the MAX configuration, and accessing the Telnet interface.

Chapter 4, “Example Configurations,” provides examples of MAX configurations.

Chapter 5, “Reference,” provides complete descriptions of all the options in the MAX 200Plus Administrator’s Console.

This guide also includes an index.

What you should know

This guide is intended for the person who will configure and maintain the MAX 200Plus. To configure the MAX 200Plus, you need to understand the following:

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

Manual set

The MAX 200Plus documentation set includes:

- The *MAX 200Plus Getting Started Guide* explains how to install and troubleshoot your MAX 200Plus.
- *MAX 200Plus Getting Windows 95 User's Guide* explains how to dial into the MAX 200Plus using Windows 95 dial-in client.
- *MAX 200Plus Windows/DOS User's Guide* explains how to dial into the MAX 200Plus using the MAXDial dial-in client for Windows 3.1 and DOS.
- The *MAX 200Plus Supplemental Documentation Set* explains how to use the MAX 200Plus Telnet interface. Although the MAX 200 Plus Administrator's Console allows you to perform most common configurations of your MAX 200Plus, you need to consult the supplemental documentation set if you want to:
  - use a Remote Authentication Dial-In User Service (RADIUS) server
  - configure security card authentication for incoming users
  - add filtering
  - add static Routes
  - configure the MAX 200 Plus as a terminal server
  - fine-tune the dynamic bandwidth allocation (DBA) parameters
  - monitor routing and bridging tables

– monitor the MAX 200 Plus traffic

– fine-tune Routing Information Protocol (RIP)

Documentation conventions

This section shows the documentation conventions used in this guide.

Convention	Meaning
`Monospace text`	Monospace text represents information that you enter exactly as shown, and it identifies onscreen text, such as, statistical information.
[]	Square brackets indicate an optional attribute that you append to a command. To include an attribute, type only the information inside the brackets. Do not type the brackets unless they appear in bold type.
italics	Italics represent variable information. Do not enter the words themselves in the command; enter the information they represent.
Key1-Key2	Keys displayed next to each other represent combination keystrokes. To enter combination keystrokes, press one key and hold it down while you press one or more other keys. Release all the keys at the same time.
|	The | symbol separates command choices that are mutually exclusive.
Note:	A note signifies important additional information.
 **Caution:**	A caution means that a failure to follow the recommended procedure could result in a loss of data or damage to equipment.
 **Warning:**	A warning means that a failure to take appropriate safety precautions could result in physical injury.

Getting Acquainted with the MAX 200Plus

1

This chapter introduces the MAX 200Plus and provides an overview on how it works. It contains these sections:

How you can use the MAX 200Plus

The MAX 200Plus is an eight-port remote access switch that enables computer network communication across the wide-area telephone network, using either analog modems or Integrated Services Digital Network (ISDN) BRI cards. By providing high-performance WAN access through a single device, the MAX 200Plus provides the technology you need to extend your corporate backbone network to remote users and to provide access to the Internet.

Typically, a corporate backbone network is a closed system, made up of circuits that connect to fixed destinations over defined paths inside the network's boundaries. This type of network, however, is inadequate if users need to access the corporate network from a variety of locations.

MAX 200Plus supports two different kinds of connections:

- client dial-in involves users of personal computers dialing into the MAX 200, typically using modems or an ISDN device, to access the resources of the local area network. These users include telecommuters, workers in remote offices, at home, at customer sites, at vendor sites, and on the road.
- network-to-network connections are made when the MAX 200Plus communicates with another routing or bridge device (such as an Ascend MAX 200Plus or Pipeline product) to connect two local area networks together, or to connect a LAN to the Internet.

Figure 1-1 shows a typical scenario in which home users, remote offices, and customer sites access the backbone network of a major investment banking firm.

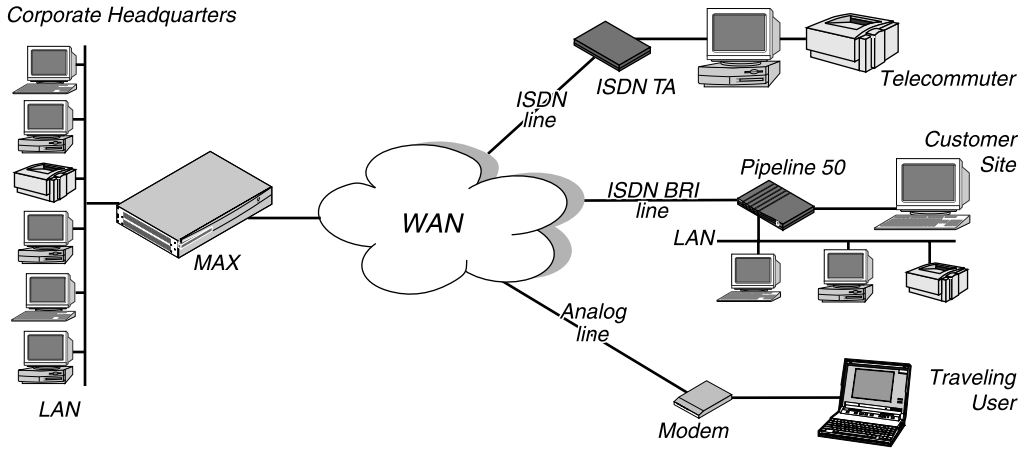


Figure 1-1. Using the MAX 200Plus as a remote access switch

Brokers with home workstations can log into the corporate LAN using a Pipeline from their home. Remote offices connect to the backbone using the Pipeline 50. Customers who need access to current market information can also access selected corporate network resources. In addition, a traveling computer user with an analog modem can dial into the central LAN.

Notice that each user can access the MAX 200Plus using a different type of line. One user may access the MAX 200Plus using the switched circuit on an ISDN BRI line, while another user may use an analog modem.

MAX 200Plus features

The MAX 200Plus provides a wide of range of sophisticated features specifically designed for telecommuting and remote LAN access. These include:

- protocol-independent bridging
- Internet Protocol (IP) routing
- Internetwork Packet Exchange (IPX) routing
- Inverse multiplexing
- dynamic bandwidth allocation

- comprehensive security
- flexible management options

LAN Protocols

Protocols are the languages computers use to communicate with each other on networks. The MAX 200Plus supports these LAN protocols:

- IP is the protocol used on the Internet. It is also the protocol used for communication between the MAX 200Plus and the administration program.
- IPX is used for communication with Novell NetWare servers.
- AppleTalk is the protocol used by Apple Computer products.

Note that both IP and IPX can also be used as the transport protocol for the network facilities of Microsoft Windows for Workgroups, Windows 95, or NT.

WAN encapsulation protocols

In order to send data over the WAN in a form understandable by the receiver, the sending device must encapsulate the data—that is, the sending device must make sure that the data appears to the receiver in a mutually agreed upon format. The MAX 200Plus supports the WAN encapsulation protocols described in this section.

Point-to-Point Protocol (PPP)

PPP (RFC 166) provides a standard means of encapsulating data packets sent over a single-channel WAN link. It is the standard WAN encapsulation protocol for the interoperability of bridges and routers. PPP is also supported in workstations, allowing direct dial-up access from a personal computer to a corporate LAN or Internet Service Provider (ISP).

Multilink PPP (MP)

MP is an extension of PPP that supports the ordering of data packets across multiple channels and offers inverse multiplexing. For information on inverse multiplexing, see “Inverse multiplexing” on page 1-7.

Multilink Protocol Plus (MP+)

MP+ is Ascend’s proprietary protocol that supports inverse multiplexing and bandwidth management. MP+ allows you to combine individual channels into a single high-speed connection.

For information on inverse multiplexing, see “Inverse multiplexing” on page 1-7. For information on bandwidth management, see “Dynamic Bandwidth Allocation (DBA)” on page 1-7.

AppleTalk Remote Access (ARA)

ARA is a protocol developed by Apple Computer to enable a Macintosh system to dial into another Macintosh or into a central network via asynchronous modem. ARA uses V42 Alternate Procedure as its data link, which limits ARA to the use of asynchronous modems.

ARA relies on AppleTalk, and a minimal AppleTalk stack has been added to the MAX 200Plus for ARA support. ARA is primarily a dial-in protocol. Dial-out is used only to support callback.

In the MAX 200Plus, ARA is implemented as a link encapsulation method, which enables administrators to control it on a per-connection or global basis. Unlike PPP or MP+ encapsulation, ARA does not use PAP or CHAP authentication, so it is important to disable ARA guest logins if you want to provide login security for ARA users.

Bridging and routing (network-to-network)

You can use the MAX 200Plus as both a bridge and a router. The MAX 200Plus bridges and routes TCP/IP (Transmission Control Protocol/Internet Protocol) and IPX, and uses protocol-independent bridging to handle any other protocols. You can use routing and bridging simultaneously over the same link.

Using the MAX 200Plus as a bridge

A bridge connects two LAN segments using physical station address information. Most users implement a bridge to divide a busy network into segments, reducing traffic on each side. The bridge prevents traffic on one segment from going to another segment.

Using the MAX 200Plus as a router

A router sends data over a WAN using logical rather than physical addresses; a WAN consists of two or more remote LANs connected across a network.

To determine how to route data, the MAX 200Plus uses both RIP (Routing Information Protocol) and static routing protocols. Using RIP, you can determine whether the MAX 200Plus sends or receives routing path updates over its Ethernet interface. You can also define static connections to remote networks.

Dial-in Users

You can configure these kinds of users to access the MAX 200Plus:

- **Macintosh**—The MAX 200Plus is compatible with ARA versions 1.0 and 2.x. Mobile Macintosh users can use ARA to dial into their network through the MAX 200Plus. Appendix A, “Using AppleTalk Remote Access and MacTCP,” explains how to configure ARA users to dial into the MAX 200Plus.
- **Windows 3.x PCs**—The MAXLink client software that comes with the MAX 200Plus contains Novell’s IP and IPX as well as the Novell IPX client for easy access to the MAX 200Plus. MAXLink client contains

extensive online help and is specifically designed to provide seamless access to the MAX 200Plus.

- **Windows 95 PCs**—These users can dial in to the MAX 200Plus using the IPX or TCP/IP Remote Clients that come with Windows 95.

Inverse multiplexing

The MAX 200Plus inverse multiplexing technology is a method of combining individual channels into a single, higher-speed channel. Each end of the connection must use a device that supports inverse multiplexing, such as a MAX. For example, with inverse multiplexing three ISDN channels can be combined into a single channel, providing a higher bandwidth connection for more data intensive applications.

These protocols support inverse multiplexing on the MAX 200Plus:

- MP (Multilink PPP)
- MP+ (Multilink Protocol Plus)

Dynamic Bandwidth Allocation (DBA)

Closely related to inverse multiplexing is Dynamic Bandwidth Allocation (DBA). DBA is a technology that enables the MAX 200Plus to automatically add or subtract bandwidth from a switched connection in real time without terminating the link. MP+ supports Dynamic Bandwidth Allocation.

The MAX 200Plus calculates average line utilization (ALU) over a set period of time, and then compares the ALU to a target percentage threshold. When ALU exceeds the threshold for a specified period of time, the MAX 200Plus attempts to add channels. When ALU falls below the threshold for a specified period of time, the MAX 200Plus attempts to remove channels.

If you use a circuit between two locations to capacity 24 hours per day, using a dedicated line is more cost effective than using a switched line. However, if you need the circuit only sporadically, or if the circuit is sometimes underutilized, it often makes more sense to use a switched channel as traffic requirements dictate.

For example, you might establish some connections only when you need to transfer data. In this case, a single circuit can accommodate low traffic levels. However, if traffic levels grow beyond the capacity of the circuit (such as during a large file transfer), DBA automatically adds additional switched channels. When traffic levels subside, DBA automatically removes the channels from the connection. The bandwidth and connection costs are thereby reduced. You pay only for bandwidth when you need it.

Comprehensive security

The MAX 200Plus provides full WAN security using the features described in this section.

PAP (Password Authentication Protocol)

PAP provides a simple method for a host to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment, and does not use encryption. PAP is used with a PPP connection.

CHAP (Challenge-Handshake Authentication Protocol)

CHAP is more secure than PAP. CHAP provides a way to periodically verify the identity of a host using a three-way handshake and encryption. Authentication takes place upon initial link establishment; the MAX 200Plus can repeat the authentication process any time after the connection is made. PAP is used with a PPP connection.

Callback security

You can specify that the MAX 200Plus call back any user dialing into it. The callback number is registered in the MAX 200Plus and is associated with the address and name of the dial-in user. Callback security provides the highest level of confidence in the control and security of the network and its topology. PAP is used with a PPP connection.

Security-card authentication

The MAX 200Plus supports hand-held personal security cards, such as those provided by Enigma Logic® and Security Dynamics®. These cards have dynamic passwords that provide a higher level of security than traditional static password methods. 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.

User list

You can assign each user that needs access to the MAX 200Plus a username and password.

System management

The MAX 200Plus provides several sophisticated management mechanisms. These tools are described in this section.

Windows 95 Management Console

You can perform the most common configuration tasks using the MAX 200Plus Windows 95 Management Console. There may be some situations, however, when you will need to use the Telnet, character-based interface to configure your MAX. In particular, you must use the Telnet interface if you want to:

- create or apply filters
- create static routes
- monitor IP and IPX statistics
- view the MAX routing tables
- use a RADIUS authentication server

In addition, there are other advanced features that cannot be configured using the Windows 95 Management Console.

Refer to the *MAX 200Plus Supplemental Documentation Set* for details on using the Telnet interface to configure your MAX.

SNMP management

The MAX 200Plus can be managed using the Simple Network Management Protocol (SNMP). In SNMP, two types of communicating devices exist: agents and managers. An agent (such as the MAX 200Plus) provides networking information to a manager application running on another computer. The agents and managers share a database of information, called the Management Information Base (MIB). An agent can use a message called a traps-PDU (Protocol Data Unit) to send unsolicited information to the manager.

Because the WAN interface is integrated into the MAX 200Plus, you can manage it using SNMP MIB II and Ascend Enterprise MIBs from a central SNMP manager, such as SunNet Manager or HP Open View. The MAX 200Plus can send management information to an SNMP manager without being polled.

SNMP security uses a community name sent with each request. The MAX 200Plus supports two community names, one with read-only access, and the other with read/write access to the MIB.

You must use the Telnet interface to change the SNMP community names as well as set up SNMP managers to receive MAX SNMP traps.

Refer to the *MAX 200Plus Supplemental Documentation Set* for details on using the Telnet interface to configure your MAX.

TCP/Telnet management

After you have performed the initial configuration of your MAX using the Windows 95 Management Console you can remotely manage a MAX 200Plus by establishing a Telnet session to the MAX 200Plus from any Telnet workstation on the corporate network. When you enter the appropriate password, you can view the MAX 200Plus character-based user interface on a VT-100 window, and perform all configuration, diagnostic, management, and other control functions.

Refer to the *MAX 200Plus Supplemental Documentation Set* for details on using the Telnet interface to configure your MAX.

FLASH memory upgrades and remote software upgrades

FLASH RAM technology enables you to perform software upgrades in the field without opening the unit or changing memory chips.

Activity Log

The Activity Log provides a database of information about each call, including:

- event type
- time and date of call
- session number
- slot number
- comment

Introduction to Ascend bridging

This section provides an overview of packet bridging and when to use bridging instead of a routing configuration. It also explains how the MAX 200Plus brings up a bridging connection.

When to use bridging

Bridges are used primarily to provide connectivity for protocols other than IP and IPX. 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 200Plus are:

- To provide AppleTalk or other non-routed protocol connectivity with another site

- To link any two sites so that their nodes appear to be on the same LAN
- To support protocols that depend on broadcasts to function, such as BOOTP

Bridges run in promiscuous mode; that is, they examine all packets on the LAN, so they incur greater processor and memory overhead than routers do. On heavily loaded networks, this increased overhead can result in slower performance.

In addition to the performance benefit of routing, routers have other advantages over bridging as well. 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.

How a bridging connection is initiated

The MAX 200Plus handles dial-in and dial-out aspects of WAN connections, and bridges packets between networks. At the appropriate point in a session negotiation, the MAX 200Plus begins passing packets to its bridging/routing software. The MAX 200Plus then operates like a regular LAN bridge with ports on two different Ethernet segments.

When the MAX 200Plus is configured to bridge, it accepts all packets on the network. It brings up a connection to a remote network when the destination address in a packet is one of the following:

- A physical address that is not on the local Ethernet segment (the segment to which the MAX 200Plus 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 200Plus receives a packet whose destination MAC address is not on the local network, it first checks its internal bridge table (see "Transparent bridging" on page 1-14 for information on how the MAX builds a bridging table).

If it finds the packet's destination MAC address in its bridge table, the MAX 200Plus dials the connection and bridges the packet.

If the address is *not* specified in its bridge table, the MAX 200Plus checks for active sessions that have bridging enabled. If there are one or more active bridging links, the MAX 200Plus forwards the packet across *all* active sessions that have bridging enabled.

Note: The MAX 200Plus does not ordinarily dial a connection for packets that are not on the local network and not specified in its bridge table, because it has no way of finding the proper number to dial. You can, however, configure the MAX to dial connections when it receives broadcast packets as explained in the next section.

Broadcast addresses and bridging connections

A broadcast address is recognized by multiple nodes on a network. For example, the Ethernet broadcast address at the physical level is:

```
FFFFFFFFFFFF
```

All devices on the same network accept packets with that destination address.

If the MAX 200Plus receives a packet whose destination MAC address is a broadcast address, it forwards the packet across all active sessions that have

bridging enabled. You can also configure the MAX to dial an inactive connection whenever it receives a broadcast packet.

Transparent bridging

The MAX 200Plus is a transparent bridge (also called a learning bridge). It keeps track of where a particular address is located and the number needed to bring up that interface. As it forwards a packet, it notes the packet's source address and creates a bridge table that associates node addresses with a particular interface.

For example, Figure 1-2 shows the physical addresses of some nodes on the local Ethernet and at a remote site. The MAX 200Plus at site A is configured as a bridge.

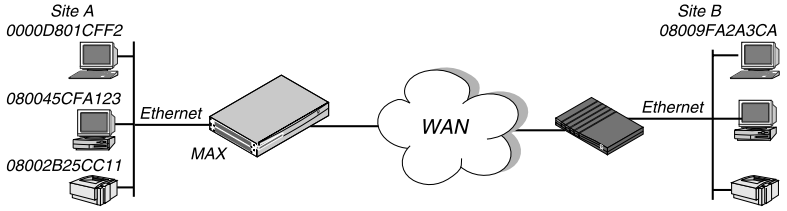


Figure 1-2. Physical addresses on two Ethernet segments

The MAX 200Plus 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:

```
0000D801CFF2SITEA
080045CFA123SITEA
08002B25CC11SITEA
08009FA2A3CASITEB
```

The connection to Site B is associated with a bridging link either because it was used to dial the link or because it matched an incoming call.

Entries in its bridge table must be relearned within a fixed aging time limit; otherwise they are removed from the table.

Introduction to Ascend IP routing

The MAX 200Plus implements these protocols in the TCP/IP suite:

- IP (Internet Protocol)
- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)
- ICMP (Internet Control Message Protocol)
- ARP (Address Resolution Protocol)
- RIP (Routing Information Protocol)
- SNMP (Simple Network Management Protocol)

The MAX 200Plus supports TCP/IP over any type of WAN connection, and is fully interoperable with non-Ascend products that support TCP/IP.

About IP addresses

IP addresses are 32-bit numbers which are normally expressed as four decimal numbers separated by periods. This is called “decimal-dot notation.” A portion of the address is used for the network number, and a portion is used for the node (that is, the single workstation) address.

IP addresses come in different classes, depending on how many network nodes will be attached to the Network. Class C addresses, for example, can accommodate up to 254 nodes.

IP network addresses are administered from a central authority in such a way that each network in the world has a unique address. If you intend to connect to the Internet, you should obtain an IP network address from your Internet Service Provider. If you never intend to connect to the Internet, or to any other IP network, you can use a non-routable address, such as 127.1.1.0. The first node would be 127.1.1.1, and the second 127.1.1.2.

A subnet mask is a way to subdivide a network into smaller networks, so you can have a greater number of computers on a network with a single IP address.

Note: If the MAX 200Plus is connected to a local subnet and will connect to a remote subnet of the *same* IP network, both sides of the connection must use the same subnet mask.

When to use IP routing

Use IP routing in the MAX 200Plus to connect two sites that both have an IP address. The most common uses for IP routing in the MAX 200Plus are:

- To enable many independent connections to the Internet (using an Internet Service Provider)
- To integrate multiple IP subnets that are geographically distributed (telecommuting hubs)

The MAX 200Plus can be configured as a bridge, a router, or both. However, you cannot both bridge and route TCP/IP packets across the same connection. When you configure the MAX 200Plus as an IP router, IP packets are no longer bridged at the link layer. They are *always* routed at the network layer. All other protocols continue to be bridged unless you turn off bridging.

How an IP routing connection is initiated

The MAX 200Plus handles dial-in and dial-out aspects of WAN connections, and routes packets between networks. At the appropriate point in a session negotiation, the MAX 200Plus begins passing packets to its bridging/routing software. The MAX 200Plus then operates as a regular IP router, with two interfaces on two different networks or subnets.

An IP routing connection can be network-to-network or host-to-network:

- Typically, a network-to-network connection is initiated when a user starts up a TCP/IP application, such as a World Wide Web browser or Telnet, and enters a URL, hostname, or IP address that is not on the local network. This creates an outbound IP packet (a packet whose destination address is not on that network). The calling device places the

call and the answering device (the MAX 200Plus) picks it up. If the session is negotiated successfully, the IP packet is passed to the MAX and routed appropriately.

- A host-to-network connection is usually initiated by a user starting up PPP and calling the MAX 200Plus. The calling host may be connected to a modem or wireless communication device.

Host requirements

IP hosts on the local IP network, such as UNIX systems, Windows or OS/2 PCs, or Macintosh systems, must have appropriately configured TCP/IP software or "stack." A remote user calling into the local IP network must also have PPP software.

UNIX systems typically include a TCP/IP stack, DNS software, and other software, files, and utilities used for Internet communication. UNIX network administration documentation describes how to configure these programs and files.

PCs running Windows or OS/2 need a TCP/IP stack. The stack 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 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.

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 200Plus, the TCP/IP software must be configured to allow dynamic allocation of IP addresses (see"Dynamic IP routing" on page 1-19 for more information).

If a DNS server is supported on your local network, you should also configure the host software with the DNS server's address. Specifying DNS information enables users on remote networks to access local network resources using hostnames instead of IP addresses.

Typically, the host software is configured with the MAX 200Plus as its default router.

Creating and maintaining the IP routing table

When IP routing is enabled, the MAX 200Plus creates a routing table during initialization. Each entry in the routing table specifies at least two pieces of information: a destination network address, and the router used to forward a packet toward that destination. The routing table contains entries that are learned either from RIP or from any connections you have configured. If RIP is turned off, the MAX 200Plus must rely on the IP parameters configured in a connection to reach a destination.

When a packet's destination is not on the local IP network, the MAX 200Plus scans its routing table to determine where to forward the packet. If two possible routes exist for forwarding the outbound packet, the MAX 200Plus uses the route with the lower metric. A lower metric indicates that this route is more easily reached.

If no routes exist, it forwards the packet to the default gateway.

For applications such as Telnet and ping, which require that packets be transmitted in both directions, both the calling and answering devices must have appropriate routes.

Dialing non-Ascend routers

When the MAX 200Plus answers an incoming PPP call, it examines the IP source address, assumes the source is a router, and builds a temporary route back to the source network. Since the source subnet mask is not given, the MAX 200Plus assumes the network address is class A, B, or C, based on the source IP address. If you have dialed a non-Ascend router that does not build this initial temporary route, you may have to use RIP or static routes to build a route back.

Dynamic IP routing

The MAX 200Plus uses Routing Information Protocol (RIP), a protocol in the TCP/IP protocol suite, to dynamically build its routing table. RIP broadcasts routing updates every 30 seconds.

RIP can be enabled on the Ethernet interface, the WAN interface, or both. Typically, it is enabled on the Ethernet interface if other routers (such as a Cisco router or a UNIX system running the route daemon) are connected to the local IP network. Many sites turn off RIP on the WAN interface, because it tends to cause very large local routing tables.

When the MAX 200Plus establishes an IP routing connection on the WAN interface, it adds that destination to its routing table. If RIP is enabled on the Ethernet interface, the next RIP packets broadcast by the MAX 200Plus on the Ethernet side will contain information about the new route. Within a minute or so, all routers on the local network will be informed about the new route.

If RIP is enabled on the WAN interface, the MAX 200Plus also broadcasts its routing information to the remote network, and listens for RIP updates from that network. Gradually, all routers on both networks have consistent routing tables (all of which may become quite large).

Note that enabling RIP on the WAN interface could prevent the connection from timing even if the remote session has been idle for a very long time (such as might happen if a remote user forgot to hang up their phone).

Static routes

Each connection you create defines a fixed route to a particular location, rather than a dynamic route as explained in the previous section. These fixed routes are called static routes, and are not updated by RIP when your network configuration changes.

If the MAX has a dynamic route and static route to the same destination, it determines which route to use based on the metric of the route. The MAX sends packets via the route with the lower metric.

To ensure that the MAX always routes packets to a particular destination using its static route, turn RIP off. When RIP updates are turned off, the dynamic entries in the routing table age and expire, leaving only the static route entries.

Note: You cannot use static routes with dynamically assigned IP addresses. In addition, static routes require maintenance, while dynamic routes are maintained automatically.

The default route

If no routes exist for the destination address of a packet, the MAX 200Plus forwards the packet to the default gateway. If you do not define a default gateway the MAX drops any packet it doesn't have a route to.

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).

How connections work as static routes

Each IP connection defines a static route. For example, in the network diagram shown in Figure 1-3, the connection itself is a static route to the remote device with the address 10.9.8.10/22. With this address, the static route is defined with these addresses:

- Destination=10.9.8.10/22
- Default Gateway=10.9.8.10

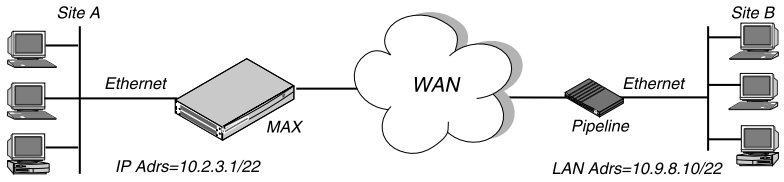


Figure 1-3. A connection serving as a static route

Planning an IP routing configuration

This section provides these sample IP routing configurations:

- an host to network connection—in this case, a single user is connecting to the MAX 200Plus using a modem or ISDN PC Card
- network-to-network connection—in this case, the MAX 200Plus is used to connect to networks together

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.

An example host connection via modem

Figure 1-4 shows an example configuration in which the MAX 200Plus is connected to a backbone IP network that will communicate with telecommuters via modem.

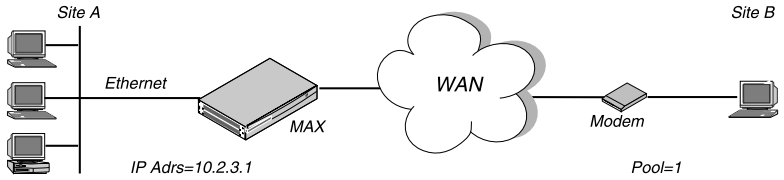


Figure 1-4. Host-to-network connection

In this example, site A is a backbone network and site B is one PC with a modem, TCP/IP stack, and PPP software. The PC will be assigned an address on the local IP network (an address between 10.2.3.10 and 10.2.3.19, as defined in Pool 1).

Chapter 4, “Example Configurations,” provides the MAX 200Plus settings required for the above example.

An example network-to-network connection

Figure 1-5 shows an example configuration in which the MAX 200Plus connects its local network to another remote IP network.

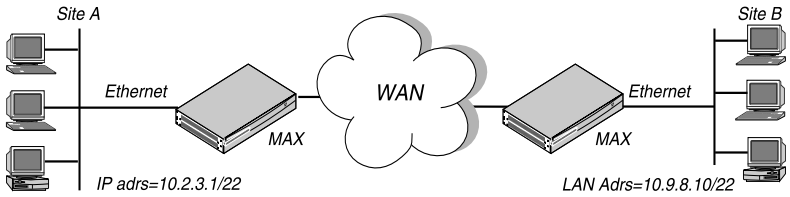


Figure 1-5. Network-to-network connection

Chapter 4, “Example Configurations,” provides the MAX 200Plus settings required for the above example.

Introduction to Ascend IPX routing

The MAX 200Plus (and Ascend Pipeline products) supports IPX routing over PPP and MP+. IPX routing can be configured along with protocol-independent bridging and IP routing in any combination.

Ascend IPX routing works with Novell NetWare version 3.11 or newer.

Note: This chapter does not explain basic IPX concepts. It assumes that you are adding the MAX 200Plus to an existing Novell LAN. If you are not familiar with NetWare or IPX routing, we recommend that you read the applicable Novell documentation.

When to use Ascend IPX routing

Use Ascend IPX routing to connect a local Novell LAN to another site that supports NetWare. The most common uses are:

- To allow geographically remote NetWare clients to access your local NetWare servers. See “An example host connection via modem” on page 1-21.
- To integrate your local NetWare servers and clients with remote sites to form an interconnected wide-area network.

  See “Planning a connection with servers on both sides of the link” on page 1-29.

Standard IPX routing using RIP

All IPX routers periodically broadcast IPX RIP (Routing Information Protocol) packets that inform other routers about available networks. IPX RIP is similar to the routing information protocol in the TCP/IP protocol suite, but it is a different protocol. (In this section, RIP always refers to IPX RIP.)

Most IPX routers, including the MAX 200Plus, use RIP broadcasts to create and update their internal routing table. When an IPX router receives an IPX packet, it consults its routing table to see where to forward the packet. In the MAX, the routing table affects which connection(s) are brought up.

Because entries in a routing table age and expire when updates are not renewed frequently enough (for example, if a connection has not been up for a while), the Ascend extensions are necessary for reliable IPX routing over the WAN.

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. This scheme was not designed for WAN operations, and Ascend provides these extensions to standard IPX for enhancing WAN functionality:

- Dial on Query
- Watchdog spoofing

Dial on Query

When you enable Dial on Query for a connection the MAX 200Plus brings up that connection whenever a NetWare client on the local network queries for a server and the MAX 200Plus unit's routing table is empty. Note that if there are any servers in the MAX 200Plus unit's routing table, either from an IPX connection or learned through RIP, Dial on Query has no effect.

Watchdog spoofing

NetWare servers send out NetWare Core Protocol (NCP) watchdog packets to monitor client connections. Clients that respond to watchdog packets remain logged into the server. If a client does not respond for a certain amount of time, the NetWare server logs the client out.

Repeated watchdog packets would cause a WAN connection to stay up, even if there was no "real" data being sent. But if the MAX simply filtered those packets, client sessions would be dropped by the remote NetWare server. To prevent this, the MAX responds to NCP watchdog packets 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.

Watchdog spoofing allows the remote client to maintain a logical connection to the MAX and the NetWare network while the physical connection is brought down. To the NetWare server, a spoofed connection looks like a normal, active client login session.

The spoofing timer begins counting down after a link has been idle for two minutes. When the spoof time has expired, the connection between the MAX

and the remote client is brought down. If the remote client begins to send data to the NetWare network before the spoofing time has expired, the MAX re-establishes the physical connection and the spoofing timer is reset.

Dial-in NetWare clients

The MAX 200Plus allows individual NetWare clients that are not connected to an Ethernet to dial in and be assigned to an IPX network. The client—such as a MAXLink client—must be running PPP client software to connect to an IPX network through the MAX 200Plus.

When a NetWare client dials into the MAX it is assigned a WAN network number and the MAX treats the dial-in client as a single node. It does not send RIP and Service Advertising Protocol (SAP) advertisements across the connection and ignores RIP and SAP advertisements received from the client. However, it does respond to RIP and SAP queries received from dial-in clients.

Managing the NetWare server table

In NetWare 3.*x*, NetWare servers broadcast SAP packets every 60 seconds to make sure that all routers and bridges know about available services. In NetWare 4.0 and later, built-in directory services eliminates the need for SAP. Services are located through directory services instead. Like other IPX routers, the MAX 200Plus builds a server table based both on statically configured IPX routes and information contained in SAP broadcast packets.

Planning an IPX WAN connection

This section describes how to get the local IPX information you need, and shows how to plan two common IPX WAN configurations:

- A connection with IPX servers on one side of the link only
- A connection with IPX servers on both sides of the link

Making the MAX 200Plus compatible with the local IPX network

The IPX configuration for the Ethernet interface of the MAX 200Plus must be consistent with other NetWare servers connected to the same Ethernet segment. This means:

- The MAX 200Plus must use the same IPX network number as NetWare servers on the Ethernet.
- The MAX 200Plus must be configured with the same IPX frame type used by the NetWare servers.

IPX network number

The MAX 200Plus can learn the correct IPX network number on Ethernet by listening to other routers. Leave the LAN network number at zero to allow this learning behavior. If you enter a value other than zero, the MAX 200Plus becomes a "seeding" router and other routers can learn their number from the MAX 200Plus. For more details about seeding routers, see the Novell documentation.

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 need to know both the external and internal network numbers in use at all sites.

IPX frame type

The MAX 200Plus can route only one packet frame type, and it routes and spoofs IPX packets only if they are encapsulated in that frame. If a connection has both bridging and IPX routing enabled in the same connection, the MAX 200Plus can only route a single IPX frame type, and it will bridge any other IPX packet frame types.

If you are not familiar with the concept of packet frames, see the Novell documentation.

Checking local NetWare configurations

NetWare clients on a wide-area network do not need special configuration in most cases. However, here are some issues that may affect IPX routing performance over the WAN:

- 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 that requires the least expensive connection costs.

- Local copy of LOGIN.EXE

  Try to use the WAN primarily for transferring files, not for executing programs. We recommend that you 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. It is included automatically in server and client software for NetWare 3.12 or later. If local servers are running NetWare 3.11, the servers should have PBURST.NLM and PC clients should have BNETX.COM. Refer to your Novell documentation for more information.

- Macintosh or UNIX clients

  Both Macintosh and UNIX clients can use IPX to communicate with servers. However, both types of clients also support native support using AppleShare (Macintosh) or TCP/IP (UNIX).

  If Macintosh clients must access NetWare servers across the WAN by using AppleShare client software (rather than MacIPX), the WAN link must support bridging. Otherwise, AppleTalk packets will not make it across the connection.

  If UNIX clients will access NetWare servers via TCP/IP (rather than UNIXWare), the MAX 200Plus must also be configured as a bridge or IP router. Otherwise, TCP/IP packets will not make it across the connection.

Deciding on authentication for IPX incoming calls

Unlike an IP routing configuration, where the MAX 200Plus uniquely identifies the calling device by its IP address, an IPX routing configuration does not include a built-in way to identify incoming callers. For that reason, password authentication using PAP or CHAP is required unless IP routing is configured in the same connection.

If a connection requires both IPX and IP routing, you are not required to configure incoming password authentication. The MAX 200Plus uses station names and passwords to sync up the connection with the remote device.

Planning a connection with servers on one side of the link only

Note: When the MAX 200Plus will connect to an existing Novell LAN, you need to work with the administrator of that network to obtain network numbers and server-specific information.

Figure 1-6 shows an example of a network configuration in which the MAX is connected to a local IPX network that supports both servers and clients.

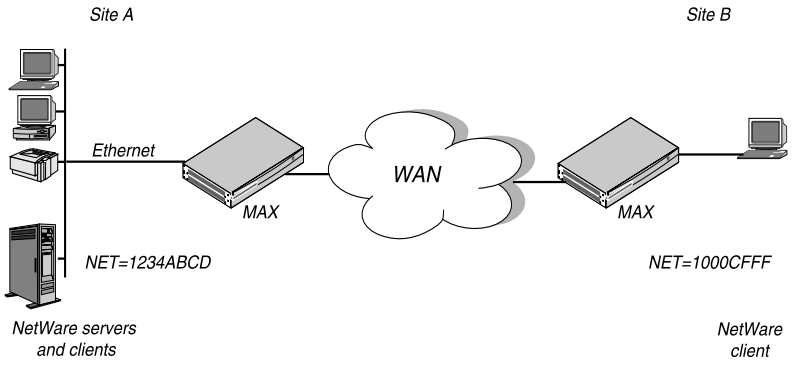


Figure 1-6. Servers on one side of the connection only

In this example, site A supports NetWare 3.12 servers, NetWare clients, and a MAX 200Plus.

Site B is a home office that consists of one PC and a Pipeline. It is not an existing Novell LAN, so the Pipeline configuration creates a new IPX network (1000CFFF in this example).

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.)

Note: If one of the calling units is set to answer only, only the incoming authentication parameters are needed. If a unit is configured to call only, only the outbound authentication is used.

Chapter 4, "Example Configurations," provides the MAX 200Plus settings required for the above example.

Planning a connection with servers on both sides of the link

Figure 1-7 shows an example of a network configuration in which the MAX 200Plus is connected to an IPX network that supports both servers and clients and will connect with a remote site that also supports both servers and clients.

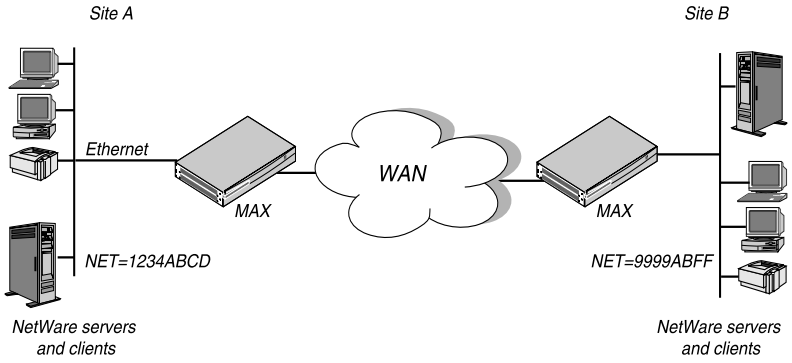


Figure 1-7. Servers on both sides of the connection

In this example, site A and site B are both existing Novell LANs that support NetWare 3.12 and NetWare 4 servers, NetWare clients, and a MAX 200Plus.

Note: If one of the calling units is set to answer only, only the incoming authentication parameters are needed. If a unit is configured to call only, only the outbound authentication is used.

Chapter 4, “Example Configurations,” provides the MAX 200Plus settings required for the above example.

Configuring the MAX 200Plus

2

This chapter explains how to configure the MAX 200Plus.

Note: For detailed information on the options in the Management Console, refer to Chapter 5, “Reference.”

The chapter contains these sections:

Before you configure the MAX 200Plus

Before you configure the MAX 200Plus, gather the following information:

MAX 200Plus identification information

- The name of the MAX 200Plus
- The name of the system administrator or Technical Support contact
- The location (the room, floor or department) of the MAX 200Plus

Protocol information

- If you use IPX, the LAN and WAN numbers, and the frame type
- If you use AppleTalk, the zone name
- If you use IP, you must know the IP address, default gateway, and subnet mask. In addition, your network configuration may require you to enter the following additional information:
  - the primary and secondary Domain Name Service (DNS), primary and secondary Windows Internet Name Service (WINS), port address assignments for Pool 1 and Pool 2, and the range for each of the dynamic address pools

Connections information

- The station name (the name of the remote device)
- If you require a caller ID, the ID
- the password remote users must enter to access the MAX 200Plus
- The callback phone number
- The billing number
- The dial-out number
- The password and auxiliary password
- If you enable IPX routing, the IPX net number
- If you enable IP routing, the LAN address

BRI Card configuration information

- switch type
- Primary and secondary phone numbers for B1 and B2
- Service profile identifier numbers for B1 and B2

Configuring a MAX 200Plus for the first time

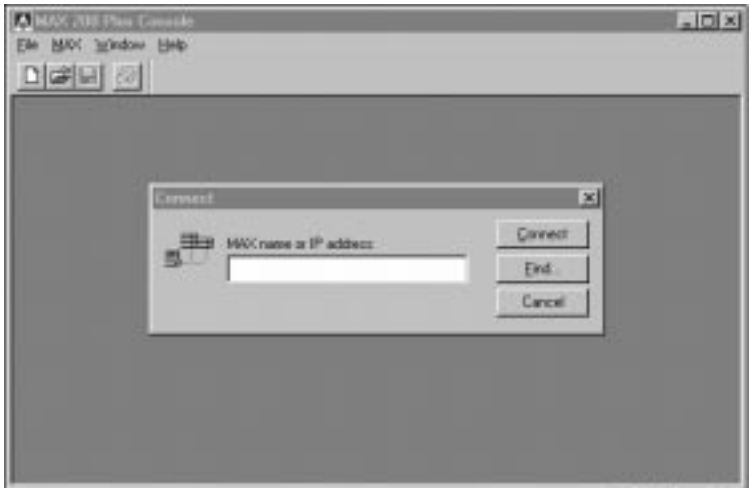
The Management Console finds new MAX 200Plus units on the same subnet as the PC running the console by sending out a broadcast message.

Unconfigured MAX 200Plus units respond to this broadcast with their unique Media Access Control (MAC) address. Once the Management Console has discovered new MAX 200Plus units, it displays them in the Find MAXs dialog box. From this dialog box you can connect to your MAX 200Plus and configure it.

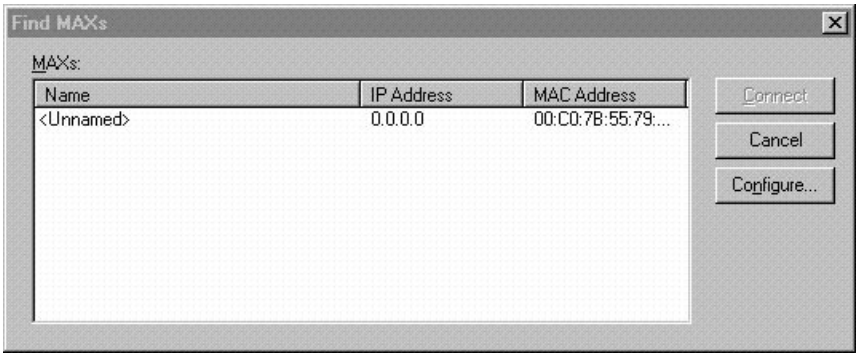
To connect to a MAX 200Plus for the first time:

1 Start the Management Console application.

A new configuration file window opens and the Connect dialog box appears.



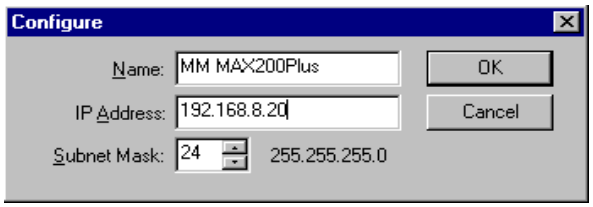
2 Click Find and the Find MAXs dialog box appears.



If unconfigured MAX 200Plus are connected to the same subnet, they appear in the list as “Unnamed” with an IP address of 0.0.0.0, and their MAC addresses (also referred to as the Ethernet address).

3 Select the MAX 200Plus you want to configure.

4 Click Configure and the Configure dialog box appears.



5 Type the name of the MAX 200Plus, its IP address and subnet mask.

6 Click OK.

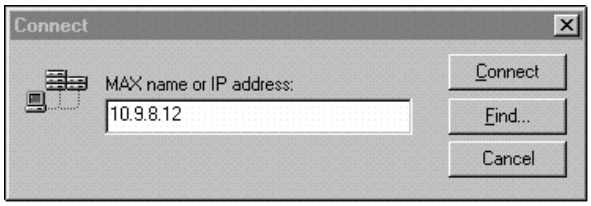
The Management Console software assigns the name, IP address and subnet to the MAX 200Plus. Once the MAX 200Plus has this information, you can proceed to configure it.

Connecting to a MAX 200Plus

To connect to a MAX 200Plus:

1 Start the Management Console application.

The Connect dialog box appears.



2 In the Connect dialog box, enter the name or IP address of the MAX 200Plus you want to connect to.

3 Click Connect.

When you connect to a MAX 200Plus, the Management Console downloads the MAX 200Plus configuration file to your PC. None of the configuration changes you make the MAX 200Plus take effect until you Update the MAX 200Plus with the configuration file using the Update command from the MAX menu.

While the Management Console is downloading this configuration file, a status message appears confirming the data transfer, and the MAX Info tab appears. You can now proceed to configure your MAX 200Plus.

Overview of configuring the MAX 200Plus

You must enter various types of information in the following tabs to fully configure the MAX 200Plus:

- The MAX Info tab allows you to configure the information that identifies the MAX 200Plus as well as the encapsulation protocols and authentication for incoming calls.
- The Protocols tab allows you to configure routing and bridging protocols for the MAX 200Plus.

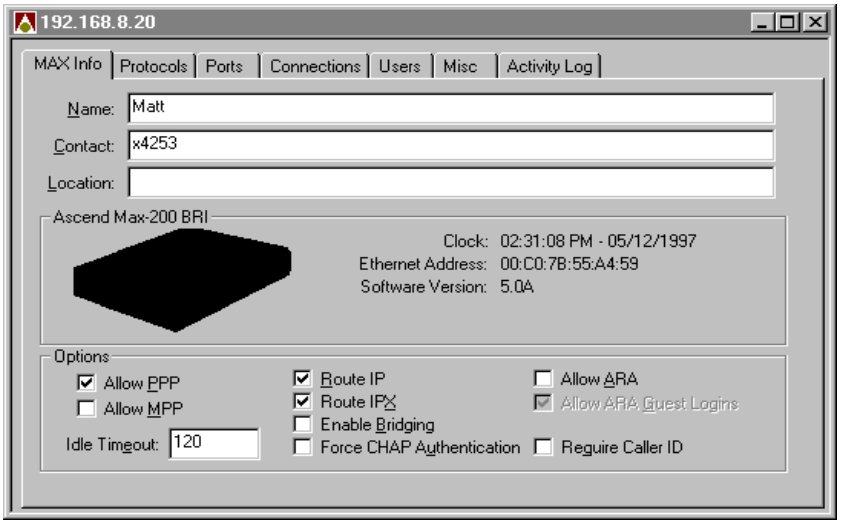
- The Ports tab displays the status of the PC Cards installed on your MAX 200Plus and allows you to configure BRI cards.
- The Connections tab allows you to configure dial-in and dial-out connections. The Connections tab is typically used to configure network-to-network connections.
- The Users tab allows you to configure the MAX 200Plus userlist by assigning names and passwords to callers dialing into the MAX 200Plus. The Users tab is typically used to configure network-to-network connections.
- The Misc tab allows you to configure the terminal server.

Configuring MAX information

After you connect to the MAX 200Plus, a Management Console window appears, displaying a MAX Info tab. Use this tab to:

- enter the name and location of the MAX 200Plus
- enter the name of the system administrator
- select bridging and routing for incoming calls to the MAX 200Plus
- select encapsulation type for incoming and outgoing calls
- view the MAX 200Plus software version
- view the MAX 200Plus Ethernet (MAC) address
- set the idle timeout

To configure MAX information, click the MAX Info tab.



Configuring general MAX 200Plus information

In the MAX Info tab, enter the following information:

- **Name**: The MAX 200Plus name.

  The system name assigned to the MAX 200Plus must *exactly* match the station name on the remote end of a network-to-network connection.
- **Contact**: The name of the system administrator.
- **Location**: The location of the MAX 200Plus.

Configuring incoming call options

Use the Options area in the MAX Info tab to configure incoming call options.

Many of these options have corresponding entries for individual connections in the Connection tab. You must enable any options you are going to use for incoming calls using the MAX Info tab, but you can disable these options for individual connections when you define the connections in the Connections tab.

Enter the appropriate incoming call options:

- **Allow PPP**: Use this for dial-in users.

  The client must be running PPP client software to connect to an IP or IPX network through the MAX 200Plus.

- **Allow MPP**: Provides dynamic bandwidth allocation.
- **Idle Timeout**: Identifies length of time a connection remains active when there is no data transfer in progress.
- **Route IP**: Enables IP routing for incoming connections.

  Both sides of the connection must support IP.

- **Route IPX**: Enables IPX routing for incoming connections.

  Both sides of the connection must support IPX.

- **Enable Bridging**: (network-to-network connections only) Allows bridging for all connections that the MAX 200Plus answers or dials.
- **Allow ARA**: Use this to connect to an AppleTalk network.

  The MAX 200Plus only supports ARA connections over a modem.

- **Allow ARA Guest Login**: Use this for anonymous login for ARA calls.
- **Force CHAP Authentication**: Requires CHAP authentication for incoming calls.
- **Require Caller ID**: Verifies the origin of a call.

  If an incoming call does not have caller ID, the MAX 200Plus drops the call.

Keep in mind

This section explains how a the MAX 200Plus operates when both bridging and routing are enabled on a connection.

IP routing

The effect of the Route IP option depends upon how you set the Enable Bridging option:

- If Enable Bridging is selected and Route IP is not selected, the MAX 200Plus bridges all packets.
- If Enable Bridging is not selected and Route IP is selected, the MAX 200Plus routes only IP packets.
- If Enable Bridging is not selected and Route IP is not selected, an error occurs and you cannot save the profile.

  You must enable bridging or routing, or both.
- IP routing must be enabled on both the dialing and answering sides of the link. Otherwise, the MAX 200Plus does not route IP packets.

Note: If UNIX clients access NetWare servers via TCP/IP (rather than UNIXWare), the MAX 200Plus must also be configured as a bridge or IP router. Otherwise, TCP/IP packets will not make it across the connection.

IPX routing

If the link supports PPP or MPP, both sides of the connection must enable Route IPX for IPX routing to take place.

In addition, the effect of the Route IPX option depends upon how you set the Enable Bridging option:

- If Enable Bridging is selected and Route IPX is selected, the MAX 200Plus routes IPX packets, and bridges all other packets.

  If a connection has both bridging and IPX routing enabled in the same connection, the MAX 200Plus can only route a single IPX frame type, and it will bridge any other IPX packet frame types.
- If Enable Bridging is selected and Route IPX is not selected, the MAX 200Plus bridges all packets.

- If Enable Bridging is not selected and Route IPX is selected, the MAX 200Plus routes only IPX packets.

  The MAX 200Plus can route only one packet frame type, and it routes and spoofs IPX packets only if they are encapsulated in that frame.
- If Enable Bridging is not selected and Route IPX is not selected, an error occurs and you cannot save the profile.

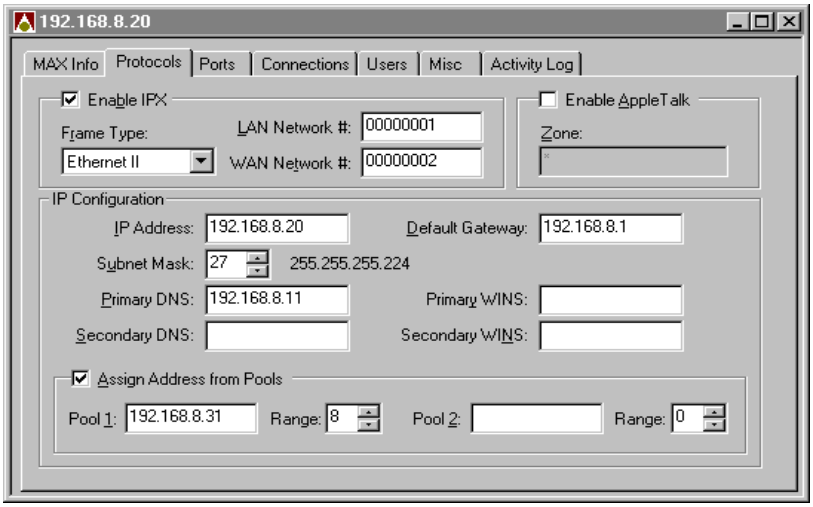
  You must enable bridging or routing, or both.

Configuring protocols

The Protocols tab allows you to configure the routing and bridging the MAX 200Plus. Use this tab to:

- configure IPX
- configure AppleTalk
- configure IP

To configure protocol information, click the Protocols tab.



Configuring IPX

Enter the appropriate information:

- **Enable IPX**: Allows IPX routing.
- **Frame Type**: (Used for bridging and routing.) Identifies the Ethernet frame type. The MAX 200Plus can only route or bridge the frame type you specify here.
- **LAN Network #**: (Used only for routing.) Identifies the local Ethernet network.

  When you accept the default setting of 00000000, the MAX 200Plus learns its IPX network number from other routers on the Ethernet network.
- **WAN Network #**: This is the IPX network number assigned to all PPP clients dialing into the MAX 200Plus.

Configuring AppleTalk

Enter the appropriate information:

- **Enable AppleTalk**: Allows AppleTalk communication.
- **AppleTalk Zone**: Identifies the network zone name.

  The default zone for this parameter is * which identifies the zone you are currently in.

Configuring IP

Enter the appropriate information:

- **IP Address**: Identifies the MAX 200Plus IP address.
- **Subnet Mask**: Identifies the subnet mask number.

  If the MAX 200Plus is connected to a local subnet and will connect to a remote subnet of the *same* IP network, both sides of the connection must use the same subnet mask.
- **Primary and Secondary DNS**: Identifies the IP addresses of the primary and secondary DNS servers.
- **Default Gateway**: Identifies the IP address of the router functioning as the default gateway.
- **Primary and Secondary WINS**: Identifies the IP addresses of the primary and secondary WINS servers.
- **Assign Address from Pools**: Enables use of a designated address pool. If an incoming caller is not configured to accept dynamic addresses, the connection is not established.
- **Pool 1** and **Pool 2**: Identifies the first IP address in the address pool.
- **Range**: Identifies the range of addresses in the pool.

Configuring ports

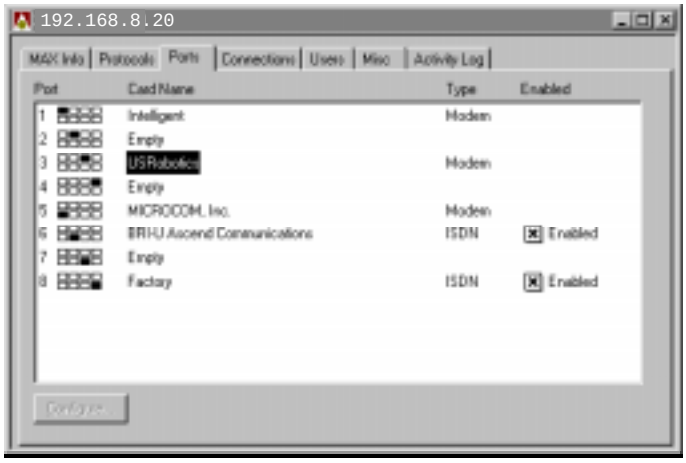
Use the Ports tab to:

- identify port location in the MAX 200Plus
- identify the card name, type, and status (enabled/disabled)
- enable and disable ISDN BRI cards
- configure BRI cards

Note: You cannot configure modem settings using the Management Console.

Viewing port information

To view port and card information, click the Ports tab:



Note: Refer to Appendix C if the Console slot numbering does not accurately reflect the actual numbering on the MAX 200Plus.

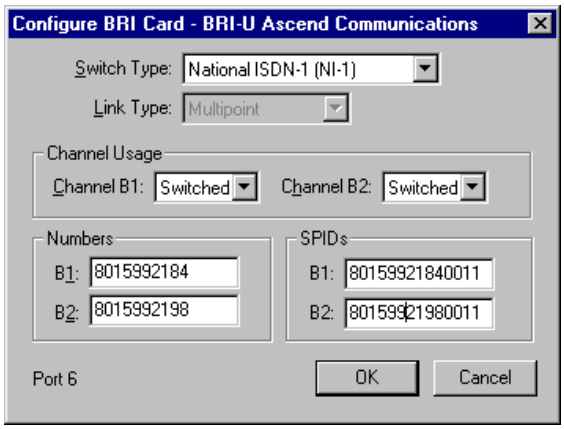
Configuring BRI cards

Note: You must get the information BRI card configuration information from your ISDN service provider. Your BRI card must be correctly configured in order to operate correctly.

To configure a BRI Card:

1 Highlight the BRI card you want to configure, then click Configure.

The Configure BRI Card dialog box appears.



2 Enter the appropriate information:

- **Switch Type**: Identifies the type of ISDN switch your ISDN line is connecting to.
- **Channel B1** and **Channel B2**: Identifies how the channels are used.

  In most cases, select Switched. Leased is used for permanent connections.
- **Numbers**: Identifies phone numbers for primary and secondary numbers for lines BI and B2.
- **SPIDs**: Identifies numbers for primary and secondary SPID numbers for lines BI and B2.

3 Click OK to save your changes.

Configuring connections

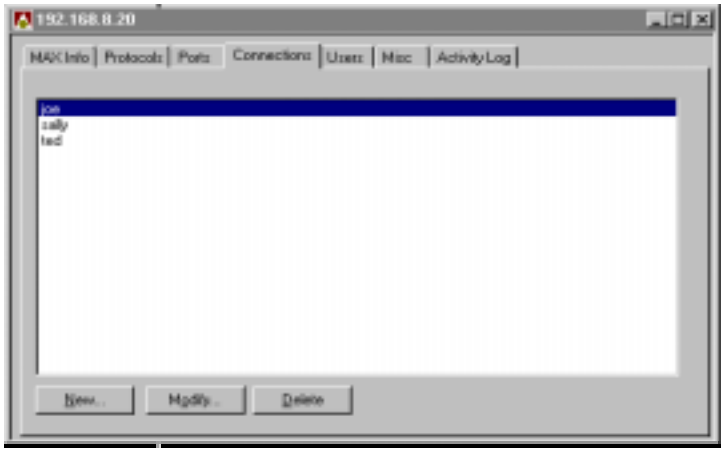
The New/Modify Connections tab provides options for network-to-network connections for networking devices. Use this tab to:

- enter the station name
- configure bridging
- configure the idle timeout
- configure the service type and encapsulation
- if enabled, configure dial-in security information
- if enabled, configure dial-out security information
- configure the protocols used for this connection

Note: The parameters contained in the General and Protocol Options tabs apply specifically to the connection identified by its station name. In addition, you must enable any options you are going to use for a connection in the MAX Info tab.

To configure dial-in and dial-out connections:

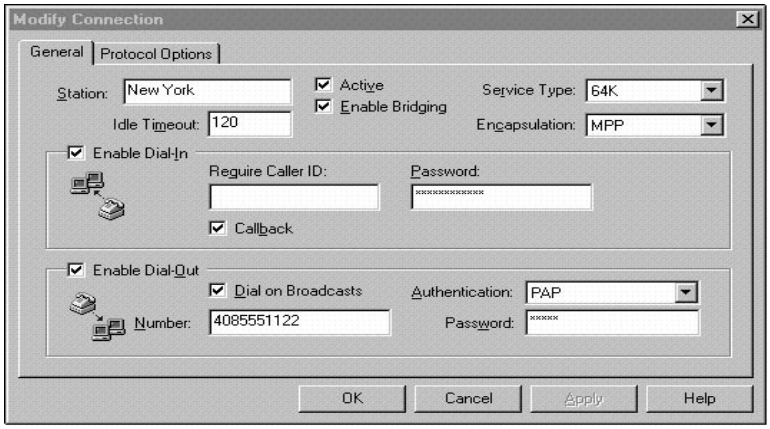
1 Click the Connections tab.



2 To create a new connection, click New.

To modify an existing connection, highlight an existing connection and click Modify.

The New/Modify Connections tab appears.



Configuring general options

Enter the appropriate information:

- **Station**: Identifies the origin or destination of a call connection.

  Use the same name on the other end of the call for authentication.

- **Idle Timeout**: Identifies length of time a connection remains active when there is no data transfer in progress.

  The length of time assigned here overrides the time specified in the MAX Info tab.

- **Active**: Activates the connection for use.
- **Enable Bridging**: Allows bridging for this connection.
- **Service Type**: Identifies the type of service for the connection.

  Choose: 56K, 56K Restricted, or Modem

- **Encapsulation**: Identifies the type of encapsulation.

  Choose: PPP, MPP, or ARA

Configuring Dial-In options

Enter the appropriate information:

- **Enable Dial-In**: Allows incoming calls.
- **Require Caller ID**: Use this option to require line identification and type the caller's ID.
- **Callback**: Use this option to activate the callback process.

  If you choose this option, the MAX 200Plus hangs up after receiving an incoming call that matches a previously entered number and then calls back the device at the remote end of the connection.

  This option increases security, ensuring that the MAX 200Plus always makes a connection with a known destination.
- **Password**: Validates the incoming call.

  This option identifies the password that is sent by the remote node. If this password does not match the password sent by the remote node, the MAX 200Plus disconnects.

Configuring Dial-Out options

Enter the appropriate information:

- **Enable Dial-Out**: Allows outgoing calls.
- **Dial on Broadcasts**: Allows broadcast packets to initiate dialing. (For bridging only.)
- **Number**: Identifies the phone number used to reach the bridge, router, or node at the remote end of the connection.
- **Authentication**: Identifies the type of authentification you want to use.

  Both sides of a connection must agree on the type of authentication used for the connection.
- **Password**: Identifies the password used to verify outgoing calls.

When you are done entering information and choosing options, choose the OK button to save your changes, or click the Protocol Options tab to configure the protocols for the connection.

Configuring connection protocol options

Use Protocol Options tab to:

- configure IPX
- configure IP

Configuring IPX

Enter the appropriate information:

- **Route IPX**: Enables IPX routing for this connection.

  Route IPX must also be selected in the MAX Info tab.

- **Dial on Query**: Use this option if you are setting up a workstation to look for a server across the connection.

  When ON, the MAX 200Plus dials the dial-out number in the General tab when a workstation on the local IPX network looks for the nearest IPX server.

  Dial on Query has no effect if there are any servers in the MAX 200Plus unit's routing table, either from an IPX connection or learned through RIP.

- **Handle IPX for**: Use this to select IPX filtering.

  Choose: Clients Only or Servers (and Clients)

  This option will not do any filtering unless you select an IPX frame type.

  Spoof: Indicates the length of time, in minutes, to perform watchdog spoofing.
- **IPX Net #**: Identifies the Ethernet network number.

Configuring IP

Enter the appropriate information:

- **Route IP**: Enables IP routing for this connection.

  Route IP must also be selected in the MAX Info tab.
- **LAN Address**: Identifies the IP address of a station or router at the remote end of the connection.
- **Subnet mask**: Identifies the subnet mask number.
- **Metric**: Identifies the number of hops allowed across a connection.
- **LAN**: Sets up RIP only on the LAN side of the connection.

  You must turn on Route IP before you can use this option.
- **WAN**: Sets up RIP only on the WAN side of the connection.

  You must turn on Route IP before you can use this option.
- **Address Pool**: Indicates use of IP address pool 1 or 2.

When you are done entering information and choosing options, choose the OK button to save your changes.

Keep in mind

The Management Console uses the following subnet mask defaults:

Class	Address range	Netmask 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
Class D	224.0.0.0 → 239.255.255.255	N/A
Class E (reserved)	240.0.0.0 → 247.255.255.255	N/A

Configuring users

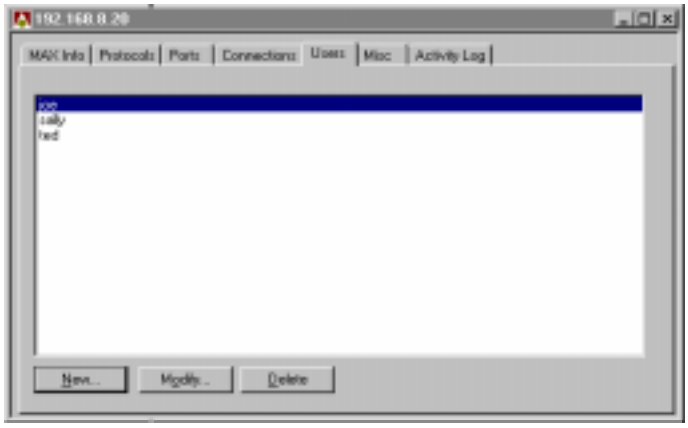
The Users tab displays a list of current users. Use this tab to:

- view user names
- set up new users and enter their passwords

To configure users:

1 Click the Users tab.

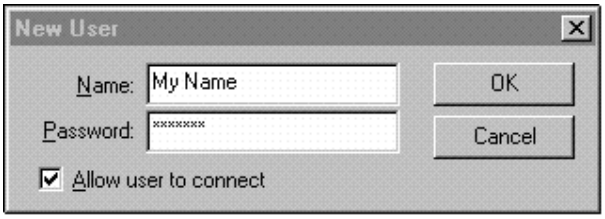
The Users dialog box appears.



2 To create a newuser, click New.

To modify an existing user, highlight an existing user and click Modify.

The New/Modify Users dialog box appears.



3 Enter the appropriate information:

Name: Identifies the user.

Because the MAX 200Plus uses the name for authentication, you must type it exactly as the remote network expects it. In this case, Name is case sensitive.

Password: Validates the incoming call.

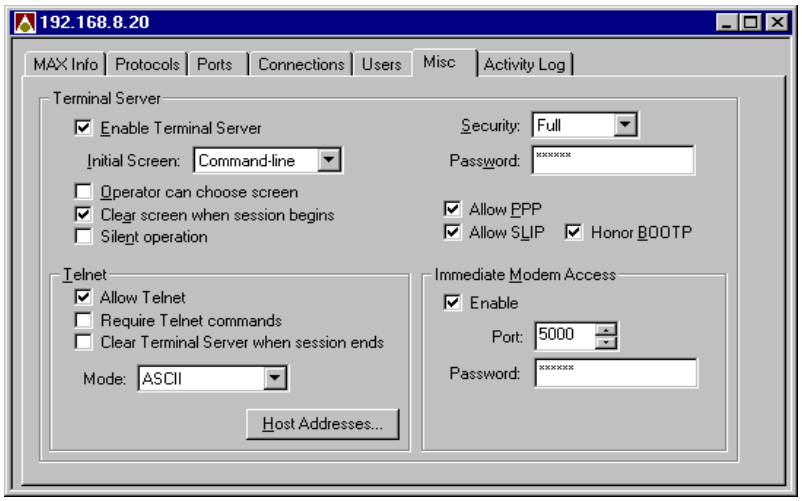
You can enter up to 20 alphanumeric characters. This password only applies if Force CHAP Authentication is selected in the MAX Info tab.

Allow user to connect: Allows the user to connect to the MAX 200Plus.

4 Click OK.

Configuring the terminal server

The Miscellaneous tab provides options to define the terminal server.



Configuring the Terminal Server

Enter the appropriate information:

- **Enable Terminal Server**: Enables or disables terminal services.
- **Initial Screen**: Specifies the type of user interface displayed at the start if a dial-in terminal server connection.

  Select Command-line or Menu.
- **Operator can choose screen**: Specifies whether an interactive user is allowed to switch between command line mode and menu mode.

  Select Yes or No.
- **Clear screen when session begins**: Specifies whether the screen clears when a terminal server session begins.

  Select Yes or No.
- **Silent operation**: Suppresses status messages when interactive users establish a terminal server connection.

  Select Yes or No.

Configuring Telnet

Enter the appropriate information:

- **Allow Telnet**: Enables or disable the Telnet command from the terminal server interface.

  Select Yes or No. The default is No.

- **Require Telnet commands**: Specifies whether the MAX interprets a command that does not include a keyword or hostname for a Telnet command.

  Select Yes or No.

- **Clear Terminal Server when session ends**: Specifies whether the dial-in connection clears when an interactive Telnet, Rlogin, or TCP session terminates.

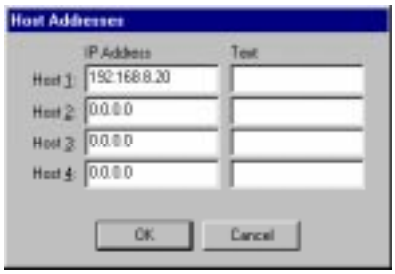
- **Mode**: Specifies the default Telnet mode terminal service Telnet users.

  Select ASCII, Binary, or Transparent.

- **Host Addresses**:

  – For Ip addresses: Specifies the IP address of the first, second, third, and fourth hosts listed in the terminal server menu-mode interface.

  – For text: Specifies a text description of the first, second, third and fourth hosts listed in the terminal server menu-mode interface.



- **Security**: Enables terminal server security.

  Select Full, Partial, or None.

- **Password**: Specifies the terminal server password.

  Specify up to 20 characters.

- **Allow PPP**: Enables the terminal server users to initiate a framed PPP session from the terminal server command line interface.
- **Allow Slip**: Specifies whether a SLIP (Serial Line IP) session can be invoked from the terminal server command line.

  Select Yes or No.
- **Honor Bootp**: Specifies whether the MAX responds to BOOTP within SLIP sessions.

  Select Yes or No.

Immediate Modem Access

Enter appropriate information:

- **Enable** (Immediate Modem): This parameter enables or disables the Immediate Modem service.
- **Port**: Specifies the port number for Immediate Modem dialout. It tells the MAX 200Plus that all Telnet sessions initiated with that port number want modem access.

  Specify a port number (5000–65535). The default is 5000.
- **Password**: Specifies a password required to dialout using the Immediate Modem service.

  Specify up to 64 characters.

You have now completed the basic configuration of your MAX 200Plus. Before any of these changes can take effect, however, you must save your configuration and update the MAX 200Plus as explained in the next section.

Saving your configuration and updating the MAX 200Plus

When you have completed all entries in the MAX Info, Protocols, Connections, Ports, Users and Miscellaneous tabs, you must save your configuration and update the MAX 200Plus with this new information.

Note: Any existing configuration information on the MAX 200Plus is overwritten by the new configuration.

To save the MAX 200Plus configuration:

- Select Save from the MAX menu.

  This saves the configuration to your hard disk. You can use this as a backup of your configuration, or to apply this configuration to another MAX 200Plus (as explained in Chapter 3, "MAX 200Plus System Administration.")

To update the MAX 200Plus configuration:

- Select Update from the MAX menu.

  This applies the configuration changes you have made to the MAX 200Plus.

  A status message appears confirming the data transfer.

Where to go next

Chapter 3, "MAX 200Plus System Administration," explains how to maintain your MAX 200Plus, including how to change the Management Console password, upgrade the software, and manually place and hang up calls using the Telnet interface.

Chapter 4, "Example Configurations," provides example bridging, IP routing, and IPX routing configurations. They provide more detail about how some of the MAX 200Plus options work together.

Chapter 5, "Reference," contains complete details on the MAX 200Plus options.

MAX 200Plus System Administration

3

This chapter explains how to perform basic system administration tasks on your MAX 200Plus.

This chapter contains these sections:

Updating the MAX 200Plus with another MAX 200Plus configuration

You can update a MAX 200Plus with an existing configuration file by using the Update To command from the MAX menu.

Note: When you update one MAX 200Plus with the configuration of another MAX 200Plus, it replaces any IP or IPX configuration information on the target MAX 200Plus with the IP or IPX configuration of the source MAX 200Plus. This could cause problems with your network configuration, since two different devices will be sharing the same information. We recommend that if you use the Update To command, you first change any IP or IPX configuration information.

To apply the configuration of one MAX 200Plus to another:

1. Open the configuration file by selecting Open Configuration File from the File menu.
2. Select Update To and the Connect dialog box appears.
3. Type the domain name, or IP address MAX 200Plus you want to configure with this configuration file
4. Click Connect.

   The configuration file is downloaded to the MAX 200Plus you specified.

Backing up your configuration files

If you want to keep a configuration file located on disk for backup in a location other than the default location (C:\ASCEND\Max200), on the File menu, click Save As and enter another location for the backup file.

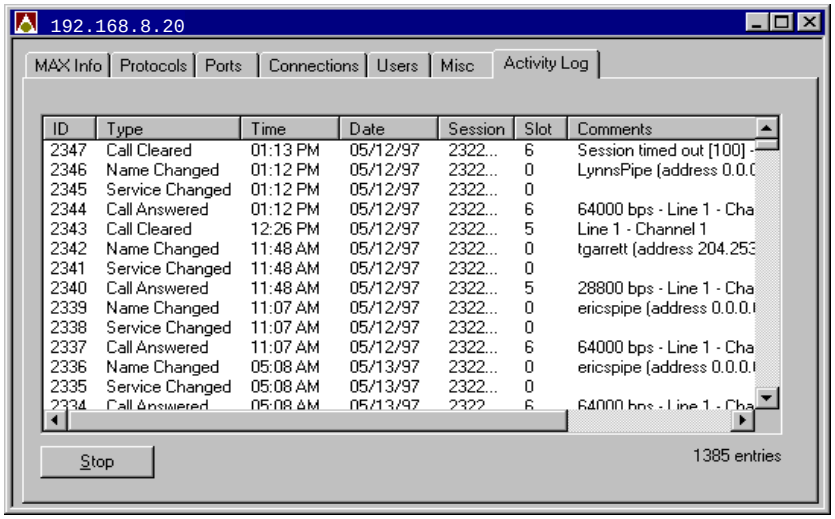
Using the Activity Log

The Activity Log lists a detailed history of messages sent to and from the MAX 200Plus. You can print or save the log entries (in tab-delimited text). Use this tab to:

- view the type of activity, time, date, session identification, slot location and comments.

1 Select the Activity Log tab in the MAX window to display the Activity Log window.

The log displays the activity that has taken place on the MAX 200Plus.



2 Click Refresh to update the display and get the most recent activity.

Network activity is being monitored from the MAX 200Plus and the information is not displayed in the window until you choose Refresh.

3 To save the log, select File menu, click Save.

If you want to save the log in a location other than the default location (C:\ASCEND\Max200), on the File menu, click Save Activity Log As, and choose a location to save the file.

The file is saved in tab-delimited format that you can open in a spreadsheet, database, or word processing application.

4 To print the log, on the File menu, click Print.

Changing the password

The MAX 200 Plus Administrator's Console is password protected to protect your MAX 200Plus from unauthorized access. By default, the password is a null string (that is, there is no password). We highly recommend you change this password as soon.

Note: The MAX 200 Plus Administrator's Console password is also used to restrict Telnet access.

To change the MAX 200 Plus Administrator's Console password

1 Select Set Password from the MAX menu.

2 Enter the password needed to access the MAX 200Plus MAX 200 Plus Administrator's Console.

You can enter up to 20 alphanumeric characters.

3 Click OK.

Accessing the Telnet interface

In addition to the Management Console, you can configure the MAX 200Plus using the Telnet interface. You can perform most of the configuration necessary to successfully operate your MAX 200Plus using the Management Console. However, you must use the Telnet interface if you want to configure:

- perform a software update as explained in "Upgrading the MAX 200Plus software" on page 3-6
- manually place or hang up calls as explained in "Manually dialing out from the MAX 200Plus" on page 3-5
- use a Remote Authentication Dial-In User Service (RADIUS) server
- configure security card authentication for incoming users
- add filtering
- add static Routes

- configure the MAX 200Plus as a terminal server
- fine tune the dynamic bandwidth allocation (DBA) parameters
- monitor routing and bridging tables
- monitor the MAX 200Plus traffic
- fine tune Routing Information Protocol (RIP)

To access the Telnet interface, set your terminal to VT-100 mode and telnet to the MAX 200Plus.

The *MAX 200Plus Supplemental Documentation Set* contains complete instructions for using the Telnet interface.

Manually dialing out from the MAX 200Plus

The Management Console does not allow you to manually place or hang up calls. To do this you must use the Telnet interface. Manually placing and hanging up calls is explained in detail in the *MAX 200Plus Supplemental Documentation Set*. This section, however, provides a quick reference on how to do this.

Before you can manually place a or hang up a call, the Connection profile for that call must be open. Connection profiles can be created either through the Connections tab or through the Telnet interface. Any connection you defined using the Management Console will appear as a Connection profile in the Telnet interface.

To manually place a call:

1 Select Ethernet, then press Enter.

2 Select Connections, then press Enter.

A list of all the connections you have defined on the MAX 200Plus appears.

3 Select the Connection profile for the destination you want to call.

Use the arrow keys or Control-N (next) or Control-P (previous) to select the profile.

4 Press Enter to open the Connection profile.

5 Press Ctrl-D to invoke the DO menu.

```
10-101 brian-gw
DO...
>0=ESC
 1=Dial
 P=Password
```

6 Press 1 (or select 1=Dial) to invoke the Dial command.

Watch the information in Sessions status window on the right side of the screen. You should see the number being called, followed by a message that the network session is up.

To manually clear a call:

1 Open the active Connection profile you want to clear.

2 Press Ctrl-D to open the DO menu.

When you open the DO menu for an active session, it looks similar to this one:

```
10-200 5105559999
DO...
>0=ESC
 2=Hang Up
 P=Password
```

3 Press 2 (or select 2=Hang Up) to invoke the Hang Up command.

The status window will indicate when the call has been terminated.

Upgrading the MAX 200Plus software

To update the MAX 200Plus system software, you must use Trivial File Transfer Protocol (TFTP).

Before you begin make sure:

- You have a properly configured TFTP server
- you have the system software file stored on the TFTP server. For example:

  `/tftpboot/ascend.bin`

To access the TFTP command:

1 From the MAX 200Plus Telnet interface, access the debug monitor by typing these characters in rapid succession:

```
Esc [ Esc =
```

2 At the > prompt, type:

```
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.

For example, the command:

```
tloadcode tftp-server ascend.bin
```

will load a new the new software ascend.bin into flash from the machine named tftp-server. The current configuration is also saved to flash before new code is received, as a precaution. Upon the next reset, the new code will be run out of DRAM. If necessary, the saved configuration will be loaded and a second reset performed automatically.

Where to go next

Chapter 4, “Example Configurations,” provides example bridging, IP routing, and IPX routing configurations. They provide more detail about how some of the MAX 200Plus options work together.

Chapter 5, “Reference,” contains complete details on the MAX 200Plus options.

Example Configurations

4

This chapter provides example MAX 200Plus bridging, IP routing, and IPX routing configurations.

This chapter contains these sections:

Planning a bridging connection

This section describes how to get the local information you need, and shows how to plan a bridging configuration using PPP encapsulation.

How a bridging connection is established

The MAX 200Plus uses station names and passwords to sync up a bridging connection, as shown in Figure 4-1.

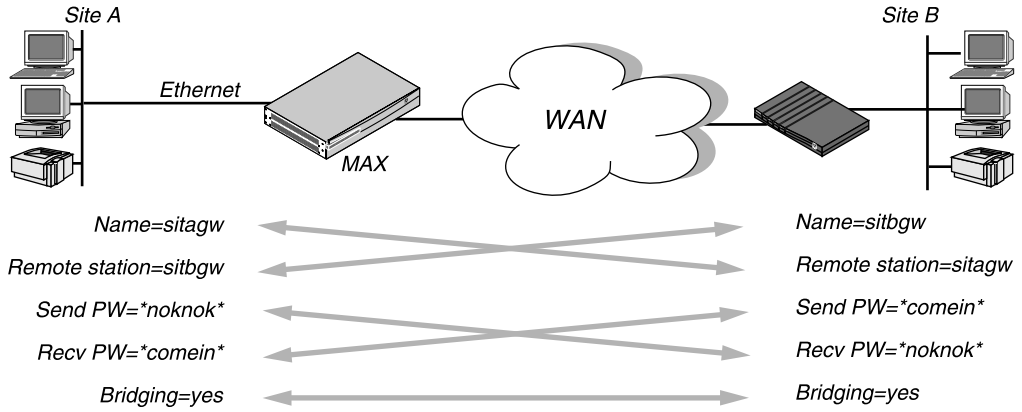


Figure 4-1. Negotiating a bridge connection (PPP encapsulation)

The system name assigned to the MAX 200Plus in the MAX Info tab must *exactly* match the device name specified in the Connection tab on the remote bridge, including case changes. Similarly, the name assigned to the remote bridge must exactly match the name specified in the Station field of a connection on the local MAX 200Plus, 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 200Plus or the remote device. Often case changes are not specified, or a dash, space, or underscore is not entered.

An example bridging connection

In this example, site A wants to set up a connection that enables a user at site B to open an AppleTalk Remote Access (ARA) connection into the site A network. Both site A and site B support the CHAP (Challenge Handshake Authentication Protocol) and require passwords for entry.

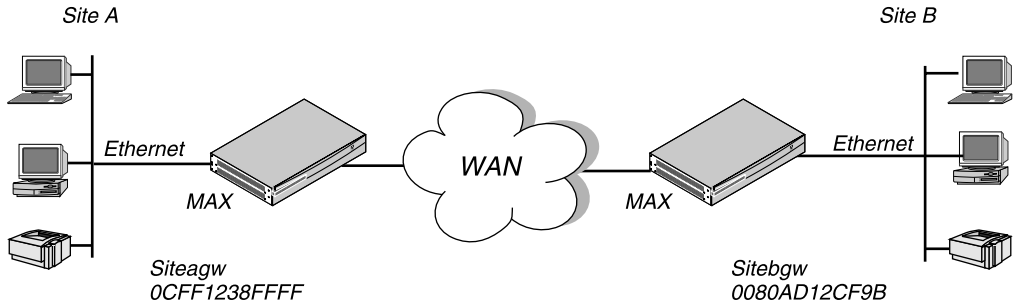


Figure 4-2. An example bridge connection

The site A MAX 200Plus bridging configuration is shown in Table 4-1.

Table 4-1. Bridging configuration for site A

Location	Parameter	Explanation
MAX Info tab	Name=SiteA	This is the name of the MAX 200Plus at Site A. This name must be entered in the Station field (in the Connections tab) of the MAX 200Plus at Site B.
MAX Info tab	Enable Bridging=Yes	This globally enables bridging on the MAX 200Plus
Protocol tab	Enable IPX=Yes	This allows you to select an frame type for the bridging connection.
Protocol tab	Frame Type=frame type of the network	The MAX 200Plus can only bridge the frame type selected here.

Table 4-1. Bridging configuration for site A (continued)

Location	Parameter	Explanation
Connections→General tab	Enable Bridging=Yes	This enables bridging for this connection
Connections→General tab	Dial on Broadcast=Yes	This tells the MAX 200Plus to bring up an inactive connection whenever it receives a broadcast packet.
Connections→General tab	Authentication=PAP (or CHAP)	This is the authentication used for the connection. It must be the same on both sides of the connection.
Connections→General tab	Dial-In Password	This is the password the MAX 200Plus at Site B will send to authenticate the call.
Connections→General tab	Dial-Out Password	This is the password MAX 200Plus at Site A will send to authenticate the call.
Connections→Protocol tab	Route IPX=No	This turns off IPX routing for this connection; the MAX 200Plus will bridge IPX packets defined in the MAX Protocol tab.
Connections→Protocol tab	Handle IPX for=Client	With this setting the MAX 200Plus applies a data filter that discards IPX Routing Information Protocol (RIP) and Service Advertisement Protocol (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.

The configuration for the site B unit is shown in Table 4-2.

Table 4-2. Bridging configuration for site B

Location	Parameter	Explanation
MAX Info tab	Name=SiteB	This is the name of the MAX 200Plus at Site B. This name must be entered in the Station field (in the Connections tab) of the MAX 200Plus at Site A.
MAX Info tab	Enable Bridging=Yes	This globally enables bridging on the MAX 200Plus
Protocol tab	Enable IPX=Yes	This allows you to select an frame type for the bridging connection.
Protocol tab	Frame Type=frame type of the network	The MAX 200Plus can only bridge the frame type selected here.
Connections→General tab	Enable Bridging=Yes	This enables bridging for this connection
Connections→General tab	Dial on Broadcast=Yes	This tells the MAX 200Plus to bring up an inactive connection whenever it receives a broadcast packet.
Connections→General tab	Authentication=PAP (or CHAP)	This is the authentication used for the connection. It must be the same on both sides of the connection.
Connections→General tab	Dial-In Password	This is the password the MAX 200Plus at Site A will send to authenticate the call.
Connections→General tab	Dial-Out Password	This is the password MAX 200Plus at Site B will send to authenticate the call.
Connections→Protocol tab	Route IPX=No	This turns off IPX routing for this connection; the MAX 200Plus will bridge IPX packets defined in the MAX Protocol tab.

Table 4-2. Bridging configuration for site B (continued)

Location	Parameter	Explanation
Connections→Protocol tab	Handle IPX for=Client	With this setting the MAX 200Plus applies a data filter that discards IPX Routing Information Protocol (RIP) and Service Advertisement Protocol (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.

IPX client bridging

Note: If the local network supports NetWare clients *and no NetWare servers*, you want to enable a client to bring up the WAN connection by querying (broadcasting) for a NetWare server on a remote network. To do this when you are bridging an IPX connection, use the settings shown in Table 4-3.

Table 4-3. IPX bridging for local clients only

Location	Parameter	Explanation
MAX Info tab	Name=SiteA	This is the name of the MAX 200Plus at Site A. This name must be entered in the Station field (in the Connections tab) of the MAX 200Plus at Site B.
MAX Info tab	Enable Bridging=Yes	This globally enables bridging on the MAX 200Plus
Protocol tab	Enable IPX=Yes	This allows you to select an frame type for the bridging connection.

Table 4-3. IPX bridging for local clients only (continued)

Location	Parameter	Explanation
Protocol tab	Frame Type=frame type of the network	The MAX 200Plus can only bridge the frame type selected here.
Connections→General tab	Enable Bridging=Yes	This enables bridging for this connection
Connections→General tab	Dial on Broadcast=Yes	This tells the MAX 200Plus to bring up an inactive connection whenever it receives a broadcast packet.
Connections→Protocol tab	Route IPX=No	This turns off IPX routing for this connection; the MAX 200Plus will bridge IPX packets defined in the MAX Protocol tab.
Connections→Protocol tab	Handle IPX for=Client	With this setting the MAX 200Plus applies a data filter that discards IPX Routing Information Protocol (RIP) and Service Advertisement Protocol (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.

IPX server bridging

Note: If the local network supports NetWare servers (or a combination of clients and servers) and the remote network supports NetWare clients only, you want to enable the MAX 200Plus to respond to NCP watchdog requests for remote clients, but to bring down inactive connections whenever possible. To do this when you are bridging an IPX connection, use the settings shown in Table 4-4.

Table 4-4. IPX bridging for local servers

Location	Parameter	Explanation
MAX Info tab	Name=SiteA	This is the name of the MAX 200Plus at Site A. This name must be entered in the Station field (in the Connections tab) of the MAX 200Plus at Site B.
MAX Info tab	Enable Bridging=Yes	This globally enables bridging on the MAX 200Plus
Protocol tab	Enable IPX=Yes	This allows you to select an frame type for the bridging connection.
Protocol tab	Frame Type=frame type of the network	The MAX 200Plus can only bridge the frame type selected here.
Connections→General tab	Enable Bridging=Yes	This enables bridging for this connection
Connections→General tab	Dial on Broadcast=Yes	This tells the MAX 200Plus to bring up an inactive connection whenever it receives a broadcast packet.
Connections→Protocol tab	Route IPX=No	This turns off IPX routing for this connection; the MAX 200Plus will bridge IPX packets defined in the MAX Protocol tab.
Connections→Protocol tab	Handle IPX=Server	With this setting the MAX 200Plus applies a data filter that discards RIP and SAP broadcasts at its WAN interface, but forwards RIP and SAP queries.

Table 4-4. IPX bridging for local servers (continued)

Location	Parameter	Explanation
Connections→Protocol tab	Spoof=30	This is 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." The MAX 200Plus can perform watchdog spoofing only for the IPX frame type specified in the MAX Protocol tab. For example, if IPX Frame=802.3, only connections to servers using that packet frame type will be spoofed.

Servers on both sides of the connection

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 200Plus brings down an inactive WAN connection.

IP Routing

This section provides two examples of common IP routing configurations:

- A host-to-network connection using dynamic IP addressing
- A network-to-network connection

An example host connection via modem

In this example, the MAX 200Plus is connected to a backbone IP network that will communicate with telecommuters via modem. It shows how to add one telecommuter as a host-to-network connection using dynamic address assignment. The MAX 200Plus is configured to assign IP addresses from a

pool and the host software is configured to accept a dynamic address assignment.

You cannot assign a pooled address to most IP routers, because the router already has an address on an existing network. Typically, dynamic address assignment is used for incoming calls from hosts that use a PPP link, although some routers can accept a dynamic address assignment as an alias for a network address.

The user at site B starts up PPP and dials the MAX 200Plus on a modem. The MAX 200Plus answers the call and looks to see if the caller is in the MAX 200Plus user list or has a connection defined.

If it finds a matching connection with no IP address in the LAN Address field (in the Connections Protocol tab), or if it finds the user on its user list, the MAX 200Plus checks for a pointer to a pool of IP addresses and requests that the caller accept the next available IP address from that pool. If the caller accepts the assignment, the connection is established. The MAX 200Plus hangs up if the pool is empty (that is, if all addresses are being used) or if the caller rejects the dynamic address assignment.

Note: When the MAX 200Plus assigns an IP address from a pool, it adds that route to its routing table. The MAX 200Plus then uses RIP to inform the other routers on the local network of this new route.

Figure 4-3 shows a network diagram for this example.

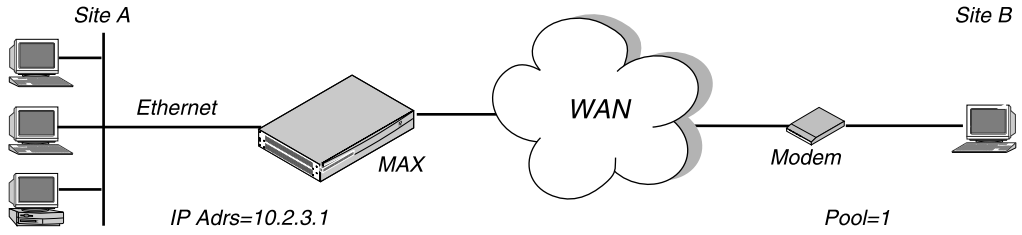


Figure 4-3. Host-to-network connection

In this example, site A is a backbone network and site B is one PC with a modem, TCP/IP stack, and PPP software. The PC will be assigned an address on the local IP network (an address between 10.2.3.10 and 10.2.3.19, as defined in Pool 1).

The configuration of the MAX 200Plus at site A sets the IP routing parameters shown in Table 4-5. (All other IP parameters use the default values.)

Table 4-5. Example IP configuration for incoming modem connection

Location	Parameter	Explanation
MAX Info tab	Route IP=Yes	This enables IP routing for incoming connections
MAX Info tab	Allow PPP=Yes	This allows incoming PPP connections.
MAX Protocol tab	Assign Address from Pools=Yes	This tells the MAX that if a user or a station dials in without an IP address, assign it an IP address from the MAX 200Plus IP address pool.
MAX Protocol tab	Pool 1 (2)	Enter the first address of the IP address pool.
MAX Protocol tab	Range	Select the number of IP addresses in the pool.
MAX Protocol tab	IP Address=10.2.3.1	This is the IP address of the MAX 200Plus.
MAX Protocol tab	Primary DNS=10.2.3.55	This is IP address of the primary Domain Name System (DNS) server on the local network. This allows users to log into network machines using names instead of IP addresses.
MAX Protocol tab	Secondary DNS=10.2.3.4	This is the secondary DNS server. It is used if the primary DNS server is unavailable.
New User dialog box	Name	Enter the name of the remote user.
New User dialog box	Password	Enter the password of the remote user.

Table 4-5. Example IP configuration for incoming modem connection (continued)

Location	Parameter	Explanation
New User dialog box	Allow user to connect=Yes	This enables the user to connect to the MAX 200Plus.

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 200Plus:

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
Baud rate=38400
Hardware handshaking ON
VAN Jacobsen compression ON

An example network-to-network connection

In this example, the MAX 200Plus connects its local network to another remote IP network. Figure 4-4 shows network diagram for this example.

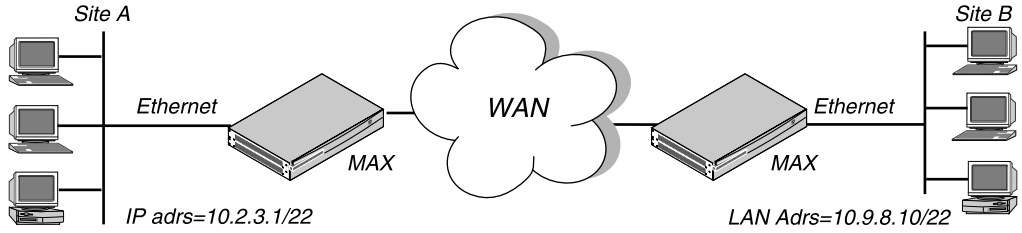


Figure 4-4. Network-to-network connection

The site A MAX 200Plus configuration is shown in Table 4-6. (All other IP parameters use the default values.)

Table 4-6. IP configuration for site A

Location	Parameter	Explanation
MAX Info tab	Name=SiteA	This is the name of the MAX 200Plus at Site A. This name must be entered in the Station field (in the Connections tab) of the MAX 200Plus at Site B.
MAX Info tab	Route IP=Yes	This enables IP routing for incoming connections.
MAX Protocol tab	IP Address=10.2.3.1	This is the IP address of the MAX 200Plus.
MAX Protocol tab	Subnet Mask=22	This is the subnet mask of the MAX 200Plus.
Connection→General tab	Station=SiteB	This is the name of the MAX 200Plus at Site B. It must match the Name (in the MAX Info tab) of the MAX 200Plus at Site B.
Connection→General tab	Service Type= 64K	This is an ISDN connection.
Connection→General tab	Encapsulation=MPP	This allows the MAX 200Plus units on both sides of the connection to combine channels for additional bandwidth when needed.
Connections→General tab	Authentication=PAP (or CHAP)	This is the authentication used for the connection. It must be the same on both sides of the connection.
Connections→General tab	Dial-In Password	This is the password the MAX 200Plus at Site B will send to authenticate the call.
Connections→General tab	Dial-Out Password	This is the password MAX 200Plus at Site A will send to authenticate the call.

Table 4-6. IP configuration for site A (continued)

Location	Parameter	Explanation
Connection→Protocol tab	Route IP=Yes	This enables IP routing for this connection.
Connection→Protocol tab	LAN Address=10.9.8.10	This is the IP address of the remote device.
Connection→Protocol tab	RIP LAN and WAN off	The MAX 200Plus will not use RIP to broadcast the route to the remote network.
MAX Protocol tab	Primary DNS=0.2.3.55	This is IP address of the primary Domain Name System (DNS) server on the local network. This allows users to log into network machines using names instead of IP addresses.
MAX Protocol tab	Secondary DNS=0.2.3.4	This is the secondary DNS server. It is used if the primary DNS server is unavailable.

The site B Ascend unit configuration is shown in Table 4-7. (All other IP parameters can use the default values.)

Table 4-7. IP configuration for site B

Location	Parameter	Explanation
MAX Info tab	Name=SiteB	This is the name of the MAX 200Plus at Site B. This name must be entered in the Station field (in the Connections tab) of the MAX 200Plus at Site A.
MAX Info tab	Route IP=Yes	This enables IP routing for incoming connections.
MAX Protocol tab	IP Address=10.2.3.1	This is the IP address of the MAX 200Plus.

Table 4-7. IP configuration for site B (continued)

Location	Parameter	Explanation
MAX Protocol tab	Subnet Mask=22	This is the subnet mask of the MAX 200Plus.
Connection→General tab	Station=SiteA	This is the name of the MAX 200Plus at Site A. It must match the Name (in the MAX Info tab) of the MAX 200Plus at Site A.
Connection→General tab	Service Type= 64K	This is an ISDN connection.
Connection→General tab	Encapsulation=MPP	This allows the MAX 200Plus units on both sides of the connection to combine channels for additional bandwidth when needed.
Connections→General tab	Authentication=PAP (or CHAP)	This is the authentication used for the connection. It must be the same on both sides of the connection.
Connections→General tab	Dial-In Password	This is the password the MAX 200Plus at Site A will send to authenticate the call.
Connections→General tab	Dial-Out Password	This is the password MAX 200Plus at Site B will send to authenticate the call.
Connection→Protocol tab	Route IP=Yes	This enables IP routing for this connection.
Connection→Protocol tab	LAN Address=10.9.8.10	This is the IP address of the remote device.
Connection→Protocol tab	RIP LAN and WAN off	The MAX 200Plus will not use RIP to broadcast the route to the remote network.

Table 4-7. IP configuration for site B (continued)

Location	Parameter	Explanation
MAX Protocol tab	Primary DNS=10.2.3.55	This is IP address of the primary Domain Name System (DNS) server on the local network. This allows users to log into network machines using names instead of IP addresses.
MAX Protocol tab	Secondary DNS=0.2.3.4	This is the secondary DNS server. It is used if the primary DNS server is unavailable.
MAX Info tab	Route IP=Yes	This enables IP routing for incoming connections.
MAX Info tab	IP Address=10.2.3.1	This is the IP address of the MAX 200Plus.

IPX routing

This section provides two examples of common IPX routing configurations:

- A connection with IPX servers on one side of the connection
- A connection with IPX servers on both sides of the connection

Planning a connection with servers on one side of the link only

In this configuration, the MAX 200Plus is connected to a local IPX network that supports both servers and clients. To plan a connection that allows one or more NetWare clients on a geographically remote network to access the local NetWare servers, read this section.

Note: When the MAX 200Plus will connect to an existing Novell LAN, you need to work with the administrator of that network to obtain network numbers and server-specific information.

Figure 4-5 shows a network diagram for this example.

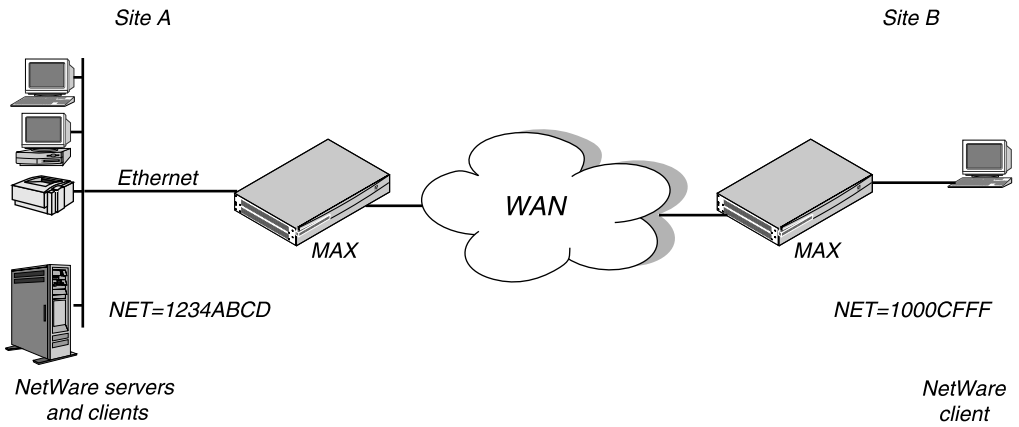


Figure 4-5. Servers on one side of the connection only

In this example, site A supports NetWare 3.12 servers, NetWare clients, and a MAX 200Plus. The NetWare server at site A is configured with this 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 a Pipeline. It is not an existing Novell LAN, so the Pipeline configuration creates a new IPX network (1000CFFF in this example).

Note: The new IPX network number assigned to site B in this example cannot be in use *anywhere* on the entire IPX wide-area network. (It cannot be in use at site A or any network to which site A connects.)

The site A MAX 200Plus configuration is shown in Table 4-8. (All other IPX parameters can use the default values.)

Table 4-8. IPX configuration for site A

Location	Parameter	Explanation
MAX Info tab	Name=SiteAGW	This is the name of the MAX 200Plus at Site A. This name must be entered in the Station field (in the Connections tab) of the MAX 200Plus at Site B.
MAX Info tab	Route IPX=Yes	This enables IPX routing for all incoming connections.
MAX Protocol tab	Enable IPX=Yes	This enables IPX routing for the MAX 200Plus.
MAX Protocol tab	Frame Type=802.3	This is the frame type used on the network.
MAX Protocol tab	LAN Network#=1234ABCD	This specifies a unique IPX network number for the Ethernet interface. The MAX 200Plus assigns an address to a workstation when it connects to the MAX 200Plus; it derives the address from the network number.
Connections→General tab	Station=SiteBGW	This is the name of the MAX 200Plus at Site B. It must match the Name (in the MAX Info tab) of the MAX 200Plus at Site B.
Connections→General tab	Authentication=PAP (or CHAP)	This is the authentication used for the connection. It must be same for both sides.
Connection→General tab	Service Type= 64K	This is an ISDN connection.
Connection→General tab	Encapsulation=MPP	This allows the MAX 200Plus units on both sides of the connection to combine channels for additional bandwidth when needed.

Table 4-8. IPX configuration for site A (continued)

Location	Parameter	Explanation
Connections→General tab	Dial-In Password	Enter the password the MAX 200Plus at Site B will send to authenticate the call.
Connections→General tab	Dial-Out Password	Enter the password MAX 200Plus at Site A will send to authenticate the call.
Connections→Protocol tab	Route IPX=Yes	This enables IPX routing for this connection.

Note: If one of the calling units is set to answer only, only the Dial-In authentication parameters are needed. If a unit is configured to call only, only the Dial-Out authentication is used.

The site B Pipeline configuration is shown in Table 4-9. (All other IPX parameters can use the default values.)

Table 4-9. IPX configuration for site B

Location	Parameter	Explanation
MAX Info tab	Name=SiteBGW	This is the name of the MAX 200Plus at Site B. This name must be entered in the Station field (in the Connections tab) of the MAX 200Plus at Site A.
MAX Info tab	Route IPX=Yes	This enables IPX routing for all incoming connections.
MAX Protocol tab	Enable IPX=Yes	This enables IPX routing for the MAX 200Plus.
MAX Protocol tab	Frame Type=802.3	This is the frame type used on the network.

Table 4-9. IPX configuration for site B (continued)

Location	Parameter	Explanation
MAX Protocol tab	LAN Network#=1000CFFF	This specifies a unique IPX network number for the Ethernet interface. The MAX 200Plus assigns an address to a workstation when it connects to the MAX 200Plus; it derives the address from the network number.
Connections→General tab	Station=SiteAGW	This is the name of the MAX 200Plus at Site A. It must match the Name (in the MAX Info tab) of the MAX 200Plus at Site A.
Connections→General tab	Authentication=PAP (or CHAP)	This is the authentication used for the connection. It must be same for both sides.
Connection→General tab	Service Type= 64K	This is an ISDN connection.
Connection→General tab	Encapsulation=MPP	This allows the MAX 200Plus units on both sides of the connection to combine channels for additional bandwidth when needed.
Connections→General tab	Dial-In Password	This is the password the MAX 200Plus at Site A will send to authenticate the call.
Connections→General tab	Dial-Out Password	This is the password MAX 200Plus at Site B will send to authenticate the call.
Connections→Protocol tab	Route IPX=Yes	This enables IPX routing for this connection.

Table 4-9. IPX configuration for site B (continued)

Location	Parameter	Explanation
Connections→Protocol tab	Dial on Query=Yes	This tells the MAX 200Plus at site B to bring up an inactive connection to the MAX 200Plus at Site A whenever an IPX client at Site B looks for the nearest IPX server. In this example, there are no IPX servers at Site B.

Planning a connection with servers on both sides of the link

In this type of IPX WAN configuration, the MAX 200Plus is connected to an IPX network that supports both servers and clients and will connect with a remote site that also supports both servers and clients. See Figure 4-6.

Note: When the MAX 200Plus will connect to an existing Novell LAN, you need to work with the administrator of that network to obtain network numbers and service-specific information.

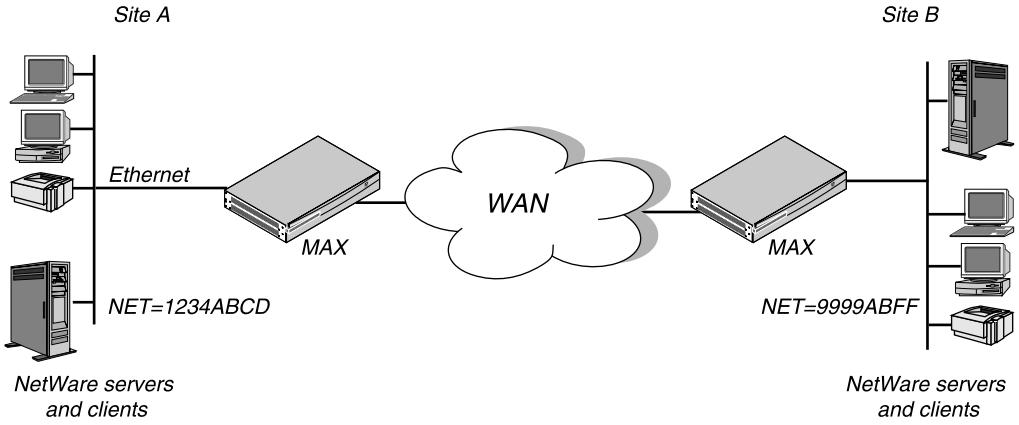


Figure 4-6. Servers on both sides of the connection

You can create an IPX connection with servers on both sides on the connection using the same configuration described in “Planning a connection with servers on one side of the link only” on page 4-16. If you

wanted to create a route to a particular IPX servers on each network, however, you must use the Telnet interface to create an IPX Route profile. Refer to the *MAX ISP and Telecommuting Configuration Guide* in the *MAX Supplemental Documentation Set* for further information.

Note: If one of the calling units is set to answer only, only the incoming authentication parameters are needed. If a unit is configured to call only, only the outbound authentication is used.

Reference

5

This chapter lists the MAX 200Plus options and menu commands that appear in the Management Console in alphabetical order.

Each listing provides information in this format:

Option Name

Description: The Description text explains what the option or command is.

Usage: The Usage text explains how to use the option or command.

Example: The Example text shows you an example setting.

Dependencies: The Dependencies text tells you what other information you need in order to configure and use the parameter.

See Also: The See Also text points you to related options or commands.

Alphabetical parameter listing

Active

Description: This activates or excavates a connection. If you activate a connection, it is available for use. If you deactivate a connection, it is not available for use.

Address Pool

Description: This specifies the address pool that incoming calls use.

Usage: Select an IP address pool to be used for this connection.

Dependencies: Keep this additional information in mind:

- If you do not specify a Pool number, and enable Assign Address from Pools is enabled, the MAX 200Plus gets IP addresses from the first defined address pool.

See Also: Assign Address from Pools, Range Pool 1 (2)

Allow ARA

Description: This specifies whether the MAX 200Plus accepts incoming Appletalk Remote Access (ARA) calls.

Usage:

- Selecting Allow ARA specifies that the MAX 200Plus accepts incoming ARA calls.

  The default is MPP enabled.
- Deselecting Allow ARA specifies that the MAX 200Plus rejects incoming ARA calls.

Dependencies: Allow ARA is not applicable if Enable Appletalk is not selected in the Protocol tab.

See Also: Encapsulation, Allow PPP, Allow ARA Guest Logins, Enable Appltalk.

Allow ARA Guest Logins

Description: This specifies whether the MAX 200Plus allows incoming Appletalk Remote Access (ARA) callers to log in as guests.

Usage:

- Selecting Allow ARA specifies that the MAX 200Plus accepts incoming ARA calls.

  The default is MPP enabled.

- Deselecting Allow ARA specifies that the MAX 200Plus rejects incoming ARA calls.

See Also: Encapsulation, Allow PPP, Allow ARA Guest Logins

Allow MPP

Description: This specifies whether the MAX 200Plus accepts incoming MP or MPP calls. MPP calls typically come from other MAX 200Plus or Pipeline units.

Usage:

- Enabling Allow MPP specifies that the MAX 200Plus accepts incoming MP or MPP calls, provided that they meet all other PPP, MP, or MPP criteria (for example, the password is correct and dynamic addressing, if used, is correctly configured on both the MAX 200Plus and the remote caller.

  The default is MPP enabled.

- Disabling MPP specifies that the MAX 200Plus rejects incoming MP or MPP calls.

See Also: Encapsulation, Allow PPP

Allow PPP

Description: This specifies whether a dial-in client can use asynchronous PPP (Point-to-Point Protocol).

PPP provides a standard means of encapsulating data packets over a single-channel WAN link that a connection sets up. It ensures basic compatibility with non-Ascend devices.

Usage:

- Selecting Allow PPP specifies that the MAX 200Plus accepts PPP calls from dial-in users.
- Deselecting Allow PPP specifies that the MAX 200Plus not accept PPP calls from dial-in users.

  PPP is disabled by default.

See Also: Encapsulations, Allow MPP

Allow Slip

Description: Specifies whether a SLIP (Serial Line IP) session can be invoked from the terminal server command line.

Usage: Specify Yes or No. The default is No.

- Yes enables users to invoke SLIP sessions from the terminal server.
- No disables this use of SLIP.

Dependencies: This parameter does not apply if terminal services are disabled.

See Also: Enable Terminal Server

Allow Telnet

Description: This enables or disables the Telnet command from the terminal server interface.

Usage: Specify Yes or No. The default is No.

- Yes means operators can invoke Telnet sessions from the terminal server interface.
- No disables the use of Telnet in the terminal server.

Dependencies: This parameter is not applicable when terminal services are disabled.

See Also: Enable Terminal Server

Assign Address from Pools

Description: This specifies whether the MAX 200Plus requires the calling station to accept an IP address from an IP address pool.

Assigning an address to a device is called performing dynamic IP. Typically, dynamic IP applies when the calling end is an individual. If the calling end is a router, it usually rejects attempts to perform dynamic IP.

Usage:

- Enabling Assign Address from Pools specifies that the MAX 200Plus requires the calling station to accept an IP address it assigns from a pool.

  If the calling station rejects the assignment, the MAX 200Plus ends the call.

- Disabling Assign Address from Pools specifies that the calling station can reject an IP address assignment and use its own IP address.

  The default is No.

Dependencies: Assign Address from Pools only applies when the calling station uses PPP encapsulation and the Pool 1 text field has a value other than 0.0.0.0.

See Also: Pool 1 (2), Range

Authentication

Description: This specifies the authentication protocol that the MAX 200Plus requests when initiating a connection using PPP or MPP encapsulation. The answering side of the connection determines which authentication protocol the connection uses (if any).

Note: If you use security cards to authenticate remote users, you must use the Ascend Password Protocol (APP) Server utility. This utility allows users to supply token passwords from a PC or UNIX host on the local network. Refer to the *MAX 200Plus Supplemental Documentation Set* or the Ascend Web site for further information about security on the MAX 200Plus.

Usage:

- None specifies that the MAX 200Plus does not request an authentication protocol for outgoing calls.

  The default is None.

- PAP specifies the Password Authentication Protocol, a PPP authentication protocol.

  PAP provides a simple method for the MAX 200Plus to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment, and does not use encryption. The remote device must support PAP.

- CHAP specifies the Challenge Handshake Authentication Protocol, a PPP authentication protocol.

  CHAP is more secure than PAP. CHAP provides a way for the remote device to periodically verify the identity of the MAX 200Plus using a three-way handshake and encryption. Authentication takes place upon initial link establishment; a device can repeat the authentication process any time after the connection is made. The remote device must support CHAP.

- PAP-TOKEN specifies an extension of PAP authentication.

  In PAP-TOKEN, the user making outgoing calls from the MAX 200Plus authenticates his or her identity by entering a password derived from a hardware device, such as a hand-held security card. The MAX 200Plus prompts the user for this password, possibly along with a challenge key.

The NAS (Network Access Server) obtains the challenge key from a security server that it accesses through RADIUS.

RADIUS (Remote Authentication Dial In User Service) is a protocol by which users can have access to secure networks through a centrally managed server. You can store virtually all Connection Profile information on the RADIUS server in a flat ASCII database.

- PAP-TOKEN-CHAP specifies a type of authentication almost identical to PAP-TOKEN.

  In all authentication protocols, including PAP-TOKEN and PAP-TOKEN-CHAP, the MAX 200Plus individually authenticates all channels of an MPP call. If the answering unit requires security card authentication, PAP-TOKEN and PAP-TOKEN-CHAP begin identically when authenticating the first channel of an MPP call. However, when the MAX 200Plus adds additional channels to the MPP call, PAP-TOKEN requires security-card authentication for each new channel, while PAP-TOKEN-CHAP uses CHAP authentication for all new channels. CHAP authentication works automatically, without the use of a hand-held security card.

- CACHE-TOKEN begins authentication using a hand-held security card, and fills a token cache set up for you on the RADIUS server.

  CHAP authenticates your subsequent calls without using your hand-held security card. After a period of time configured in your entry in the RADIUS users file, the token cache expires and the next call you place must again be authenticated using your hand-held security card.

Dependencies: Keep this additional information in mind:

- The link must use PPP or MPP encapsulation (Encapsulation set to PPP or MPP).
- If you request PAP or CHAP, you must also specify a password in the Dial-Out Password field.
- If you request PAP-TOKEN-CHAP, you must enter an auxiliary password in the Password field. This password must match the password in the RADIUS entry for authenticating the call.

  If you do not enter identical passwords in the Password fields and the RADIUS entry, the MAX 200Plus cannot extend the MPP call beyond a single channel.

- If you request CACHE-TOKEN, the Enable Dial-Out Password field must match the Ascend-Receive-Secret attribute in the RADIUS entry that authenticated the call.

  If you do not enter identical passwords in the Enable Dial-Out Password field and Ascend-Receive-Secret attribute, CACHE-TOKEN calls are rejected after initial access through hand-held security card authentication.
- PAP-TOKEN and PAP-TOKEN-CHAP require configuration of a SAFEWORD or ACE entry in the NAS's RADIUS users file with the caller's name.

  For information on prompting the user for their password at the MAX 200Plus unit's terminal server, see the description of the set password command in the *MAX 200Plus 200 Plus Supplemental Documentation Set.*
- Dial on Broadcasts must be enabled when a PC on the same Ethernet as the MAX 200Plus runs the APP Server utility to open a connection protected by security-card authentication.

See Also: Dial on Broadcasts, Encapsulation, Enable Dial-In Password, Enable Dial-Out Password

Callback

Description: This enables or disables the callback feature.

When you enable the callback feature, the MAX 200Plus hangs up after receiving an incoming call that matches the one specified in a connection. The MAX 200Plus then calls back the device at the remote end of the link using the Dial-Out Number specified in the connection.

You can use the Callback parameter to tighten security, as it ensures that the MAX 200Plus always makes a connection with a known destination.

Usage:

- Selecting the Callback checkbox enables the callback feature.
- Deselecting the Callback checkbox disables the callback feature.

  Callback is disabled by default.

Dependencies: Keep this additional information in mind:

- The Callback parameter does not apply if all channels of the link are leased (Channel B1 and Channel B2 are set to Leased in the Configure BRI Card dialog box).
- If you enable Callback, you must also select Enable Dial-Out and specify a Number for the MAX 200Plus to dial, because the connection must both answer the call and call back the device requesting access.

  Similarly, any device calling into a connection set for callback must be configured to both dial calls and answer them.

See Also: Enable Dial-Out, Enable Dial-In, Number

Channel B1

Description: This specifies whether the first B channel on an ISDN BRI line is leased, switched, or not used by the MAX 200Plus.

Usage:

- Leased specifies that the channel is permanently connected.
- Switched specifies that the channel supports switched connectivity.

  The default is Switched.
- Unused specifies that the MAX 200Plus does not use the channel.

Dependencies: The Channel B1 parameter applies only when an ISDN BRI PC Card is installed.

See Also: Channel B2

Channel B2

Description: This specifies whether the second B channel on an ISDN BRI line is leased, switched, or not used by the MAX 200Plus.

Usage:

- Leased specifies that the channel is permanently connected.
- Switched specifies that the channel supports switched connectivity.

  The default is Switched.

- Unused specifies that the MAX 200Plus does not use the channel.

Dependencies: The Channel B2 parameter applies only when an ISDN BRI PC Card is installed.

See Also: Channel B1

Clear Terminal Server when session ends

Description: Specifies whether the dial-in connection is cleared when an interactive Telnet, Rlogin, or TCP session terminates. If set to No, the user is returned to the terminal server menu when the Telnet, Rlogin, or TCP session terminates.

Usage: Specify Yes or No. The default is No.

- Yes means the MAX clears the call when a Telnet, Rlogin, or TCP session terminates.
- No means the MAX returns the user to the terminal server menu when a Telnet, Rlogin, or TCP session terminates.

Dependencies: This parameter is not applicable when terminal services are disabled.

Clear screen when session begins

Description: Specifies whether the screen is cleared when a terminal server session begins.

Usage: Specify Yes or No. The default is Yes.

- Yes means the MAX clears the screen when a terminal server session begins.
- No means the MAX does not clear the screen.

Dependencies: This parameter is not applicable when terminal services are disabled.

See Also: Enable Terminal Server

Clock

Description: This displays the time of the day in hours:minutes:seconds format. This is either:

- The system clock of the PC running the Management Console.
- The system clock of the MAX 200Plus.

You can configure the clock by selecting Set Clock from the MAX menu.

Close

Description: The Close command on the MAX menu closes the open, active configuration file.

Save any open configuration file before closing it.

Connect

Description: The Connect command on the MAX menu allows you to:

- Connect to a previously configured MAX 200Plus by entering its IP address or name.
- Find a new, unconfigured MAX 200Plus on the same subnet as the Management Console.

The Management Console finds new MAX 200Plus units on the network by sending out a broadcast message. Unconfigured MAX 200Plus units respond to this broadcast with their unique Media Access Control (MAC) address. Once the Management Console has discovered new MAX 200Plus units, it displays them in the Find MAXs dialog box with their default name (“unnamed”) and MAC address.

Once it appears in the Find MAXs dialog box, you can click Configure button to assign the MAX 200Plus its Name, IP address, and Subnet Mask. Once this information is entered, you can proceed to configure your MAX 200Plus.

See Also: Find

Contact

Description: Use this field to specify the person or department to contact if you experience problems using the MAX 200Plus.

Usage: Type the name of the contact person or department. You can enter up to 38 characters. An SNMP management application can read this field, but the value you enter does not affect the operation of the MAX 200Plus.

See Also: Location

Default Gateway

Description: This specifies the IP address of the router that a packet must go through to reach the destination station of the route if the MAX 200Plus doesn't have a route to the packets destination. The MAX 200Plus can route packets in these ways:

- using its routing table, created at initialization time and updated using Routing Information Protocol (RIP)
- through this default gateway
- through a connection defined in the Connection tab

Usage: Enter the IP address of the router.

An IP address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0.

Example: 200.207.23.1

Dependencies: Keep this additional information in mind:

- If you do not know the right IP address to enter, you must obtain it from the network administrator.

  Do not attempt to configure an IP address by guesswork!

See Also: Encapsulation, LAN Address, Route IP, RIP

Dial on Broadcasts

Description: This specifies whether broadcast packets initiate dialing.

Usage:

- Selecting Dial on Broadcasts specifies that the MAX 200Plus dials a link if:
  - the link is not online and
  - the MAX 200Plus receives a frame whose MAC address is set to broadcast

  When a device on the local Ethernet interface sends out broadcast packets that the MAX 200Plus must bridge to another network, the MAX 200Plus starts up a session for each connection in which Dial on Broadcasts is enabled.
- Deselecting Dial on Broadcasts specifies that broadcast packets do not initiate dialing.

  If you choose this setting, the MAX 200Plus relies on its bridging table to forward packets.

  Dial on Broadcasts is disabled by default.

Dependencies: The Dial on Broadcasts parameter applies only if both Bridging and Dial-Out are enabled for the connection.

See Also: Enable Bridging, Dial Query

Dial on Query

Description: This specifies whether the MAX 200Plus places a call to the location indicated in the connection when a workstation on the local IPX network looks for the nearest IPX server. More than one connection can enable Dial on Query. As a a result, several connections can occur at the same time.

Usage:

- Selecting Dial on Query specifies that the MAX 200Plus places a call to the location specified in the connection when a workstation looks for the nearest IPX server.

  Note that a workstation is likely to stop attempting to find a server before the MAX 200Plus establishes any connections with the Dial on Query mechanism.
- Deselecting Dial on Query specifies that the MAX 200Plus does not place a call to the location specified in the connection when a workstation looks for the nearest IPX server.

  Dial on Query is disabled by default.

Dependencies: If there is an entry in the MAX 200Plus unit's routing table for the location specified by the connection, Dial on Query has no effect.

Enable Appletalk

Description: This parameter specifies whether the MAX 200Plus enables a minimal AppleTalk stack to support ARA (AppleTalk Remote Access) connections. The MAX 200Plus does not support full Appletalk routing.

Usage:

- Selecting Enable Appletalk specifies that the MAX loads the AppleTalk stack to support ARA calls.
- Deselecting Enable Appletalk specifies that the MAX does not run AppleTalk.

  Appletalk is disabled by default.

See Also: Allow ARA, Encapsulation, Zone

Enable Bridging (Connection tab)

Description: This parameter enables or disables protocol-independent bridging for this connection. If you disable bridging, you must enable IP or IPX routing in the Connections Protocol tab.

Usage:

- Select the checkbox to enable bridging.
- Deselect the checkbox to disable bridging.

  The default is Bridging disabled.

Dependencies: The effect of the enable bridging for a connection depends on how you set IP and IPX routing.

Bridging and IP routing

- If Enable Bridging is selected and Route IP is selected, the MAX 200Plus routes IP packets, and bridges all other packets.
- If Enable Bridging is selected and Route IP is deselected, the MAX 200Plus bridges all packets.
- If Enable Bridging is deselected and Route IP is selected, the MAX 200Plus routes only IP packets.
- If Enable Bridging is deselected and Route IP is deselected, an error occurs and you cannot save the profile.

Bridging and IPX routing

- If Enable Bridging is selected and Route IPX is selected, the MAX 200Plus routes IPX packets, and bridges all other packets.
- If Enable Bridging is selected and Route IPX is deselected, the MAX 200Plus bridges all packets.
- If Enable Bridging is deselected and Route IPX is selected, the MAX 200Plus routes only IPX packets.
- If Enable Bridging is deselected and Route IPX is deselected, an error occurs and you cannot save the profile.

Additional Dependencies

- Bridging must be enabled on both the dialing and answering sides of the link.

  The Connection on the dialing side and the Answer Profile on the answering side must both set the Bridge parameter to Yes. Otherwise, the MAX 200Plus does not bridge the packets.

- The Enable Bridging parameter does not apply if you disable bridging in the MAX Info tab.
- The Enable Bridging parameter in the MAX Info tab applies to incoming calls for which no connection has been defined. If a connection has been defined, the setting of the Enable Bridging checkbox in the Connection tab takes precedence.
- Do not confuse the Enable Bridging parameter in the MAX Info tab with the Enable Bridging parameter in the Connection tab.
  - The Enable Bridging parameter in the MAX Info tab globally enables or disables bridging.
  - Enable Bridging parameter in the Connection tab applies only to a specific connection.

See Also: Enable Bridging (MAX Info tab), Encapsulation, Route IP, Route IPX

Enable Bridging (MAX Info tab)

Description: This parameter allows you to globally enable or disable bridging for all connections that the MAX 200Plus answers or dials.

Usage:

- Selecting the checkbox globally enables bridging.

  When you choose this setting, the MAX 200Plus operates in promiscuous mode. The Ethernet controller in the MAX 200Plus accepts all packets and passes them up the protocol stack for a higher-level decision on whether to route, bridge, or reject them. This mode is appropriate if you are using the MAX 200Plus as a bridge.

- Deselecting the checkbox globally disables bridging.

  When you choose this setting, the Ethernet controller filters out all packets except broadcast packets and those explicitly addressed to the MAX 200Plus. This disables bridging for all incoming and outgoing connections

  This mode significantly reduces processor and memory overhead when the MAX 200Plus is routing, and can result in much better performance, especially in moderate to heavily loaded networks.

  Bridging is globally disabled on the MAX by default.

Dependencies: Do not confuse the Enable Bridging parameter in the MAX Info tab with the Enable Bridging parameter in the Connection tab.

- The Enable Bridging parameter in the MAX Info tab globally enables or disables bridging.
- Enable Bridging parameter in the Connection tab applies only to a specific connection.

See Also: Enable Bridging (Connection tab), Encapsulation, Route IP, Route IPX

Enable Dial-In

Description: This specifies whether the MAX 200Plus can receive incoming calls. The setting you choose only affects dialing in from the destination specified in this connection.

See Also: LAN Address, Station

Enable Dial-Out

Description: This specifies whether the MAX 200Plus can initiate outgoing calls.The setting you choose only affects dialing in from the destination specified in this connection.

See Also: LAN Address, Station

Enable (Immediate Modem)

Description: This parameter enables or disables the Immediate Modem service. If Immediate Modem service is enabled, users can Telnet to a MAX 200Plus to access the MAX 200Plus unit's modems, so that they can place outgoing calls without going through MAX 200Plus terminal server interface. The MAXDial software offers the same outgoing call ability, but through a GUI interface.

Note: The MAX 200Plus provides per-user control and accounting for both the Immediate Modem feature and MAXDial to control access to the modems.

Usage: Specify Yes or No. The default is No.

- Yes enables Immediate Modem service.
- No disables this service.

Dependencies: This parameter is not applicable if terminal services are disabled.

See Also: Port

Enable IPX

Description: This specifies whether IPX routing is globally enabled on the MAX 200Plus. When you enable IPX routing, the MAX 200Plus can perform these functions:

- Establish IPX routing
- Forward IPX packets
- Generate RIP and SAP packets
- Interpret incoming RIP and SAP packets

Usage:

- Select Enable IPX in the Protocol tab to perform IPX routing functions.

  IPX Routing is enabled by default.

- Deselect Enable IPX in the Protocol tab to disable the MAX 200Plus from performing IPX routing functions.

  You may want to disable IPX routing if your network uses a protocol other than IPX, or if your IPX network maintains such large RIP and SAP tables that the MAX 200Plus is spending too much time maintaining them.

Dependencies: Keep this additional information in mind:

- The enabling or disabling IPX routing does not affect watchdog spoofing in IPX bridging.
- If you disable IPX Routing while a WAN connection routing IPX exists, the MAX 200Plus does not tear down the connection, but no further IPX traffic can take place on the connection.
- If you disable IPX Routing in the MAX Protocol tab, you disable IPX routing for all incoming and outgoing connections.

See Also: Dial on Query, LAN Network#, WAN Network#, Route IPX

Enable Terminal Server

Description: This enables or disables terminal services.

Usage: Specify Yes or No. The default is No.

- Yes enable the terminal server.
- No disables the terminal server. Note that terminal services must be enabled to support incoming calls from analog modems or V.120 terminal adapters.

Encapsulation

Description: This enables you to choose the encapsulation method to use when exchanging data with a remote network.

Usage: You can choose one of the following settings:

PPP

PPP (Point-to-Point Protocol) provides a standard means of encapsulating data packets over a single-channel WAN link that a connection sets up. It ensures basic compatibility with non-Ascend devices.

For this setting to work, both the dialing side and the answering side of the link must support PPP.

MPP

MPP (Multilink Protocol Plus) extends the capabilities of MP (Multilink PPP) to support inverse multiplexing, session management, and bandwidth management. MP is an extension of PPP that supports the ordering of data packets across multiple channels.

MPP allows you to combine individual channels into a single high-speed connection.

MPP consists of these components:

- a low-level channel identification, error monitoring, and error recovery mechanism
- a session management level for supporting bandwidth modifications and diagnostics

MPP enables the MAX 200Plus to perform Dynamic Bandwidth Allocation (DBA)—that is, MPP enables the MAX 200Plus to add or remove channels without disconnecting a link as the need for bandwidth increases or decreases.

Both the dialing side and the answering side of the link must support MPP. If only one side supports MPP, the connection uses MP or standard single-channel PPP.

Dependencies: Keep this additional information in mind:

- The Encapsulation parameter does not apply when the MAX 200Plus answers a call, or if the link consists of only leased channels (Channel

B1 and Channel B2 are set to Leased in the Configure BRI Card dialog box).

- If Encapsulation is set to MPP, the MAX 200Plus adds or subtracts switched channels on the connection as required by the Dynamic Bandwidth Allocation (DBA) parameters on either side of the connection.

  DBA, or Dynamic Bandwidth Allocation, enables the MAX 200Plus to use average line utilization (ALU) of transmitted data as the basis for adding or subtracting bandwidth from a switched connection without terminating the link.

  The MAX 200Plus samples the bandwidth usage of the line every 15 seconds and calculates the average line utilization during that period. When the average line utilization exceeds 70%, the MAX 200Plus attempts to bring up another B channel to increase the bandwidth available to the call. If the average line utilization falls below 70%, the MAX 200Plus brings down any additional channels of a multichannel call.

  If the two sides of the connection disagree on the number of channels needed, the side requesting the greater number prevails.

- When you set Encapsulation to MPP, both the dialing side and the answering side of the link must support MPP. If only one side supports MPP, the connection uses MP or standard single-channel PPP. When you set Encapsulation to PPP, the connection uses only PPP.

See Also: Allow MPP, Allow PPP

Ethernet Address

Description: This displays the Media Access Control (MAC) address of the MAX 200Plus.

Exit

Description: The Exit command on the File menu exits the Management Console.

Save any open configuration files before exiting the Management Console.

Find

Description: The Find command on the MAX menu displays the Find MAXs dialog box. Use this dialog box to see and connect to all the MAXs currently on your network.

The Management Console finds new MAX 200Plus units on the network by sending out a broadcast message. Unconfigured MAX 200Plus units respond to this broadcast with their unique Media Access Control (MAC) address. Once the Management Console has discovered new MAX 200Plus units, it displays them in the Find MAXs dialog box with their default name ("unnamed") and MAC address.

The Management Console only displays MAX 200Plus units on your local network. You can, however, manage any MAX 200Plus by using the Connect command from the MAX menu.

See Also: Connect

Force CHAP Authentication

Description: This parameter specifies that incoming PPP or MPP connections must use Challenge Handshake Authentication Protocol (CHAP) authentication. CHAP provides a way to periodically verify the identity of a host using a three-way handshake and encryption. Authentication takes place upon initial link establishment; the MAX 200Plus can repeat the authentication process any time after the connection is made. The remote device must support CHAP.

Usage:

- Deselect Force CHAP Authentication to disable CHAP authentication for the call.

  Note that this disables all login security on the MAX 200Plus.

- Select Force CHAP Authentication to specify that the MAX 200Plus uses the CHAP, a PPP authentication protocol for incoming calls.

Dependencies: Keep this additional information in mind:

- Deselecting Force CHAP Authentication disables all log in security on the MAX 200Plus.
- The link must use PPP or MPP encapsulation (Encapsulation is set to PPP or MPP) to use CHAP authentication.
- If you force CHAP authentication, you must also specify a password in Enable Dial-In Password field for each connection.
- When you force CHAP authentication, and the LAN address parameter has a fixed value, the MAX requires that the caller use that address.

See Also: Authentication, Password

Frame Type

Description: This specifies the Ethernet frame type to use for IPX on the Ethernet interface.

IPX packets can appear in more than one Ethernet frame type on an Ethernet segment. If your MAX 200Plus routes IPX, it can recognize only a single IPX frame type. The MAX 200Plus does not route other IPX frame types, and may attempt to bridge them. In addition, the MAX 200Plus can only route and perform watchdog spoofing for the IPX frame type specified by the Frame Type setting.

Usage:

- 802.3 specifies the 802.3 frame type.

  This setting indicates that IPX clients and servers on the local Ethernet cable follow the IEEE 802.3 protocol for the MAC (Media Access

Control) header, also called Raw 802.3. The frame does not contain the LLC (Logical Link Control) header in addition to the MAC header.

For NetWare 3.11 or earlier, select 802.3.

- 802.2 specifies the 802.2 frame type.

  This setting indicates that the IPX clients and servers on the local Ethernet cable follow the IEEE 802.2 protocol for the MAC header. The framer contains the LLC header in addition to the MAC header.

  For NetWare 3.12 or later, select 802.2.

  The default is 802.2.

- SNAP specifies the SNAP frame type.

  This setting indicates that the IPX clients and servers on the local Ethernet network follow the SNAP (SubNetwork Access Protocol) for the MAC header. This specification includes the IEEE 802.3 protocol format plus additional information in the MAC header.

- Enet II specifies the Ethernet II frame type.

  This setting indicates that IPX clients and servers on the local Ethernet network follow the Ethernet II protocol for the MAC header.

- None disables IPX-specific features.

  If you choose this setting, the MAX 200Plus can bridge or route IPX, but without watchdog spoofing or the automatic RIP (Routing Information Protocol) and SAP (Service Advertising Protocol) data filters described in Handle IPX.

Dependencies: To determine the IPX frame type in use, enter the Config command on a NetWare server, or look at the NET.CFG file on an IPX client. Choose a setting based on this information:

- Select 802.3 if Frame=Ethernet_802.3.
- Select 802.2 if Frame=Ethernet_802.2.
- Select SNAP if Frame=Ethernet_SNAP.
- Select Enet II if Frame=Ethernet_II.

Dependencies: If you disable IPX Routing for a connection, Frame Type is not applicable.

Handle IPX for

Description: This enables you to configure a connection that bridges IPX.

Usage: Press Enter to cycle through the choices.

- None specifies that special IPX behavior does not take place.

  Choose this setting when the LAN on each side of the bridge has one or more IPX servers.

  The default is None.

- Clients Only specifies that the MAX 200Plus discards RIP (Routing Information Protocol) and SAP (Service Advertising Protocol) periodic broadcasts at its WAN interface, but forwards RIP and SAP queries.

  The WAN interface is the port on the MAX that is connected to a WAN line. RIP and SAP queries enable a client workstation to locate a NetWare server across the network. Choose this setting when *both* these conditions are true:

  – The local LAN has IPX clients but no servers.

  – The MAX 200Plus is acting as a bridge to another LAN containing only IPX servers or a combination of IPX servers and clients.

- Servers (and Clients) specifies that the MAX 200Plus discards all RIP and SAP periodic broadcasts and queries at its WAN interface.

  Server mode allows the MAX 200Plus to bring down calls during idle periods without breaking client/server or peer-to-peer connections.

  Ordinarily, when a NetWare server does not receive a reply to the watchdog keepalive packets it sends to a client, it closes the connection. When you select Server mode, however, the MAX 200Plus replies to NCP watchdog requests on behalf of clients on the other side of the bridge; in other words, the MAX 200Plus tricks the server watchdog process into believing that the link is still active. This process is called watchdog spoofing.

  Choose this setting when *both* these conditions are true:

  – The MAX 200Plus is acting as a bridge to a remote LAN with IPX clients, but no servers.

  – The local LAN contains only IPX servers, or a combination of IPX clients and servers.

Dependencies: Keep this additional information in mind:

- If you select the Servers (and Clients) setting, you must also specify a Spoof value, indicating the maximum length of idle time during which the MAX 200Plus performs watchdog spoofing for NetWare connections.
- If the bridging is not enabled for the connection (Enable Bridging in the Connections tab is deselected), the Handle IPX parameter does not apply.
- If IPX routing is not enabled in the Connection tab (Route IPX is deselected in the Connection tab), the Handle IPX parameter does not apply.
- We highly recommend that you:
  - Enable Dial on Broadcasts when Handle IPX is set to Clients Only
  - Disable Dial on Broadcasts is disabled when Handle IPX is set to Servers (and Clients)

  When a client on the local Ethernet interface sends out broadcast packets to locate a server, and the MAX 200Plus must bridge these packets to another network, the MAX 200Plus starts up a session for each connection in which Dial on Broadcasts is enabled. The server need not broadcast and then dial, so disable Dial on Broadcasts to keep broadcast packets from causing the MAX 200Plus to dial automatically.
- If the MAX 200Plus on one LAN sets Handle IPX set to Servers (and Clients) and the LAN on the other side of the connection has only NetWare clients, the MAX 200Plus on the client-only LAN should set Handle IPX to Clients Only.

  If both LANs contain servers, both sides of the connection should set Handle IPX to None.
- Although Handle IPX is not applicable for if Bridging is disabled for a connection or IPX Routing is enable for a connection, the MAX 200Plus automatically performs watchdog spoofing just as though you had set Handle IPX to Servers (and Clients). However, the MAX 200Plus does not filter as though you had set Handle IPX to Servers (and Clients).

See Also: Dial on Broadcasts, Spoof

Honor BOOTP

Description: Specifies whether or not the MAX responds to BOOTP within SLIP sessions. If a unit dials into the MAX unit's terminal server and runs SLIP, it can get an IP address through a BOOTP request. This IP address is taken from the MAX unit's IP address pool or by the Ascend-IP-Pool-Definition attribute in the RADIUS database.

Usage: Specify Yes or No. The default is No.

- Yes enables the MAX to respond to a BOOTP request from the calling unit during a SLIP session.
- No disables BOOTP for SLIP sessions.

Dependencies: This parameter does not apply if terminal services are disabled or if SLIP is set to No.

See Also: Pool # Count, Pool # Start, Enable Terminal Server

Host addresses

Description: Specifies the IP address and a text description of the first, second, third, and fourth hosts listed in the terminal server menu-mode interface.

Usage: Specify the IP address and a text description of the host. The default IP address value is 0.0.0.0/0.

Dependencies: This parameter is not applicable if terminal services are disabled.

Idle Timeout

Description: This specifies the number of seconds the MAX 200Plus waits before clearing a call when a session is inactive.

Usage: Enter a number between 0 and 65535. If you specify 0 (zero), MAX 200Plus does not enforce a limit; an idle connection stays open indefinitely. The default setting is 120 seconds.

Dependencies: Keep this additional information in mind:

- The Idle Timeout value in the MAX Info tab applies to incoming calls for which no Connection exists (that is, for individual users dialing in); if a Connection exists, its Idle Timeout value takes precedence.

See Also: Encapsulation

Initial Screen

Description: Specifies the type of user interface displayed at the start of a dial-in terminal server connection.

Usage: Specify one of the following values:

- Command line (the default) to display the command-line interface ("terminal mode").
- Menu to display the menu interface ("menu mode").

IP Address

Description: This specifies the IP address of the MAX 200Plus on the local Ethernet network.

Usage: Enter the IP address of the MAX 200Plus on the local Ethernet network.

The address consists of four numbers between 0 and 255, separated by periods.

Separate the optional netmask from the address with a slash. The IP address must be a valid IP address on the local Ethernet network. The default value is 0.0.0.0/0.

Example: 10.2.1.1/24

In this example, 10.2.1.1 is the MAX 200Plus unit's IP address. The number 24 represents the number of bits in the MAX 200Plus unit's netmask. Masking 24 bits in the MAX 200Plus unit's address provides a subnet of 10.2.1.0.

Dependencies: Keep this additional information in mind:

- The value of the IP Address parameter on the local MAX 200Plus must match the value of the LAN Address parameter of the unit at the remote end of the link.
- If you do not know the right IP address to enter, you must obtain it from the network administrator.

  Do not attempt to configure an IP address by guesswork!

See Also: Encapsulation, Route IP, Subnet Mask

IPX Net#

Description: This parameter enables you to create a static route to another Ethernet network through a connection. The value of IPX Net# specifies the network number of the router at the remote end of the connection.

Usage: Enter an Ethernet network number using an 8-digit (4-byte) hexadecimal value. Specify the network number of the router at the remote end of the connection only if the router requires that the MAX 200Plus know its network number before connecting. You almost never need to set this parameter.

The default is 00000000. If you accept the default, the connection is still valid, but the MAX 200Plus does not advertise the route until it makes a connection to the Ethernet network

Dependencies: IPX Net# is not applicable if the MAX 200Plus is not set up for IPX routing (Enable IPX is deselected in the MAX Protocol tab).

See Also: Route IPX

LAN Address

Description: This specifies the IP address of a station or router at the remote end of the link specified by the connection.

Usage: Enter the IP address of a remote station or router. The MAX 200Plus automatically enters a subnet mask in the Subnet Mask field based on the address you enter. This subnet mask is correct in most situations.

An IP address consists of four numbers between 0 and 255, separated by periods. The default setting is 0.0.0.0. This means that an answering connection with this setting matches all incoming IP addresses.

Example: 200.207.23.101

Dependencies: Keep this additional information in mind:

- The value of the LAN Address parameter on the local MAX 200Plus must match the IP address the remote end of the link is expecting.
- No two connections should have the same LAN Address.
- Setting LAN Address to 0.0.0.0 and clearing the Station parameter resets all parameters in the connection to their defaults.
- The LAN Address parameter is not applicable if the Route IP is not enabled for the connection.
- If you do not know the right IP address to enter, you must obtain it from the network administrator.

  Do not attempt to configure an IP address by guesswork!

See Also: Encapsulation, IP Address, Route IP, Station, Subnet Mask

LAN Network

Description: This specifies a unique IPX network number for the Ethernet interface.

The MAX 200Plus assigns an address to a workstation when it connects to the MAX 200Plus; it derives the address from the network number.

Usage: Enter an IPX network number using an 8-digit (4-byte) hexadecimal value. The default is 00000000. The number you specify must be unique within your wide area IPX network, and must match the configuration of other routers on the local Ethernet network.

When you accept the default setting of 00000000, the MAX 200Plus learns its IPX network number from other routers on the Ethernet network. If you enter a value other than zero, the MAX 200Plus becomes the “seeding”

router and sets its IPX network number for the other routers on the Ethernet network.

Example: **`DE040600`**

Dependencies: The LAN Network# is not applicable if the MAX 200Plus is not set up for IPX routing by enabling IPX routing in the MAX Protocol tab.

Location

Description: This specifies the location of the MAX 200Plus.

Usage: Enter a description of the MAX 200Plus unit's location. You can enter up to 38 characters. An SNMP management application can read this field, but the value you enter does not affect the operation of the MAX 200Plus.

See Also: Contact

Metric

Description: This determines the virtual hop count of the link.

The Metric ensures that the MAX 200Plus uses an active connection before using an inactive connection if there are two routes available to a single destination network. Although the actual hop count of the link or route is 1, you can enter any value between 1 and 15. This value is the virtual hop count. The higher the value entered, the less likely that the MAX 200Plus brings the link or route online.

Usage: Enter a number between 1 and 15. The default setting is 7.

Example: If connection A has a route to a station and has a metric of 3, and Connection B has a route to the same station with a metric of 4, the MAX 200Plus brings up connection A when it receives a packet destined for the station.

Dependencies: Keep this additional information in mind:

- If you enable RIP (Routing Information Protocol) across the WAN in a connection, the hop count for the route can differ from the value of the Metric parameter in the Route Profile because the MAX 200Plus always uses the lower hop count.
- The hop count includes the metric of each switched link in the route.

See Also: RIP

Mode

Description: Specifies the default Telnet mode for terminal server Telnet users.

Usage: Specify one of the following values:

- ASCII

  Standard 7-bit mode. In 7-bit mode, bit 8 is set to 0 (zero); 7-bit telnet is also known as NVT (Network Virtual Terminal) ASCII. This is the default if no other mode is specified.

- Binary

  The MAX 200Plus attempts to negotiate the telnet 8-bit binary option with the server at the remote end. You can run X -Modem and other 8-bit file transfer protocols using this mode.

  In 8-bit binary mode, the telnet escape sequence does not operate. The telnet session can close only if one end of the connection quits the session. If you are a local user not connected through a digital modem, the remote-end user must quit.

  A user can override the binary setting on the Telnet command line.

- Transparent

  You can send and receive binary files without having to be in Binary mode. You can run the same file transfer protocols available in Binary mode.

Dependencies: This parameter is not applicable when terminal services are disabled.

See Also: Enable Terminal Server

Name

Description: This specifies the name of the MAX 200Plus. This name is sent to the remote end of a PPP or MPP connection whenever the MAX 200Plus establishes a outgoing call.

When the MAX 200Plus receives a PPP or MPP call from an Ascend unit, it tries to match the caller's Name to the value of the Station field in a connection.

If the MAX 200Plus finds a match and authentication is enabled, the MAX 200Plus then verifies that the incoming call contains the correct Enable Dial-in Password.

If the password is correct, the connection is established: if it is not correct, the MAX 200Plus refuses the connection.

Usage: Enter a name. You can enter up to 16 characters.

Dependencies: Because the MAX 200Plus uses the Name for authentication, you must type it exactly as the remote network expects it. In this case, Name is case sensitive.

New Configuration File

Description: The New Configuration File command on the File menu opens a new configuration file with a default configuration. This configuration file can be modified with the appropriate parameters and then uploaded to a MAX 200Plus using the Update command from the MAX menu.

See Also: Update, Update To, Find, Connect, Open Configuration File

Number

Description: Use this field to specify the phone number the MAX 200Plus dials to reach the bridge, router, or node at the remote end of the link.

Usage: Enter a telephone number, up to 37 characters. You must limit those characters to the following:

`1234567890()[]!z-*#|`

The MAX 200Plus sends only the numeric characters to place a call. The default value is null.

Dependencies: Keep this additional information in mind:

- Number does not apply when all channels are leased (Channel B1 and Channel B2 are set to Leased in the Configure BRI Card dialog box).

See Also: Channel B1, Channel B2, Encapsulation

Numbers B1 (B2)

Description: This specifies the phone numbers for the ISDN BRI line.

Your carrier assigns two phone numbers to your line, except when you use an AT&T switch in point-to-point mode. If you are using a multipoint switch (Switch Type is set to Multi-P), enter a second telephone number. If you use a point-to-point switch (that is, Switch Type is set to AT&T Point-To-Point), do not enter a second telephone number.

When the MAX 200Plus receives a multichannel MPP call, it reports the two phone numbers to the calling party. The calling MAX 200Plus can then add more channels. If you do not specify a phone number and the calling MAX 200Plus needs to add more channels, it redials the phone number it used to make the first connection.

Usage: Enter a telephone number up to 16 characters; you must limit those characters to numbers, hyphens, and parentheses.

Typically, the phone numbers assigned to a line share a group of leading digits. Enter only the rightmost digits identifying the phone number, excluding digits that the phone numbers have in common.

Example: Suppose that 777-3330 is the first number for line #1, and 777-3331 is the second number for line #1. Set the B1 number to 30 and the B2 number to 31.

Dependencies: The phone number you specify for second phone number is for this MAX 200Plus only. Do not enter the phone number of the MAX 200Plus you are calling.

See Also: Numbers, Switch Type, Encapsulation

Open Configuration File

Description: The Open Configuration File command on the File menu opens an existing configuration file. This configuration file can be modified with the appropriate parameters and then uploaded to a MAX 200Plus using the Update command from the MAX menu.

See Also: Update, Update To, Find, Connect, New Configuration File

Operator can choose screen

Description: Specifies whether an interactive user is allowed to switch between menu mode and the terminal server command line. Users switch to menu mode by using the terminal server Menu command, and switch from menu mode to the command line by pressing the zero key. If this parameter is set to No, the menu command and 0 command are disabled.

Usage: Specify Yes or No. The default is Yes.

- Yes means terminal server users can switch between terminal mode and menu mode.
- No means users have access only to the screen configured to come up initially.

Dependencies: This parameter is not applicable when terminal services are disabled.

See Also: Initial Screen

Password

Description: The MAX 200Plus uses the following Passwords:

- Password, Enable Dial-In (in the Connections tab) specifies the password that the remote end of the link must send. If the user does not enter the correct password, the MAX 200Plus disconnects the link. This password is typically used for a network-to-network connection.

- Password, Enable Dial-Out (in the Connections tab) specifies the password that the MAX 200Plus sends to the remote end of a connection on outgoing calls. If the password sent by the MAX 200Plus does not match the password the remote end is expecting, the remote end disconnects the link. This password is typically used for a network-to-network connection.
- User Password (in the New User dialog box) specifies the password the remote user must enter to connect to the MAX 200Plus. This is used for an individual connecting to the MAX 200Plus.
- Password (Security in Misc tab) specifies the terminal server password.
- Password (Immediate Modem Access in Misc tab) specifies a password required to dialout using the Immediate Modem service.

Usage:

- Password, Enable Dial-In: Enter the password for the remote device on an incoming call. You can enter up to 20 characters; the password is case sensitive.
- Password, Enable Dial-Out: Enter a password that the remote end requires the MAX 200Plus to send. You can enter up to 20 characters; the password is case sensitive. Leave the field blank if the remote end does not require a password.
- User Name: Enter the password for the remote user on an incoming call. You can enter up to 20 characters; the password is case sensitive.
- Password (Security in Misc tab): Specify up to 20 characters.
- Password (Immediate Modem Access in Misc tab): Specify up to 64 characters.

Dependencies: Keep this additional information in mind:

- If Authentication is set to PAP-Token-CHAP, you must enter an auxiliary password in the Dial-Out Password field. This is the password that the MAX 200Plus sends when it adds channels to a security-card MPP call. The MAX 200Plus obtains authentication of the first channel of this MPP call from the hand-held security card.

  This password must match the password in the RADIUS entry for authenticating the call. In this case, you must use the Ascend Password

Protocol (APP) server utility. This utility allows users to supply token passwords from a PC or UNIX host on the local network.

Refer to the *MAX 200Plus Supplemental Documentation Set* or the Ascend Web site for further information about security on the MAX 200Plus.

- If Force CHAP Authentication is not enabled in the MAX Info tab, there is no authentication of incoming callers.
- You must specify a value for Enable Dial-In Password when the connection uses PPP or MPP encapsulation and Force CHAP Authentication is enabled.

  When you set Encapsulation to MPP, both the dialing side and the answering side of the link must support MPP. If only one side supports MPP, the connection uses MP or standard single-channel PPP. When you set Encapsulation to PPP, the connection uses only PPP.
- You must specify a value for Enable Dial-Out Password when the connection uses PPP or MPP encapsulation and the MAX 200Plus uses PAP, CHAP, or CACHE-TOKEN authentication.
- Password (Security in Misc tab): This parameter is not applicable if Terminal Server is disabled.
- Password (Immediate Modem Access in Misc tab): This parameter is not applicable if both Terminal Server and Immediate Modem access are disabled.

See Also: Authentication, Encapsulation, Security, Enable Terminal Server

Pool 1 (2)

Description: This specifies the first IP address in an IP address pool. The MAX 200Plus chooses an address from the pool and assigns it to an incoming call when Assign Address from Pools is selected or when the calling station requests an address assignment.

Usage: Enter the first IP address in the pool. The address consists of four numbers between 0 and 255, separated by periods. The address you specify does not need to be on the same LAN segment as the MAX 200Plus. The default is 0.0.0.0.

Example: 200.207.23.1

Dependencies: Pool 1 (2) applies only when the calling station uses PPP encapsulation.

See Also: Assign Address from Pools, Range

Port

Description: Specifies the port number for Immediate Modem dialout. It tells the MAX 200Plus that all Telnet sessions initiated with that port number want modem access.

Usage: Specify a port number (5000–65535). The default is 5000.

Dependencies: This parameter is not applicable if terminal services are disabled.

See Also: Enable (Immediate Modem)

Primary DNS

Description: This parameter the IP address of the primary domain name server.

Domain Name System (DNS) is a TCP/IP service that enables you to specify a symbolic name instead of an IP address. A symbolic name consists of a username and a domain name in the format <username>@<domain name>. The username corresponds to the host number in the IP address; the domain name corresponds to the network number in the IP address. A symbolic name might be steve@abc.com or joanne@xyz.edu.

DNS maintains a database of network numbers and corresponding domain names on a domain name server. When you use a symbolic name, DNS translates the domain name into an IP address, and sends it over the network. When the Internet service provider receives the message, it uses its own database to look up the username corresponding to the host number.

Usage: Enter the IP address of the primary domain name server. The address consists of four numbers between 0 and 255, separated by periods.

The default value is 0.0.0.0. Accept this default if you do not have a domain name server.

Example: `200.207.23.1`

See Also: Secondary DNS

Primary WINS

Description: This specifies the IP address of the primary Windows Internet Name Service (WINS) server.

WINS servers are similar to DNS servers, allowing users to log into servers using names instead of IP addresses.

Usage: Enter an IP address in dotted decimal notation. The default is 0.0.0.0.

Dependencies: Primary WINS applies only to Telnet and raw TCP connections running under the MAX 200Plus unit's terminal server interface.

See Also: Secondary WINS

Print

Description: The Print command on the File menu allows you to Print the Activity log. The Activity log records the latest 32 events on the MAX 200Plus.

Print Preview

Description: The Print Preview command on the File menu allows you to preview the Activity Log as it will be printed.

Print Setup

Description: The Print Setup command on the File menu allows you to set up the default printer.

Range

Description: This specifies the number of IP addresses in the IP address pools. The MAX 200Plus chooses an address from these pools and assigns it to an incoming call when Assign Address from Pools is selected or when the calling station requests an address assignment.

Usage: Enter a number between 0 and 254. The default is 0 (zero).

Dependencies: The Range parameter applies only when the calling station uses PPP encapsulation.

See Also: Pool 1 (2), Assign Address from Pools

Require Caller ID (Connections tab)

Description: This field specifies the calling party's phone number (also called caller ID). If authentication by caller ID is enabled by selecting Require Caller ID in the MAX Info tab, the MAX 200Plus compares the caller ID of incoming calls to the value of the phone number you enter here.

Usage: Enter the calling party's phone number, up to 20 characters.

Dependencies: Keep this additional information in mind:

- The connection must be Dial-In enabled to use Caller ID.
- If Caller ID is used to authenticate a call, name-password authentication might also be required, but the parameters of the call are established only by the CLID authentication.

See Also: Require Caller ID

Require Caller ID (MAX Info tab)

Description: This specifies whether the MAX 200Plus uses the calling party's phone number to authenticate incoming calls.

Usage:

- If Require Caller ID is deselected, the calling party information is not required for authentication.

- If Require Caller ID is selected, the calling party's phone number must match the value of the Require Caller ID field in the Connection tab before the MAX 200Plus can answer the call.

  If caller ID is not available, or does not match the Caller ID entered in the Connection tab, the MAX 200Plus does not answer the call

Dependencies: Keep this additional information in mind:

- In some installations, the WAN provider might not be able deliver caller ID, or individual callers might choose to keep their caller IDs private. In addition, caller ID is not available without end-to-end ISDN service on the call and ANI (Automatic Number Identification) from your WAN provider.

  Ask your WAN provider whether the calling party number is conveyed by the network to the receiving party. In some cases, the network does not deliver the calling party number, such as when the MAX 200Plus is behind some PBXs.

See Also: Require Caller ID (Connection tab)

Require Telnet commands

Description: Specifies whether the MAX interprets a command that does not include a keyword as a hostname for a Telnet command. To display the terminal server command keywords, enter help or a question mark (?) from the terminal server command-line interface.

Usage: Specify Yes or No. The default is Yes.

- Yes specifies that the MAX interprets any terminal server command that does not begin with a keyword as though it began with the keyword Telnet. (That is, it interprets the string typed at the prompt as a Telnet hostname.)
- No specifies that all terminal server commands must begin with a keyword.

Restart

Description: This command restarts the MAX 200Plus and clears all calls without disconnecting the device from its power source. The MAX 200Plus logs off all users, and communication with the MAX 200Plus from the Management Console is interrupted until the MAX 200Plus finishes it power-on self tests (POSTs).

RIP

Description: This specifies how the MAX 200Plus handles RIP (Routing Information Protocol) send and receive packets received from its WAN interface.

Note: Ascend recommends that all routers and hosts run RIP-v2 instead of RIP-v1. The Internet Engineering Task Force (IETF) has voted to move RIP version 1 into the "historic" category and its use is no longer recommended.

The MAX 200Plus uses RIP, a protocol in the TCP/IP protocol suite, to dynamically build its routing table. RIP broadcasts routing updates every 30 seconds.

When IP routing is enabled, the MAX 200Plus creates a routing table during initialization. Each entry in the routing table specifies at least two pieces of information: a destination network address, and the router used to forward a packet toward that destination. The routing table contains entries that are learned either from RIP or from any connections you have configured. If RIP is turned off, the MAX 200Plus must rely on the IP parameters configured in a connection to reach a destination.

RIP is always disabled on the Ethernet interface.

- The LAN checkbox controls RIP updates received from the WAN interface to the local Ethernet network.
- The WAN checkbox controls RIP updates across the WAN between the local and remote ends of the link.

Usage:

- LAN

  - Selecting LAN specifies that the MAX 200Plus both sends and receives RIP packets on its Ethernet interface.
  - Deselecting LAN specifies that the MAX 200Plus does not send or receive RIP packets on its Ethernet interface.
- WAN
  - Deselecting WAN specifies that the MAX 200Plus does not generate or receive RIP packets on its WAN interface.

  If you select WAN, the following options are available.
  - Send -v1 indicates that the MAX sends RIP-v1 packets on its WAN interface but does not receive RIP-v1 packets.
  - Receive -v1 indicates that the MAX receives RIP-v1 packets on its WAN interface but does not send RIP-v1 packets.
  - Send & Receive -v1 indicates the MAX sends RIP-v1 packets and receives RIP-v1 packets on its WAN interface.
  - Send -v2 indicates that the MAX sends RIP-v2 packets on its WAN interface but does not receive RIP-v2 packets.
  - Receive -v2 indicates that the MAX receives RIP-v2 packets on its WAN interface but does not send RIP-v2 packets.
  - Send & Receive -v2 indicates the MAX sends RIP-v2 packets and receives RIP-v2 packets on its WAN interface.

Dependencies: Keep this additional information in mind:

- The RIP parameter does not apply if the Route IP is not selected for the connection.

See Also: Route IP

Route IP

Description: This checkbox appears in both the MAX Info tab and the Connections Protocol tab:

- In the MAX Info tab it enables or disables the routing of IP data packets for all connections defined on the MAX 200Plus.
- In the Connections Protocols tab it enables or disables the routing IP data packets for a single connection defined on the MAX 200Plus.

Usage:

- Selecting Route IP enables IP routing for all incoming connections (in the MAX Info tab) or for a single connection (in the Connections Protocol tab).

  IP Routing is enabled by default.
- Deselecting Route IP disables IP routing for all incoming connections (in the MAX Info tab) or for a single connection (in the Connections Protocol tab).

Dependencies: The effect of the Route IP depends upon whether you enable bridging:

- If Enable Bridging is selected and Route IP is selected, the MAX 200Plus routes IP packets, and bridges all other packets.
- If Enable Bridging is selected and Route IP is deselected, the MAX 200Plus bridges all packets.
- If Enable Bridging is deselected and Route IP is selected, the MAX 200Plus routes only IP packets.
- If Enable Bridging is deselected and Route IP is deselected, an error occurs and you cannot save the profile.

  You must enable bridging or routing, or both.

These additional dependencies apply:

- IP routing must be enabled on both the dialing and answering sides of the link.
- Route IP in MAX Info tab applies to all incoming calls. If you deselect it in the MAX Info tab, it disables all IP routing connections.

- Route IP in Connections Protocol tab applies only to the particular connection. If you deselect it in the Connection Protocol tab, it only disables IP routing for that connection.

See Also: Enable Bridging, Encapsulation

Route IPX

Description: This specifies whether or not the MAX 200Plus requests IPX routing for the connection. If the device on the other end of the connection is not configured for IPX routing the connection fails.

This checkbox appears in both the MAX Info tab and the Connections Protocol tab:

- In the MAX Info tab it enables or disables the routing of IPX data packets for all connections defined on the MAX 200Plus.
- In the Connections Protocols tab it enables or disables the routing IPX data packets for a single connection defined on the MAX 200Plus.

Usage:

- Selecting Route IPX enables IPX routing:
  - for all incoming connections (in the MAX Info tab) or
  - for a single connection (in the Connections Protocol tab).
- Deselecting Route IPX disables IP routing:
  - for all incoming connections (in the MAX Info tab) or
  - for a single connection (in the Connections Protocol tab).

  IPX routing is disabled by default.

Dependencies: If the link supports PPP or MPP (Encapsulation is set to PPP or MPP), both sides of the connection must have IPX routing enabled in order for routing to take place.

In addition, the effect of the Route IPX parameter depends upon how you set the Enable Bridging checkbox in the Connection tab:

- If Enable Bridging is selected and Route IPX is selected for a Connection, the MAX 200Plus routes IPX packets, and bridges all other packets.
- If Enable Bridging is selected and Route IPX is deselected for a Connection, the MAX 200Plus bridges all packets.
- If Enable Bridging is deselected and Route IPX is selected for a Connection, the MAX 200Plus only routes IPX packets.
- If both bridging and IPX routing are disabled for a connection, an error occurs and you cannot save the profile.

  You must enable bridging or routing, or both.

See Also: Enable Bridging

Save

Description: The Save command from the File menu saves the active configuration file.

See Also: Update, Update To

Save Configuration As

Description: The Save Configuration As command from the File menu enables you to save all MAX 200Plus configuration information to disk. This configuration file can be used as a backup or to configure another MAX 200Plus using the Update command from the MAX menu.

The process does not save passwords; that is, the Save Configuration command does not save the Enable Dial-In or Enable Dial-Out Passwords or the User Password.

See Also: Update, Update To

Secondary DNS

Description: This specifies the IP address of the secondary domain name server.

Domain Name System (DNS) is a TCP/IP service that enables you to specify a symbolic name instead of an IP address. A symbolic name consists of a username and a domain name in the format <username>@<domain name>. The username corresponds to the host number in the IP address; the domain name corresponds to the network number in the IP address. A symbolic name might be steve@abc.com or joanne@xyz.edu.

DNS maintains a database of network numbers and corresponding domain names on a domain name server. When you use a symbolic name, DNS translates the domain name into an IP address, and sends it over the network. When the Internet service provider receives the message, it uses its own database to look up the username corresponding to the host number.

Usage: Enter the IP address of the secondary domain name server. The address consists of four numbers between 0 and 255, separated by periods. The default value is 0.0.0.0. Accept this default if you do not have a secondary domain name server.

Example: `200.207.23.1`

Dependencies: The Secondary DNS parameter applies only to Telnet and raw TCP connections running under the MAX 200Plus unit's terminal server interface.

A terminal server is a computing device to which a terminal can connect over a LAN or WAN link. The MAX 200Plus supports all the common capabilities of standard terminal servers, including Telnet, Domain Name Services (DNS), login and password control, call detail reporting, and authentication services.

Telnet is a protocol used to link two computers in order to provide a terminal with a connection to the remote machine. The remote machine is known as the Telnet host. When you start a Telnet session, you connect to the Telnet host and log in. The connection enables you to work with the remote machine as though you were at a terminal connected to it.

See Also: Domain Name, Primary DNS

Secondary WINS

Description: This specifies the IP address of the secondary Windows Internet Name Service (WINS) server.

WINS servers are similar to DNS servers, allowing users to log into servers using names instead of IP addresses.

Usage: Enter an IP address in dotted decimal notation. The default is 0.0.0.0.

Dependencies: Secondary WINS applies only to Telnet and raw TCP connections running under the MAX 200Plus unit's terminal server interface.

See Also: Primary WINS

Security

Description: This parameter enables or disables terminal server.

Usage: Specify one of the following values:

For terminal server security, the default is None.

- Full means users are prompted for a name and password upon initial login and when they switch between terminal mode and menu mode.
- Partial means they are prompted for a name and password only when entering terminal mode, not for menu mode.
- None means they are not prompted for a login name and password to enter the terminal server interface.

See Also: Initial Screen, Password, Operator can choose screen

Set Clock

Description: The Set Clock command on the MAX menu allow you to:

- Set the system date at time on the MAX 200Plus
- Synchronize the date and time displayed on the MAX Info tab with the system clock of the PC running the Management Console.

See Also: Clock

Set Password

Description: The Set Password command on the MAX menu allows you to set the password users must enter to access the MAX 200Plus from the Management Console or from Telnet.

We highly recommend that you change this password from its default value (a null string).

See Also: Update

Service Type

Description: Use this checkbox to specify the type of data service the link uses. A data service is provided over a WAN line and is characterized by the unit measure of its bandwidth. A data service can transmit either data or digitized voice.

Usage: You can specify one of the Service Type settings listed in the following table.

Setting	Description
56K	The call contains any type of data and connects to the Switched-56 data service. The only services available to lines using inband signaling (such as Switched-56 lines) are 56K and 56K Restricted.
56K Restricted	The call contains restricted data, guaranteeing that the data the MAX 200Plus transmits meets the density restrictions of D4-framed TI lines. The call connects to the Switched-56 data service. The only services available to lines using inband signaling (such as Switched-56 lines) are 56K and 56K Restricted.
64K	The call contains any type of data and connects to the Switched-64 data service.
Modem	This setting places an outgoing call on any available modem. If no modems are available, the call is not placed. The data rate depends upon the quality of the connections between modems and the types of modems used. The Modem setting requires that your MAX 200Plus has modems installed. Modem applies only when Encapsulation is set to MPP or PPP. Currently, multichannel modem calls are not supported even if Encapsulation is set to MPP.

Dependencies: Keep this additional information in mind:

- If either party requests a data service that is unavailable, the MAX 200Plus cannot connect the call.

See Also: Encapsulation

Silent operation

Description: This parameter suppresses status messages when interactive users establish a terminal server connection.

Usage: Specify Yes or No. The default is No.

- Yes suppresses status messages upon connection of interactive terminal server sessions.
- No sends all status messages.

Dependencies: This parameter is not applicable when terminal services are disabled.

Software version

Description: This displays the version of software currently running on the MAX 200Plus.

SPIDs

Description: This specifies the Service Profile Identifiers (SPIDs) for the ISDN BRI lines. A SPID is a number assigned to a domestic ISDN BRI line for service identification at the central office. It is typically formed by adding a code to the phone number assigned to the line. Your carrier provides you with one or more SPIDs.

All U.S. domestic switch types, except AT&T Point-To-Point, can have two phone numbers. Each phone number requires a corresponding SPID.

When you use AT&T Point-to-Point service, only one phone number is assigned to the ISDN BRI line, and no SPIDs are in use.

Usage: Enter up to 16 characters; you must limit those characters to numbers, hyphens, and parentheses. The default value is 0 (zero).

Dependencies: Keep this additional information in mind:

- You must enter a SPID unless you are using AT&T Point-To-Point (that is, Switch Type set to AT&T Point-To-Point) or you are operating outside of the U.S.
- If the MAX 200Plus uses only one channel of a multipoint ISDN BRI line and another device uses the other channel, you can choose to operate in single-terminal mode.

  Set one channel to unused (Channel B1 set to Unused or Channel B2 is set to Unused), and enter only one SPID. The device sharing the line must enter the other assigned SPID.
- The MAX 200Plus appends the value of the SPID with a TID if you are connected to a Northern Telecom switch running NI-1 (that is, Switch Type set to AT&T Point-To-Point NI-1).

See Also: Channel B1, Channel B2, Numbers, SPIDs, Switch Type

Spoof

Description: This specifies the length of time, in minutes, that the MAX 200Plus performs watchdog spoofing for NetWare connections.

Ordinarily, when a NetWare server does not receive a reply to the watchdog keepalive packets it sends to a client, it closes the connection. When you set Handle IPX to Server, however, the MAX 200Plus replies to NCP watchdog requests on behalf of clients on the other side of the bridge. In other words, the MAX 200Plus performs watchdog spoofing to trick the server watchdog process into believing that the link is still active.

The time period for watchdog spoofing specified by the Spoof parameter begins when the WAN session goes offline. If the WAN session reconnects, the MAX 200Plus cancels the timeout.

Usage: Enter the timeout value in minutes. You can enter any value from 0 to 65535. The default value is 0 (zero). When you accept the default, the MAX 200Plus responds to server watchdog requests indefinitely.

Dependencies: Keep this additional information in mind:

- Spoofing only applies when the MAX 200Plus is on a LAN containing a NetWare server.
- The Spoof time is not applicable when Handle IPX is set to None.

See Also: Handle IPX

Station

Description: This specifies the name of the remote device to which the MAX 200Plus makes a connection.

Usage: Enter the name of the remote device. You can enter up to 31 characters.

The value you specify is case sensitive, and must exactly match the name of the remote device. If you are not sure about the exact name, contact the administrator of the remote network.

Dependencies: Keep this additional information in mind:

- The remote device that the Station specifies is the device actually placing or answering the call; it is not necessarily the same as the source or destination of packets using the link.
- The MAX 200Plus does not currently use the Domain Name System (DNS) to determine the IP address of the device specified by the Station field.
- When the MAX 200Plus receives a PPP or MPP call from an Ascend unit, it tries to match the caller's name to the value of the Station field in some connection.

  If the MAX 200Plus finds a match and authentication is turned on, the MAX 200Plus then tries to match the caller's password to the Enable Dial-In Password in the connection.

See Also: Name, Authentication, Encapsulation

Subnet Mask

Description: This specifies the subnet mask of the MAX 200Plus.

In Ascend units, IP addresses must be specified in decimal (not hexadecimal) format, and can include a netmask modifier. For example, an IP address of

```
198.5.248.40
```

with a netmask of 30, the MAX 200Plus interprets 30 bits as the network portion of the IP address.

The netmask must be greater than the default netmask shown in the following table. If no netmask is specified in an IP address, the following default netmasks are assumed:

Class	Address range	Netmask 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
Class D	224.0.0.0 → 239.255.255.255	N/A
Class E (reserved)	240.0.0.0 → 247.255.255.255	N/A

The example address is a class C address, so the default netmask is 24 bits. If the address has a subnet of 30, this indicates that an additional 6 bits of the address be interpreted as a subnet number.

That is, the first 24 bits of the address are interpreted as the IP network number (standard for Class C), the next 6 bits are the subnet number, and only 2 bits are available for host number assignment. A 2-bit host portion allows only four hosts on that subnet.

Dependencies: Keep this additional information in mind:

- If the MAX 200Plus is connected to a local subnet and connects to a remote subnet of the *same* IP network, both sides of the connection must use the same subnet mask.

See Also: IP address

Switch Type

Description: This specifies the network switch that provides ISDN BRI lines to the MAX 200Plus.

A switch is the device that connects the calling party to the answering party. The connection is a switched circuit consisting of one or more channels.

Usage: You can select one of the BRI switch types listed int he following table:

Switch type	Explanation
AT&T	The default is AT&T.
NI-1	National ISDN-1
NT1	Northern Telecommunications, Inc.
U.K.	United Kingdom: ISDN-2 Hong Kong: HKT Switchline BRI Singapore: ST BRI Euro ISDN countries: Austria, Belgium, Denmark, Finland, Germany, Italy, Netherlands, Portugal, Spain, Sweden
SWISS	Switzerland: Swiss Net 2
GERMAN	Germany 1TR6 version: DBP Telecom
MP GERMAN	Germany: 1TR6 multipoint
FRANCE	France: FT Numeris
DUTCH	Netherlands 1TR6 version: PTT Netherlands BRI
BELGIUM	Belgium: Pre-Euro ISDN Belgacom Aline
JAPAN	Japan: NTT INS-64
AUSTR	Australia and New Zealand

Dependencies: Keep this additional information in mind:

- The Switch Type does not apply to a link using inband signaling (that is, if Service Type is set to 56K or 56K Restricted).

  For inband signaling, a line uses 8 kbps of each 64-kbps channel for WAN synchronization and signaling. The remaining 56 kbps handle the transmission of user data.
- The Switch Type applies only if the you have ISDN BRI PC Cards.
- All international switch types except German operate in multipoint mode.

See Also: Numbers, SPIDs, Channel B1, Channel B2

Update

Description: The Update command on the MAX menu updates the MAX 200Plus configuration with the file currently on the PC running the Management Console. Whenever you make a change to the MAX 200Plus configuration, you must select Update to apply the changes to the MAX 200Plus.

Updating the configuration replaces the current MAX 200Plus configuration with the configuration in the Management Console. Because of this, you must make sure that no one else makes any configuration changes to the MAX 200Plus at the same time as you are. We highly recommend you change the Connect password from its default (a null string) using the Set Password command on the MAX menu.

See Also: Update To, Set Password

Update To

Description: The Update To command on the MAX menu allows you to update one MAX 200Plus with the configuration of another MAX 200Plus. Updating the configuration replaces the current MAX 200Plus configuration with the configuration in the Management Console.

When you use this command, it replaces any IP or IPX configuration information on the target MAX 200Plus with the IP or IPX configuration of the source MAX 200Plus. This could cause problems with your network configuration, since two different devices are sharing the same information. We recommend that if you use the Update To command, you first change any IP or IPX configuration information.

See Also: Update, Set Password

WAN Network

Description: This specifies a unique IPX network number for all NetWare clients that are running PPP encapsulation and dialing in directly. The MAX 200Plus assigns network addresses to dial-in NetWare clients when they connect to the MAX 200Plus; these addresses are derived from this network number.

When you enter a value for the WAN Network #, the MAX 200Plus advertises a route to this network.

Usage: Enter an Ethernet network number using an 8-digit (4-byte) hexadecimal value. The default is 00000000. The number you specify must be unique within your wide area IPX network, and must match the configuration of other routers on the local Ethernet network.

Dependencies: Keep this additional information in mind:

- The dial-in Netware client must accept the network number set by the WAN Network #, although it can provide its own node number or accept a node number provided by the MAX 200Plus.
- If Enable IPX is disabled, the WAN Network # is not applicable.

Example: FF0000037

See Also: Enable IPX, LAN Network #

Zone

Description: This specifies the name of the AppleTalk zone in which the MAX resides. If the local Ethernet supports an AppleTalk router with configured zones, you can place the MAX in one of those zones.

Usage: Enter the name of a zone that has been configured on the local Ethernet. If you don't specify a name and AppleTalk is enabled, the MAX is placed in the default zone (denoted by an *).

Dependencies: Allow ARA is not applicable if Enable Appletalk is not selected in the Protocol tab.

Using AppleTalk Remote Access and MacTCP

A

This appendix describes what you need to know to configure and use Apple Remote Access (ARA) and MacTCP. ARA allows you to dial into to the MAX 200Plus with a Macintosh; MacTCP allows you to run TCP/IP on your Macintosh.

This appendix includes:

What is Apple Remote Access?

Apple Remote Access (ARA) is software that allows your System 7 Macintosh to communicate with another Macintosh, AppleTalk network, or remote networking server over standard telephone lines giving quick, direct access to information and shared resources like file servers, printers, and electronic mail from a remote location.

Use MAX 200Plus in conjunction with ARA to connect Macintosh computers to a Local Area Network (LAN) by modem.

The Apple Remote Access Client may be purchased from Apple Computer, Inc. For more information regarding installation or use of Apple Remote Access, refer to the *Apple Remote Access Client User's Guide* by Apple Computer, Inc.

Accessing the MAX 200Plus using a mobile computer

This section assumes that you have already installed Apple Remote Access and are ready to use it to connect to an AppleTalk network. It also assumes that you are calling from a remote location with a Macintosh and properly connected modem.

Before dialing, make sure you contact the network administrator for your login name, password, and phone number associated with the MAX 200Plus you are calling.

Creating a document

Before you connect to MAX 200Plus, create a remote access document. The document is an AppleTalk Remote Access file that contains information that the remote access software needs to make the connection to your MAX 200Plus. You can create several connection documents with different names representing their intended dial-up connection.

To create an ARA document:

1 Launch AppleTalk Remote Access by double-clicking this icon. An Untitled AppleTalk Remote Access document will open. If File Sharing

is running on your Macintosh, your owner name will appear in the documents Name text field.

2 Either select the Guest or Registered User connect option. The Guest user option will only work if the network administrator has set up the Console to allow Guest connections. If you log on as a guest user, you will not need to type a name or password.

3 If you are a registered user, type in your name exactly the same as the network administrator set up for you. If your name already appears in the Name field, make sure that it matches the name the network administrator assigned to you. Type your name and press the Tab key.

Note: The name you enter in the Name text field is **not** case-sensitive, but the Password **is** case-sensitive.

4 Type your password (if required) followed by the Tab key.

5 Type the phone number of the modem you are calling in the number field.

Note: Dashes are not required in the phone number, but may be used. Do not use parentheses or spaces. If you must dial “9”to get an outside line, insert the “9”. If you start a number with “1”or “9” use a comma after the “1” or “9” to give the modem time to pause while waiting for the long distance or outside line.

6 Click the Save my password checkbox to save your password within the connection document. If you do this, it won’t be necessary to insert a password every time you try to make that particular connection.

7 Save the connection document by selecting Save As in the File menu. You will be asked to select a name for the document. It is a good idea to select a name that represents the place the document will be calling, such as “Sales Office.”

Making the Call

Once you are connected to the network through Apple Remote Access, you will be able to see the status of your connection in the Remote Access Status window. This window lists the amount of time you have been connected and amount of time you have left.

Understanding MacTCP

MacTCP is a Control Panel that allows you to use TCP/IP protocols with your Macintosh. A Macintosh must be running MacTCP to take advantage of MAX 200Plus set port IP addresses. These instructions are for setting up MacTCP for MAX 200Plus defined IP addressing. This section describes these topics:

- MacTCP overview
- Setting up MacTCP
- Using MacTCP

MacTCP overview

Make sure you have the correct IP address and domain name for the Domain Name Server and IP Address class type. If you want to set your IP address manually, you must also get the correct gateway address and individual address for your computer from the network or system administrator. Refer to the documentation for MacTCP for more information about setting up MacTCP for manual addressing and any other questions. MacTCP comes with System 7.5, although you may need to add it to your computer with a Custom Install of the system software. If you do not have System 7.5, you can purchase MacTCP from Apple Computer, Inc.

Dynamic addressing and MacTCP

MacTCP's dynamic addressing mode is not supported with the MAX 200Plus, either for dial-in connections, or for LAN-based stations. MacTCP Dynamic addressing should not be used on any LAN to which the MAX 200Plus is attached. Automatic address assignment for dial-in connections using the MAX 200Plus address pools *is* supported using the "Server" setting in MacTCP.

Setting up MacTCP for dial-in connections over ARA

To set up MacTCP:

1. Establish an ARA call to the MAX 200Plus as explained in “Accessing the MAX 200Plus using a mobile computer” on page A-2.
2. Open the Control Panels.
3. Double-click MacTCP control panel.
4. Select the “Remote Only” icon in the upper window pane.
5. Select the MAX 200Plus zone from the pop-down zone list that appears at the bottom of the icon.
6. If EtherTalk is available, select it by clicking the icon. Otherwise select LocalTalk.
7. Click More. This window opens.
8. Click Server in the Obtain Address pane.
9. Select the correct Class for the IP address in the pop-up menu.
10. Enter the Domain Name Server and IP address, and click the Default radio button, if desired.
11. Click Close.
12. Click the close box to close the MacTCP control panel.

Using MacTCP

Dial-up the MAX 200Plus server with ARA as described in the “What is Apple Remote Access?” on page A-2. If the MAX 200Plus you are calling into is in the default network zone, you can use TCP/IP immediately. If it is in another zone, follow these steps:

1. Terminate the ARA call.
2. Restart the computer.
3. Re-establish the call.

You won’t have to change the zone in the MacTCP control panel again, unless you dial-up a MAX 200Plus server in a different zone. Now you should be able to run software that relies on IP addressing (such as Telnet or Netscape).

Index

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

W