MultiVoice Gateway for the MAX— User's Guide

Ascend Communications, Inc.
Part Number: 7820-0583-002
For software version 7.0.0
November 2, 1998

Ascend Customer Service

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

Obtaining technical assistance

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

Enabling Ascend to assist you

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

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

Calling Ascend from within the United States

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

Priority Technical Assistance

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

Ascend Advantage Pak

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

Other telephone numbers

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

Calling Ascend from outside the United States

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

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

For a list of support options in the Asia Pacific Region, you can find additional support resources at `http://apac.ascend.com`

Obtaining assistance through correspondence

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

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

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

Finding information and software on the Internet

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

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

Important safety instructions

The following safety instructions apply to the MultiVoice Gateway:

1 Product installation should be performed by trained service personnel only.

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

3 The maximum recommended ambient temperature for MultiVoice Gateway models is 104° Fahrenheit (40° Celsius). Take care to allow sufficient air circulation or space between units when the MultiVoice Gateway is installed in a closed or multirack assembly, because the operating ambient temperature of the rack environment might be greater than room ambient.

4 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.

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

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

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

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

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

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

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

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

13 If using DC power, connect the equipment to a 48 VDC supply source that is electrically isolated from the ac source. The 48 VDC source should be reliably connected to earth ground.

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

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

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

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

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

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

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

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.
- Avoid using equipment connected to telephone lines (other than a cordless telephone) during an electrical storm. There is a remote risk of electric shock from lightning.
- Do not use a telephone or other equipment connected to telephone lines to report a gas leak in the vicinity of the leak.

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

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

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

Contents

Figures

Tables

About This Guide

This guide explains how to install, configure, and test the MultiVoice Gateway for the MAX hardware. It also explains how to navigate the user interface. When you finish with the instructions in this guide, you will be ready to configure the MultiVoice Gateway.

Caution: MultiVoice Gateways running Ascend's True Access Operation System (TAOS) Release 7.0.0 are not backwards compatible with Gateways running Release 6.x.x. Calls placed between Gateways running different releases will fail. You must upgrade all Gateways to Release 7.0.0.

How to use this guide

This guide contains the following chapters:

- Chapter 1, "Introducing MultiVoice Gateway concepts," gives a brief overview of traditional voice communications and describes several applications of MultiVoice Gateway in a voice communications network.
- Chapter 2, "Getting Acquainted with the MultiVoice Gateway," lists the MultiVoice Gateway features as they apply to various applications.
- Chapter 3, "Setting Up the MultiVoice Gateway Hardware," explains how to install and test the MultiVoice Gateway hardware.
- Chapter 4, "Navigating the User Interface," introduces the user interface and explains how to navigate to configuration menus.
- Chapter 5, "Configuring the WAN Interfaces,"shows you how to configure the MultiVoice Gateway for various types of WAN connectivity.
- Chapter 6, "Configuring MultiVoice," explains how to set up the MultiVoice call operations parameters.
- Chapter 7, "Configuring Frame Relay,"explains how to set up your connections for Frame Relay.
- Chapter 8, "Configuring IP Routing,"explains how to configure the MultiVoice Gateway for IP routing.
- Chapter 9, "Configuring OSPF Routing,"explains how to configure the MultiVoice Gateway for this Internet routing protocol.
- Chapter 10, "MultiVoice Gateway System Administration," explains how to administer and manage the MultiVoice Gateway.
- Appendix A, "Troubleshooting," discusses hardware and software troubleshooting tips.
- Appendix B, "Provisioning the Switch," explains provisioning of T1, E1, ISDN PRI and ISDN BRI lines.

- Appendix C, “MultiVoice Gateway Technical Specifications,” details specifications of the MultiVoice Gateway.
- Appendix D, “Cables and Connectors,” discusses MultiVoice Gateway cabling.
- Appendix E, “Warranties and FCC Regulations,” discuss warranty information, and FCC and Canadian notices.

Note: This manual describes the full set of features for the MultiVoice Gateway running software version7.0.0. Some features might not be available with older versions or specialty loads of the software.

What you should know

Describe the skills and knowledge a user must have to perform the tasks described in the manual. For example:

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

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

Documentation conventions

Following are all the special characters and typographical conventions used in this manual:

Convention	Meaning
`Monospace text`	Represents text that appears on your computer’s screen, or that could appear on your computer’s screen.
`Boldface mono-space text`	Represents characters that you enter exactly as shown (unless the characters are also in ***`italics`***—see *Italics*, below). If you could enter the characters but are not specifically instructed to, they do not appear in boldface.
Italics	Represent variable information. Do not enter the words themselves in the command. Enter the information they represent. In ordinary text, italics are used for titles of publications, for some terms that would otherwise be in quotation marks, and to show emphasis.
[ ]	Square brackets indicate an optional argument you might add to a command. To include such an argument, type only the information inside the brackets. Do not type the brackets unless they appear in bold type.
|	Separates command choices that are mutually exclusive.
>	Points to the next level in the path to a parameter or menu item. The item that follows the angle bracket is one of the options that appears when you select the item that precedes the angle bracket.

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

Related publications

This guide does not provide a detailed explanation of products, architectures, or standards developed by other companies or organizations.

Following are some related publications:

- *MultiVoice Access Manager User's Guide*, Ascend Technical Publications
- *Delivering Voice over IP Networks*, Dan Minoli, Emma Minoli, Daniel Minoli
- *Delivering Voice Over Frame Relay and ATM*, Dan Minoli
- *The Guide to T1 Networking*, William A. Flanagan
- *TCP/IP Illustrated*, W. Richard Stevens
- *Firewalls and Internet Security,* William R. Cheswick and Steven M. Bellovin

Following are some related World Wide Web (WWW) sites:

- `http://www.itu.ch/`
- `http://www.imtc.org/main.htm`
- `http://www.cs.columbia.edu/~hgs/rtp/drafts/VoIP97-8.pdf`
- `http://www.cs.columbia.edu/~hgs/rtp/`
- `http://dcs.umd.edu/~mark/631paper.html`
- `http://www.phonezone.com/tutorial/`

Note: The listed WWW sites were available at the time of this manual's printing. Ascend does not maintain the sites, and cannot guarantee their availability in the future.

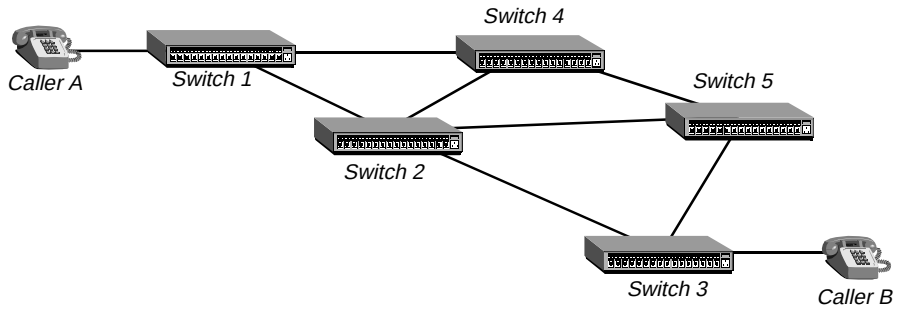
Introducing MultiVoice Gateway concepts 1

A brief overview

Traditionally, real-time voice information is sent over the Public Switched Telephone Network (PSTN). Circuit-switched technology provides every call with dedicated bandwidth, usually 64Kbps. End-to-end calls are established on the basis of a sequence of dialed digits, and the PSTN dedicates a physical path between callers. Because the telephone equipment establishes the call path at the beginning of the call, the path can change *between* calls, but never while a call is active.

Figure 1-1 illustrates an example of a PSTN network. Caller A dials Caller B's phone number. As Caller A dials the phone number, the network might route the call from Switch 1 to Switch 2 to Switch 3, which connects to Caller B. Once the PSTN establishes the call, communication travels only through Switch 1, Switch 2, and Switch 3.

Figure 1-1. Example of call routing over circuit-switched PSTN



If Caller A dials Caller B again, the PSTN might establish the call by routing it from Switch 1 to Switch 4 to Switch 5 to Switch 3 before finally connecting Caller A to Caller B. Again, the path can change between calls, but not during any specific call.

In contrast, an Internet Protocol (IP) network has a packet-switched architecture. Devices transmit data in packets, and the path from end to end can vary within an established session.

In addition to data, packets contain addressing information, which routing devices use to send information to its destination. Routing devices maintain tables which instruct them how to direct packets. Dynamic protocols, like RIP or OSPF, define methods that routing devices use to update each other as networking environments change.

In the past, the PSTN was the only network supporting voice communication. With the introduction of MultiVoice Gateway, voice traffic can be sent over IP-based packet-switched networks.

What is MultiVoice for the MAX?

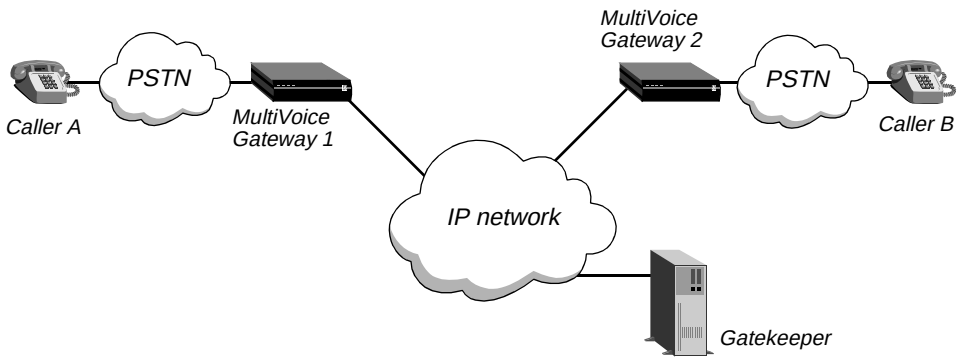
In response to customers wanting to utilize their existing IP networks to support voice communications, the International Telecommunications Union (ITU) has created the ITU-T H.323 standards. H.323 standards define a framework for the transmission of real-time voice communications by means of IP-based packet-switched networks.

In particular, H.323 standards define a Gateway and a Gatekeeper. Gateways connect the PSTN to the IP-based network. Callers dial a local Gateway, which provides them access to the IP network and, ultimately, to the destination phone. The Gatekeeper manages the network, supporting all Gateways, user profiles, and authentication.

Basic Multivoice network

MultiVoice for the MAX implements the H.323 direct call model for Voice over IP networks. Figure 1-2 shows an example of a MultiVoice network. Two Gateways connect Caller A to Caller B. A computer running the MultiVoice Access Manager (MVAM) is the Gatekeeper.

Figure 1-2. Example of a MultiVoice network



When Caller A dials Caller B, the following events occur:

1 Caller A dials MultiVoice Gateway 1, and enters their PIN authentication (if required) and Caller B's phone number.

2 MultiVoice Gateway 1 establishes a session with the Gatekeeper.

3 MultiVoice Gateway 1 forwards the phone number and PIN authentication to the MultiVoice Access Manager.

4 The Gatekeeper authenticates Caller A and, if successful, forwards the IP address of MultiVoice Gateway 2 to MultiVoice Gateway 1.

5 MultiVoice Gateway 1 establishes a session with MultiVoice Gateway 2.

6 MultiVoice Gateway 2 forwards the call request to Caller B.

When Caller B answers the phone (goes off-hook), voice traffic is tunneled in IP packets, using the IETF-standardized RTP protocol, between MultiVoice Gateway 1 and MultiVoice Gateway 2.

If the callers in Figure 1-2 used a traditional voice communications network, Caller A would require a long-distance carrier's services to reach Caller B. But, Caller A is in MultiVoice Gateway 1's *coverage area*, and can reach the Gateway with a local call. The IP-routed network performs the same function as a long-distance carrier's circuit-switched network.

Coverage Areas

Each MultiVoice Gateway services a coverage area, a group of telephone numbers that may dial and receive calls through a particular MultiVoice Gateway. Coverage areas for each MultiVoice Gateway are defined by assigning dial strings, such as country codes, area codes, country code/area code combinations, area code/exchange combinations or complete telephone numbers, and so forth, to a database on the Gatekeeper.

Individually, these phone numbers and dial strings represent individual *inclusion areas*. Together, these inclusion areas represent the coverage area for a MultiVoice Gateway. For example, an inclusion area may be specified by the partial telephone number '1732'. This number is composed of a country code of '1' and area code of '732'. A MultiVoice Gateway with this inclusion area would cover all telephone numbers within the 732 area code.

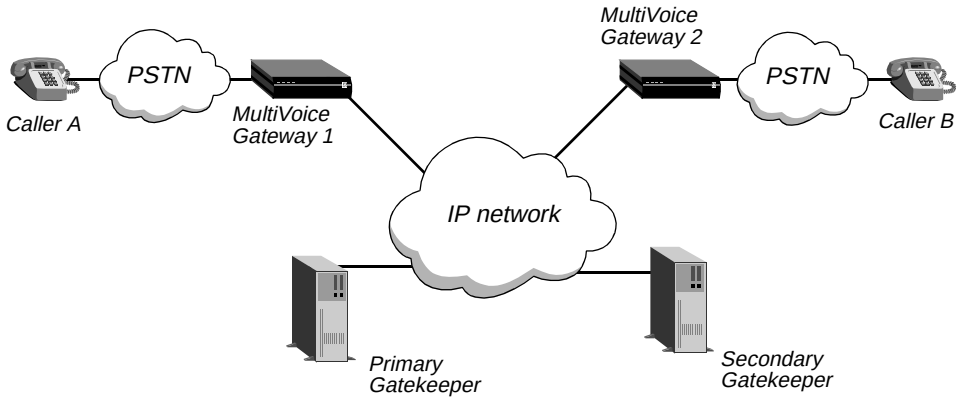
Multivoice network with a secondary Gatekeeper

Figure 1-3 shows an example of a MultiVoice network processing a call through a secondary Gatekeeper. The secondary Gatekeeper configuration is designed to provide the MultiVoice network with redundant call management capability.

Starting with TAOS Release 7.0.0, each MultiVoice Gateway may be configured to register with a secondary Gatekeeper when it cannot register with the primary Gatekeeper. This enables call processing to continue in the event that the primary Gatekeeper cannot be reached by a MultiVoice Gateway.

As illustrated in Figure 1-3, two MultiVoice Gateways connect Caller A to Caller B. Either of the systems running the MultiVoice Access Manager can be the Gatekeeper.

Figure 1-3. Example of a MultiVoice network with a secondary Gatekeeper



When Caller A dials Caller B, the following events occur:

1 Caller A dials MultiVoice Gateway 1, and enters their PIN authentication (if required) and Caller B's phone number.

2 MultiVoice Gateway 1 attempts to register with it's primary Gatekeeper.

If the registration fails, MultiVoice Gateway 1 attempts to register with its secondary Gatekeeper.

3 When registration is established with the secondary Gatekeeper, MultiVoice Gateway 1 forwards the phone number and PIN authentication to the secondary Gatekeeper.

4 The secondary Gatekeeper authenticates Caller A and, if successful, forwards the IP address of MultiVoice Gateway 2 to MultiVoice Gateway 1.

5 MultiVoice Gateway 1 establishes a session with MultiVoice Gateway 2.

6 MultiVoice Gateway 2 forwards the call request to Caller B.

The primary and secondary Gatekeepers are separate systems (Gatekeepers), each running its own copy of the MVAM application, and are designed to function independent of the other. Each Gatekeeper has unique gateway and user databases, and each maintains separate call and activity logs. To ensure coverage, the two Gatekeepers must duplicate gateway and user information. The secondary Gatekeeper does not report call activity to, nor share call records with the primary Gatekeeper.

Gatekeeper registration policy and failure detection

Registration with the primary Gatekeeper fails when the MultiVoice Gateway cannot register within five (5) registration attempts, at 5-seconds intervals, unless you change the defaults. If registration fails, the MultiVoice Gateway does one of the following:

- The MultiVoice Gateway attempts to register with the secondary Gatekeeper, if a valid IP address (non-null) is configured for the `2nd GK IP` parameter. The same registration policy applies (five registration attempts at five-second intervals) as with the primary Gatekeeper.

- The MultiVoice Gateway goes into a *slow poll* mode, in which it attempts to register with the primary Gatekeeper at 30-second intervals, if no valid IP address is configured for the `2nd GK IP` parameter.

Reregistration policy

Once the MultiVoice Gateway registers with the secondary Gatekeeper, it periodically attempts to reregister with the primary Gatekeeper. It makes one attempt after every five successful registrations with the secondary Gatekeeper. The same registration-failure detection policy applies. That is, if the MultiVoice Gateway cannot register with the primary Gatekeeper within five registration attempts, it discontinues the attempts and it maintains registration with the secondary Gatekeeper.

Note: While attempting to register with the primary Gatekeeper, the MultiVoice Gateway is effectively *unregistered* with any Gatekeeper. During this period, new calls are blocked. However, existing calls continue to operate normally.

Keep-alive registration

Once registered with a Gatekeeper, the MultiVoice Gateway reregisters every 120 seconds. This is called *keep-alive registration*. When keep-alive registration fails, the MultiVoice Gateway attempts to register with the secondary Gatekeeper, provided both a primary and secondary Gatekeeper are configured. Without a secondary Gatekeeper, the MultiVoice Gateway goes into a slow poll mode with its current Gatekeeper.

MultiVoice Access Manager uses the `registrationDuration` parameter to set the interval when a MultiVoice Gateway registration expires. This parameter defaults to 150 seconds, adding a 30-second buffer to the reregistration interval.

For example, if the MultiVoice Gateway is registered with the secondary Gatekeeper and keep-alive registration fails, then the Gateway attempts to use the primary Gatekeeper (assuming the `GK IP Adrs` parameter is non-null).

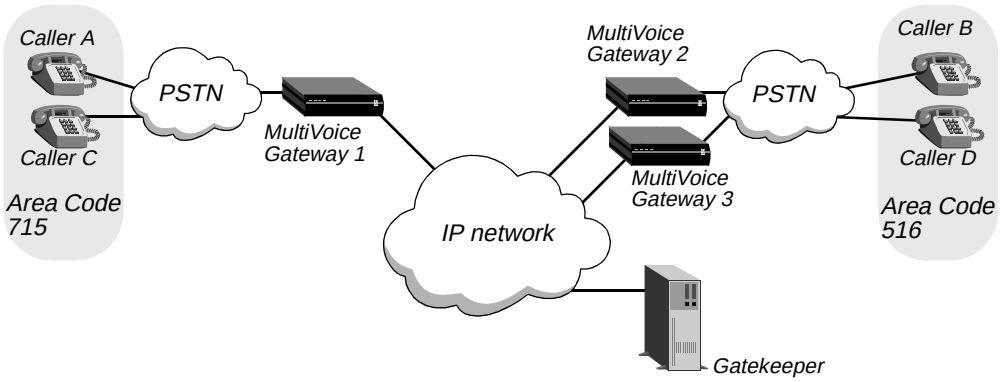
MultiVoice network with overlapping coverage areas

In a MultiVoice network with overlapping coverage areas, two or more MultiVoice Gateways can process in-coming calls to telephone numbers in the same coverage area.

Identical coverage areas may be configured on the Gatekeeper for each MultiVoice Gateway in the group. This type of network configuration provides for dynamic call management, allowing the Gatekeeper to perform call load-leveling across a group of MultiVoice Gateways.

Figure 1-4 shows an example of a MultiVoice network using overlapping coverage areas. Two Gateways provide coverage to area code 516. The MultiVoice Access Manager is the Gatekeeper.

Figure 1-4. Example of a MultiVoice network with overlapping coverage areas



When Caller A dials Caller D, then Caller C dials Caller B, and both dialed phone numbers are part of the same coverage area, the following events occur:

1 Caller A dials MultiVoice Gateway 1, and enters their PIN authentication (if required) and Caller D's phone number.

2 MultiVoice Gateway 1 establishes a session with the Gatekeeper.

3 MultiVoice Gateway 1 forwards the phone number and PIN authentication to the Gatekeeper.

4 The Gatekeeper attempts to authenticate Caller A and, if successful, identifies all the MultiVoice Gateways that support the coverage area for Caller D's phone number.

5 The Gatekeeper then forwards the IP address of MultiVoice Gateway 2 to MultiVoice Gateway 1.

6 MultiVoice Gateway 1 establishes a session with MultiVoice Gateway 2.

7 MultiVoice Gateway 2 forwards the call request to Caller D.

8 Now, Caller C dials MultiVoice Gateway 1, and their PIN authentication (if required) and Caller B's phone number.

9 MultiVoice Gateway 1 establishes a session with the Gatekeeper.

10 MultiVoice Gateway 1 forwards the phone number and PIN authentication to the Gatekeeper.

11 The Gatekeeper attempts to authenticate Caller C and, if successful, identifies the MultiVoice Gateways that support the coverage area for Caller B's phone number.

12 This time the Gatekeeper forwards the IP address of MultiVoice Gateway 3 to MultiVoice Gateway 1

13 MultiVoice Gateway 1 establishes a session with MultiVoice Gateway 3.

14 MultiVoice Gateway 3 forwards the call request to Caller B.

Since one DSP can only process one call at a time, the Gatekeeper will attempt to assign calls to each MultiVoice Gateway based upon DSP availability, alternating call assignments between covering Gateways.

In this figure, the Gatekeeper, having already routed a call from Caller A to Caller D through MultiVoice Gateway 2, determined that the call from Caller C to Caller B should be routed through MultiVoice Gateway 3 instead of MultiVoice Gateway 2; to keep the call volume balanced.

How overlapping coverage areas work

The MultiVoice Access Manager allows you to assign the same Inclusion Areas, defined by country codes, area codes, country code/area code combinations, area code/exchange combinations or complete telephone numbers, and so forth, to two or more MultiVoice Gateways, creating overlapping coverage areas.

How calls are assigned to a MultiVoice Gateway

When a call request is received from a MultiVoice Gateway, the MVAM first identifies all the MultiVoice Gateways that could be used to complete the call. The MVAM then assigns calls applying the following criteria:

- Assign the call to the MultiVoice Gateway that has the closest (longest number) match between the called number and the Inclusion Area.
- Assign subsequent calls for that Inclusion Area to the next MultiVoice Gateway which services that Inclusion Area.

Suppose the Gatekeeper receives a request from a MultiVoice Gateway to connect a call to 516-555-1111, and the Gatekeeper then identifies two registered MultiVoice Gateways whose coverage areas include 516-555 and 516-555-11, respectively, as Inclusion Areas. The Gatekeeper attempts to connect the call through the MultiVoice Gateway with the 516-555-11 Inclusion Area.

If both MultiVoice Gateways have 516-555-11 as an Inclusion Area, the Gatekeeper assigns the call to the first MultiVoice Gateway it located, then connects the next call for that Inclusion Area through the next MultiVoice Gateway.

Note: If the call is rejected by the selected MultiVoice Gateway, the call is dropped.

MultiVoice applications

MultiVoice supports a variety of applications, including:

- Basic public long-distance service
- Local 800 service
- Point-to-Point Private Branch Exchange (PBX) trunk extensions
- PBX trunk intraflow
- PC-to-phone over a VPN

Basic public long-distance service

Basic public long-distance service is the most beneficial to Competitive Local Exchange Carriers (CLECs) and Internet Service Providers (ISPs) that:

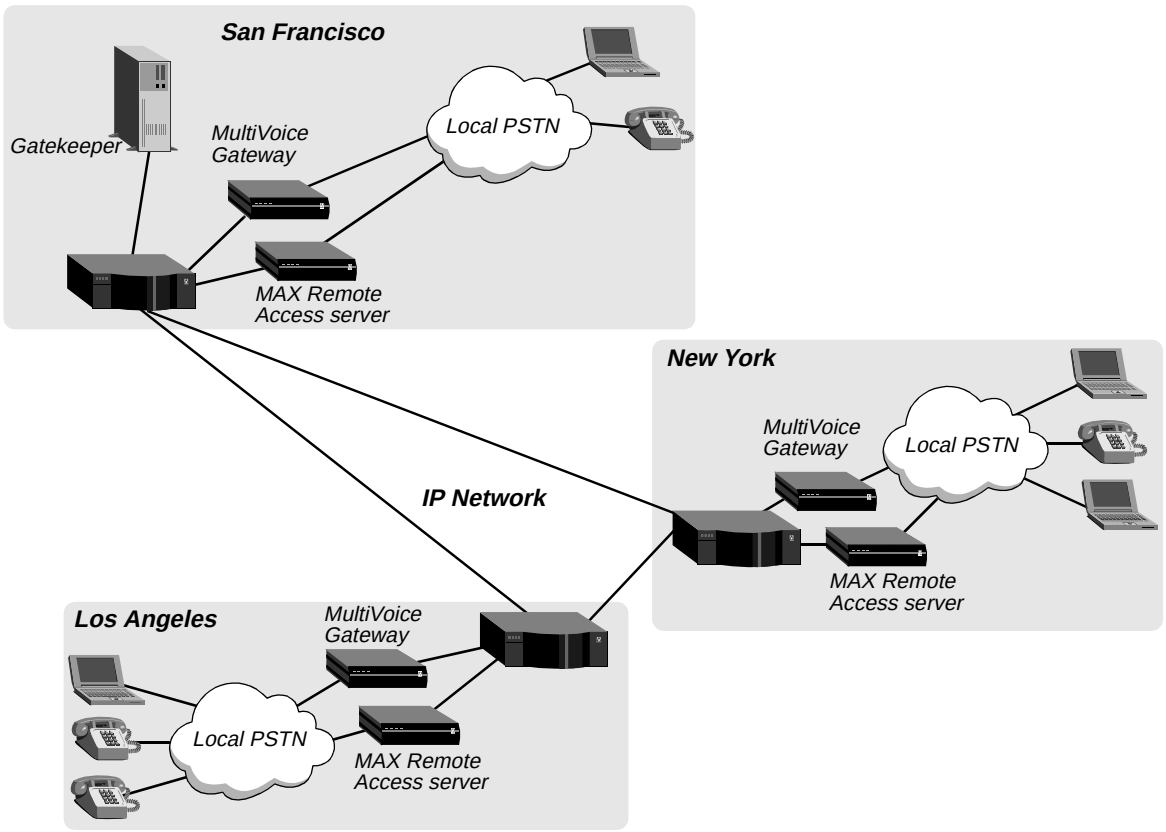
- Have an existing, extensive IP network
- Want to offer long-distance services to their customers

The IP network should be a managed infrastructure that maintains Quality of Service (QoS). Unmanaged IP networks have difficulty with consistent support for the real-time requirements of transporting voice traffic. Whereas delays due to traffic congestion are usually only an inconvenience when sending or receiving data traffic, such delays can cause more functional problems with voice traffic. In maintaining QoS, a network gives voice traffic a higher transport priority than data traffic, guaranteeing timely delivery of the voice traffic.

For networks which support service precedence, MultiVoice for the MAX provides options for configuring the Type of Service byte. The VoIP administrator may change the Precedence bits (bit0 - bit2) and the TOS bits (bit3 - bit6) of the ToS byte contained in the UDP packet header. This changes the network priority for processing UDP packets by setting user defined values for delay, throughput and reliability.

Figure 1-5 shows an example of an ISP network offering connectivity between New York, Los Angeles, and San Francisco.

Figure 1-5. Example of an ISP offering data and voice services



At each Point of Presence (PoP) in the figure, the ISP configures one MAX unit dedicated to supporting voice traffic and another MAX unit dedicated to supporting data services. Each MultiVoice Gateway and MAX Remote Access server is connected to a backbone IP router, which connects all PoPs over an IP network. System administrators use the Gatekeeper in San Francisco, to manage the MultiVoice network.

The ISP supplies MultiVoice customers with the phone number of a local MultiVoice Gateway. Data customers, using modems or ISDN devices, dial the phone number of a local MAX Remote Access server. All customers send traffic over the same IP network.

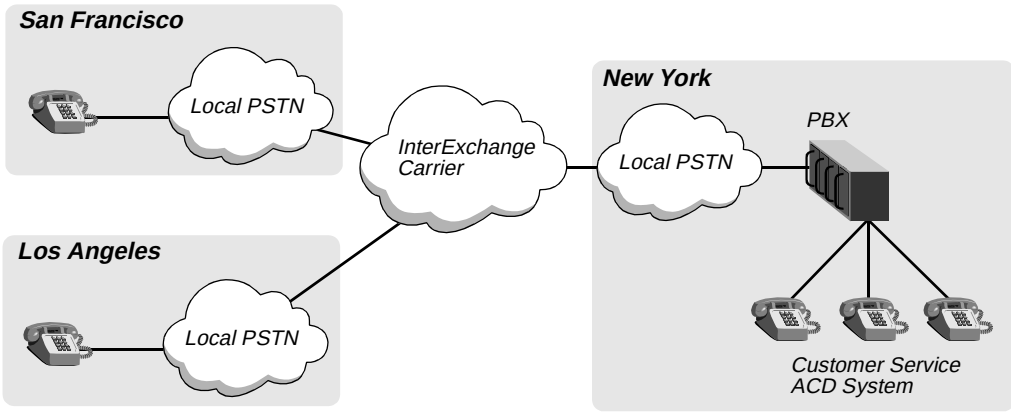
Local 800 service

For example, local 800 or 888 service can be much more cost-effective than traditional 800 or 888 service. Typically, leasing charges are less, and MultiVoice technology can eliminate long-distance phone charges. Suppose a company maintains a customer service department, offering their customers a traditional 800 or 888 phone number that they dial to receive assistance.

Example of traditional 800 service

Figure 1-6 shows an example of an environment without MultiVoice:

Figure 1-6. Traditional 800 environment



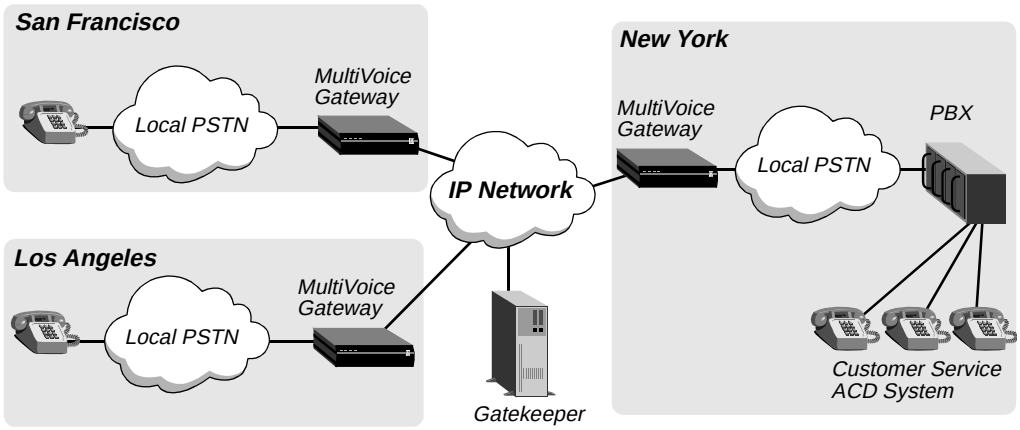
To reach a customer service representative, callers in San Francisco and Los Angeles dial an 800 or 888 phone number, which has been leased to a company's customer service department by its InterExchange Carrier (IXC).

The IXC routes the calls to the company's Automatic Call Distributor (ACD) system through a PBX. Because the dialed number is toll-free for the caller, the IXC bills the company for any long-distance charges, in addition to the leasing charges for the 800 service.

Example of using MultiVoice and local 800 service

Figure 1-7 illustrates how a company can use MultiVoice devices and local 800 service.

Figure 1-7. Using MultiVoice and local 800 service

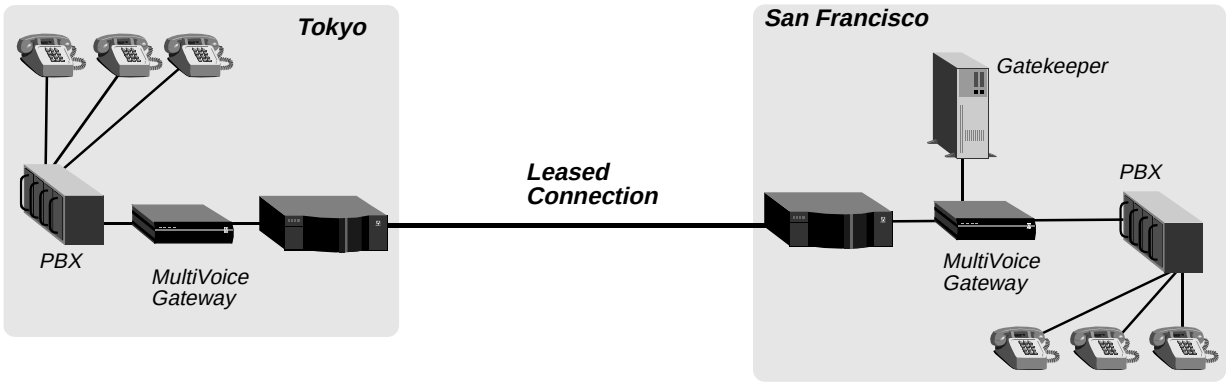


Instead of leasing traditional 800 service, the company leases local 800 service in San Francisco and Los Angeles. Each local PSTN routes local 800 calls to a local MultiVoice Gateway, which forwards them to the customer service site in New York.

Point-to-Point PBX trunk extension

Figure 1-8 shows an example of two locations connected by MultiVoice in a point-to-point configuration.

Figure 1-8. Connecting two sites by MultiVoice and a leased connection

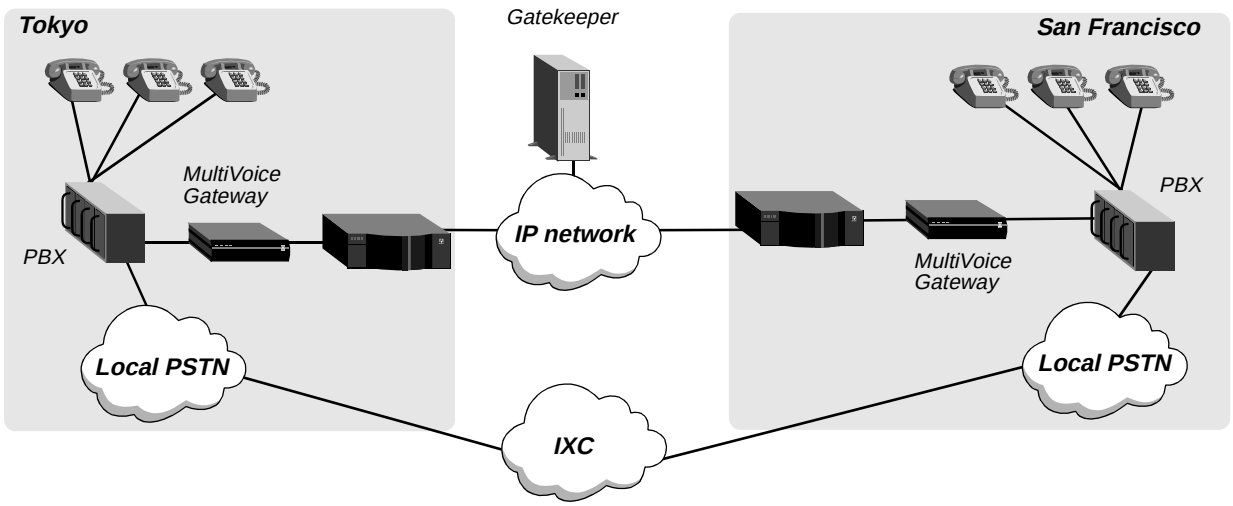


The two sites are connected by a core B-STDX network, which supports both packetized data and voice traffic. The Priority Frame standard within the B-STDX network maintains QoS.

Fault-tolerance and PBX trunk intraflow

Figure 1-9 shows connection used by a company with a managed IP network and an alternative method for connecting two sites. The alternative path gives the company fault-tolerant connectivity between the two sites.

Figure 1-9. Alternative voice-traffic paths between sites



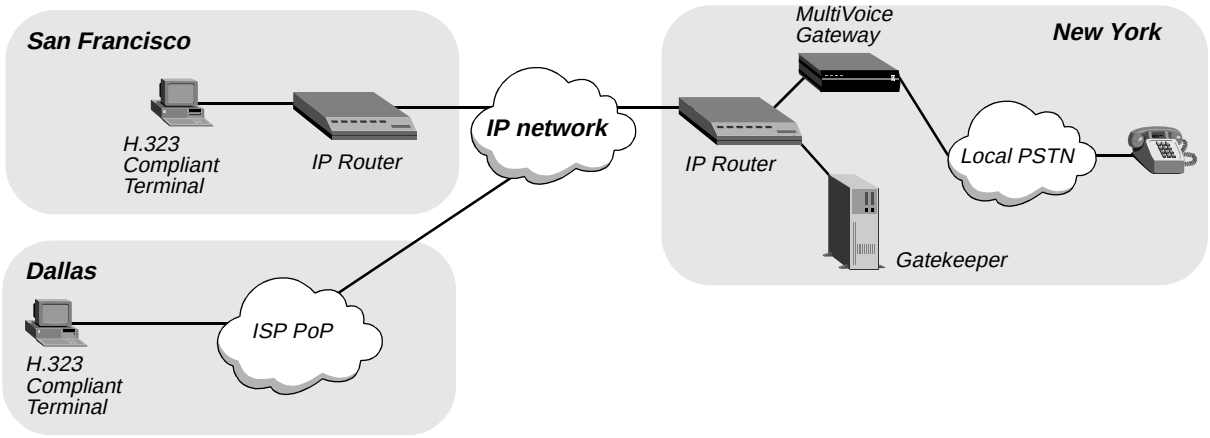
Callers in Tokyo dial *9* before the San Francisco phone number to use the traditional PSTN. They dial *8* to use the MultiVoice network.

This architecture can also support PBX intraflow. The PBX can be configured to routes calls to the alternative path when all trunks between PBXs are in use. PBX intraflow reduces the number of inter-PBX trunks the company needs, while ensuring that users can make calls even during busy periods.

PC-to-Phone calls

Figure 1-10 shows how to PC-to-Phone calls could be connected using either a *virtual private network* (VPN) or an ISP's PoP.

Figure 1-10. Virtual private network using PC telephony



The callers in San Francisco use their PCs to place calls to phone numbers in New York from inside the VPN, utilizing the backbone IP network as the link to the destination MultiVoice Gateway.

The callers in Dallas use their PCs to place calls to phone numbers in New York through a local PoP provided by an ISP, utilizing the Internet connection as the link to the destination MultiVoice Gateway.

Calls initiated from PCs connected to a network are processed as if the PC was one of the MultiVoice Gateways. This requires that the PC be a fully *H.323 compliant terminal*. It must be able to register and communicate with the Gatekeeper as if it were a MultiVoice Gateway. It must also be able to communicate with the MultiVoice Gateway at the other end of the call.

H.323 compliant terminals

An H.323 compliant terminal is described in detail in the International Telecommunications Union (ITU) Telephone Recommendation H.323. To work with Ascend's MultiVoice for the MAX, a PC must use a telephony application which supports:

- Registration, Admission and Status (RAS) messaging with a Gatekeeper
- The G.711 audio coder/decoder (required)
- The G.729(a) and G.723.1 audio coder/decoders (optional).

⚠ **Caution:** Not all third-party telephony software has full RAS messaging capability, or works with a Gatekeeper. PictureTel's LiveLAN, version 3.00, was successfully tested and proven compatible with MultiVoice networks. Calls made from PCs using other applications may fail.

Getting Acquainted with the MultiVoice Gateway

2

What is the MultiVoice Gateway?

The MultiVoice Gateway is a Wide Area Network (WAN) access router designed as the interface between the Public Switched Telephone System (PSTN) and an Internet Protocol (IP) packet network. It supports the following features:

- Digital access for most varieties of T1 or E1 WAN services
- Voice codecs that increase packet traffic performance by providing voice compression
- DTMF tone detection, generation and pass-through
- E1/R2 signal processing
- Type of Service (ToS) configuration
- ITU-T H.323 protocol stack
- Fully supported communication with Ascend's MultiVoice Access Manager

What items are included in your package?

The MultiVoice Gateway package contents vary, depending on which base unit and expansion cards you order. This section helps you confirm the items in your package.

Checking the MultiVoice Gateway base unit

Open the shipping package and verify you have received the base MultiVoice Gateway unit that you ordered. Currently, MultiVoice Gateways may be installed on the Ascend MAX 6000/4000/2000 platforms.

MAX 6000 Base Unit

Figure 2-1 shows a rear view of the AC MAX 6000 MultiVoice Gateway base unit. Figure 2-2 shows the AC Redundant MultiVoice Gateway base unit. And Figure 2-3 shows the DC MultiVoice Gateway base unit (with a DC power source).

Figure 2-1. MultiVoice Gateway base unit

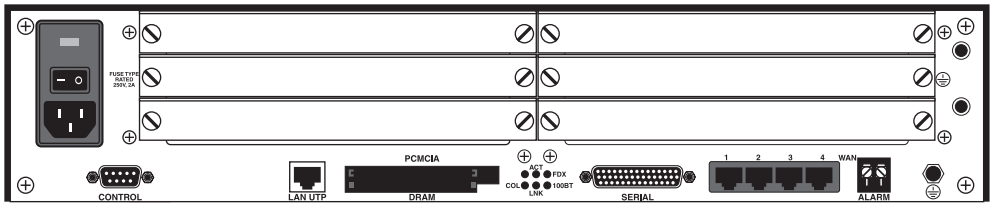


Figure 2-2. Redundant MultiVoice Gateway base unit

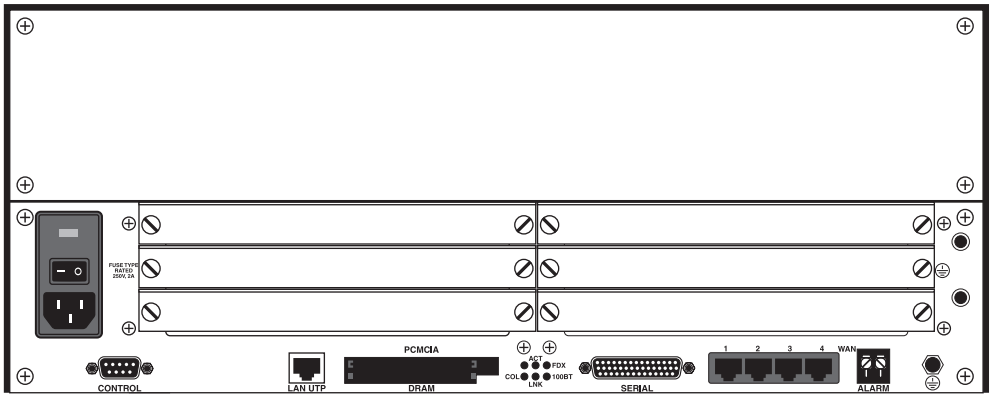
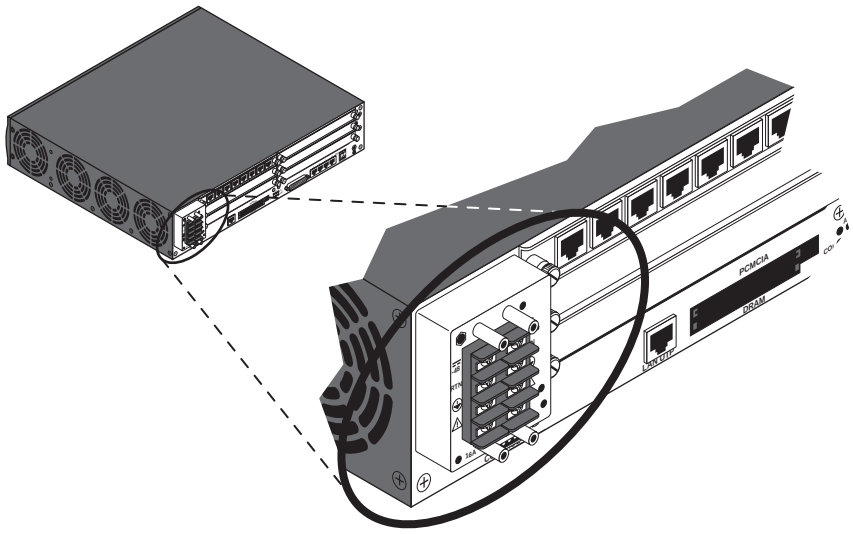


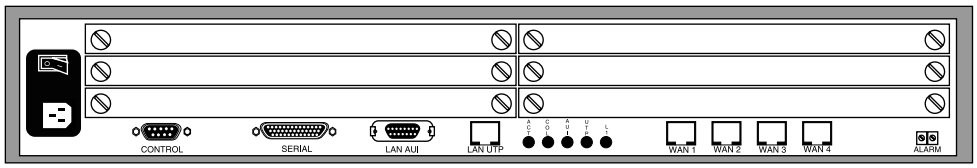
Figure 2-3. DC power source on the MultiVoice Gateway



MAX 4000 Base Unit

Figure 2-4 shows a rear view of the MAX 4004 MultiVoice Gateway base unit.

Figure 2-4. MAX 4004 base unit



MAX 2000 Base Unit

Figure 2-5 shows a rear view of the AC MAX 2000 MultiVoice Gateway base unit for T1/PRI. Figure 2-6 shows the AC MAX 2000 MultiVoice Gateway base unit for E1/PRI.

Figure 2-5. MAX 2000 T1/PRI base unit

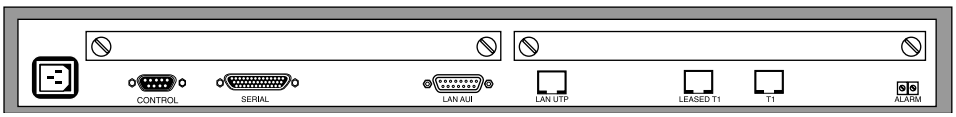
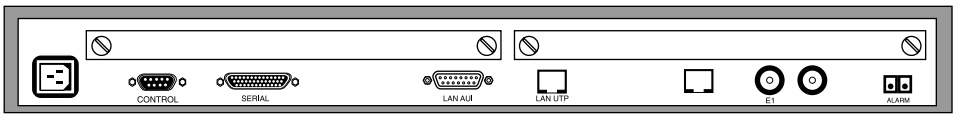


Figure 2-6. MAX 2000 E1/PRI base unit



Checking other package contents

After you verify which base unit you have, make sure that your package contains the following items:

- A console cable (null-modem)
- Two adapters
- A power cable
- A rack-mounting kit
- Separately packaged expansion modules, if you ordered them separately

If you are missing any items, contact your MultiVoice Gateway distributor.

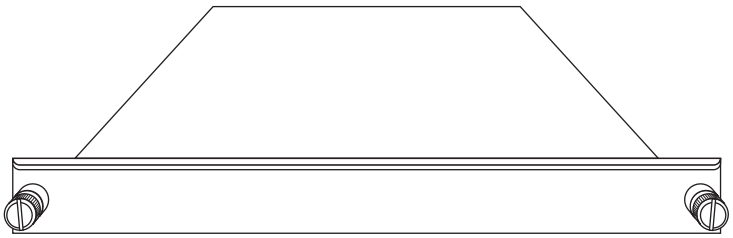
Checking the expansion cards

The MultiVoice Gateway accommodates up to six Digital Signal Processor (DSP) expansion cards (also referred to as DSP expansion modules or DSP slot cards), an ISDN BRI network interface card, and a DRAM card.

DSP card

Each DSP card (Figure 2-7) supports eight, twelve, or sixteen voice connections. These cards have no external ports. They are identified by the data label next to the right set screw, which contains the DSP card model number and serial number. You can install a maximum of six DSP cards in the MAX 6000/4000 base unit, and a maximum of two DSP cards in the MAX 2000 base unit

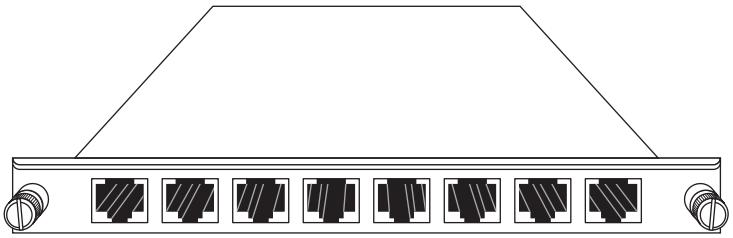
Figure 2-7. Series56 DSP card



ISDN BRI network interface card

The ISDN BRI network interface card (Figure 2-8) has eight ISDN BRI ports. You can install a single ISDN BRI network interface card in the MAX 6000/4000 MultiVoice Gateway.

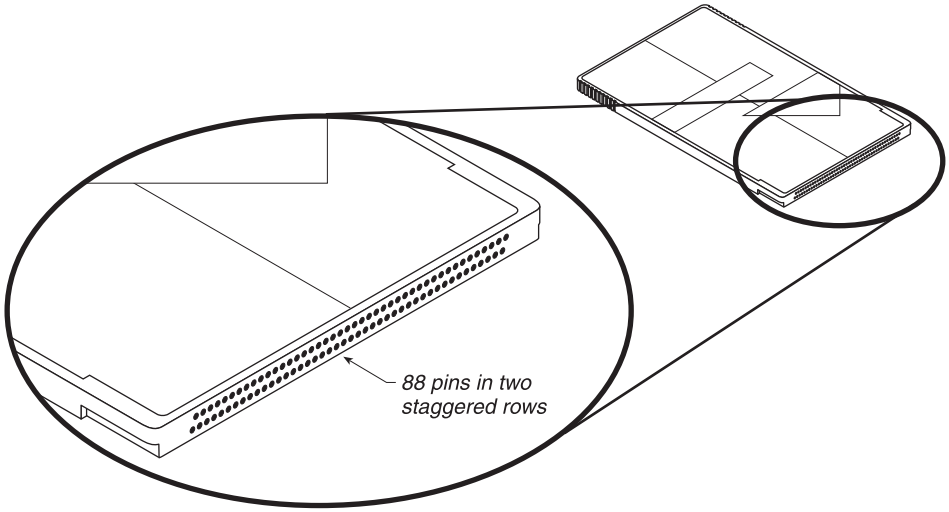
Figure 2-8. ISDN BRI network interface cards



DRAM card

The DRAM card is a proprietary Ascend card. It is *not* hot-swappable and should not be removed while the MultiVoice Gateway is running. The DRAM card attaches directly to the CPU bus of the MAX 6000 base unit. Damage might occur if you attempt to remove it.

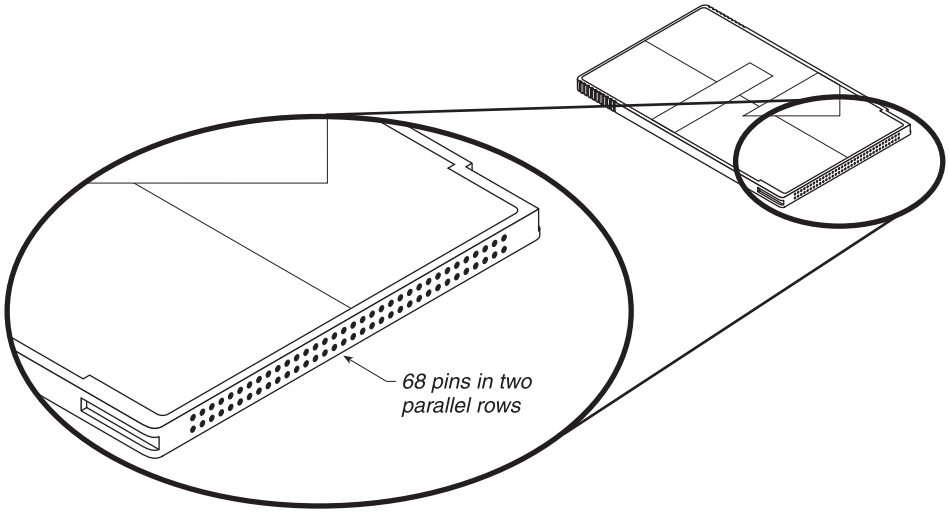
Figure 2-9. DRAM card



PCMCIA flash card

The PCMCIA flash card is a standard card that extends existing flash memory in a MAX 6000 base unit.

Figure 2-10. PCMCIA card



Interfaces on the base unit

Read this section to learn the names of the physical interfaces on the MultiVoice Gateway, and for descriptions of the interfaces. For illustrations, see "Checking the MultiVoice Gateway base unit" on page 2-1.

Common Interfaces

POWER

The power interface on the MultiVoice Gateway accepts AC or DC power, depending on the model you purchased. Figure 2-1 on page 2-2 and Figure 2-2 on page 2-2 show AC power sockets on a MAX 6000 base unit. Figure 2-3 on page 2-2 shows the DC power socket. (For further details, see Appendix C, "MultiVoice Gateway Technical Specifications.")

CONTROL

The Control port connects to a VT100 terminal or modem for access to the menu-driven user interface to the MultiVoice Gateway. The interface runs at 9600 bps (configurable through the user interface), 8 bits per character, no parity, no flow control, 1 stop bit. For details on cables that connect to this port, see Appendix D, "Cables and Connectors.")

LAN UTP

The LAN UTP port connects the MultiVoice Gateway to a UTP (unshielded twisted pair 10/100 BaseT) LAN. (For details on cables that connect to this port, see Appendix D, "Cables and Connectors.")

SERIAL V.35 DTE Port

The serial V.35 DTE port provides a point-to-point connection between the MultiVoice Gateway and another device. This set of manuals refers to it as Serial WAN port. (For details on cables that connect to the serial V.35 DTE port, see Appendix D, "Cables and Connectors.")

ALARM

The Alarm interface is a two-connector terminal block that provides indication of alarm conditions. (For further information about the alarm relay, see Appendix C, "MultiVoice Gateway Technical Specifications.")

Additional MAX 6000 Interfaces

This section describes the physical interfaces unique to the MAX 6000 base unit. For illustrations, see Figure 2-1 on page 2-2 and Figure 2-2 on page 2-2.

PCMCIA

The PCMCIA interface accepts a plug-in PCMCIA card. (For an illustration, see Figure 2-10 on page 2-5.)

DRAM

The DRAM interface accepts a plug-in DRAM card. (For an illustration, see Figure 2-9 on page 2-5.)

WAN (1 to 4)

The WAN ports are either a group of four T1 or four E1 ports providing point-to-point T1/E1 connections between the MultiVoice Gateway and other devices. These ports are called Net/T1 and Net/E1 ports in these manuals.(For details on cables that connect to the WAN ports, see Appendix D, “Cables and Connectors.”)

Additional MAX 4000 Interfaces

This section describes the physical interfaces unique to the MAX 4000 base unit. For illustrations, see Figure 2-4 on page 2-3.

LAN AUI

The LAN AUI (Attachment Unit Interface) port connects the MultiVoice Gateway to a Standard Ethernet (10Base-5) LAN. (For details of the cables that connect to this port, see Appendix D, “Cables and Connectors.”)

WAN (1 to 4)

The WAN ports are either a group of four T1 or four E1 ports providing point-to-point T1/E1 connections between the MultiVoice Gateway and other devices. These ports are called Net/T1 and Net/E1 ports in these manuals.(For details on cables that connect to the WAN ports, see Appendix D, “Cables and Connectors.”)

Additional MAX 2000 Interfaces

This section describes the physical interfaces unique to the MAX 2000 base unit. For illustrations, see Figure 2-5 on page 2-3 and Figure 2-6 on page 2-3.

LAN AUI

The LAN AUI (Attachment Unit Interface) port connects the MultiVoice Gateway to a Standard Ethernet (10Base-5) LAN. (For details of the cables that connect to this port, see Appendix D, “Cables and Connectors.”)

T1(E1)

This port is either a T1 or E1 port providing point-to-point connection between the MultiVoice Gateway and other devices. These ports are called Net/T1 and Net/E1 ports in these manuals.(For details on cables that connect to these ports, see Appendix D, “Cables and Connectors.”)

Setting Up the MultiVoice Gateway Hardware

3

Planning the hardware installation

Before you begin installation of the MultiVoice Gateway hardware, make sure that you have the items you need. Also review the guidelines for installing the MultiVoice Gateway and for reinstalling the MultiVoice Gateway.

For additional details on hardware installation, refer to the *Getting Started* guide for the MAX 2000, MAX 4000 or MAX 6000, as appropriate.

What you need before you start

Before you install the MultiVoice Gateway, make sure that you have the following items:

- A suitable location in which to install the MultiVoice Gateway hardware.
- A one-unit air gap for cooling (approximately 4 inches) between the MultiVoice Gateway and other rack-mount hardware if you are rack-mounting the MultiVoice Gateway hardware.
- One or more active line(s), with at least one line set for bidirectional calling. (Bidirectional calling allows you to test the MultiVoice Gateway hardware by having the MultiVoice Gateway dial out on one channel and answer on another channel.)
- If you have an Ethernet interface, you need the appropriate cables and connectors to set up and test your Ethernet LAN connection.
- A locally-connected host or workstation that can Ping or Telnet to the MultiVoice Gateway.

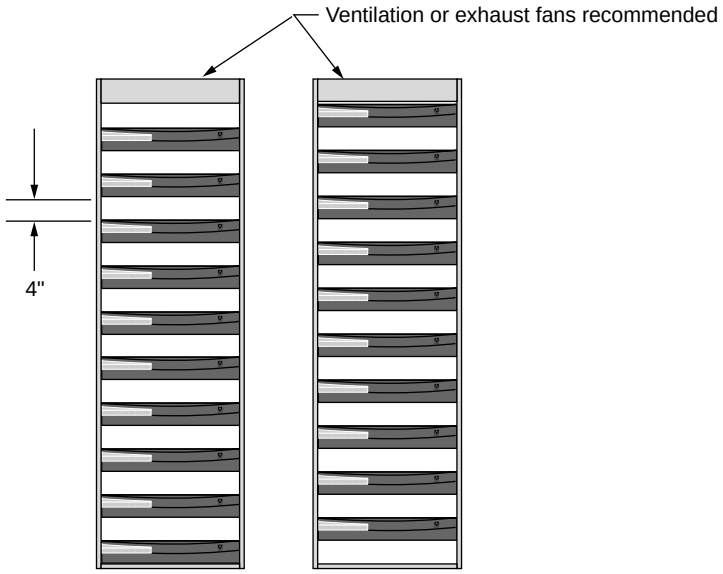
- A VT100 terminal or a workstation with an Ethernet interface and communications software that supports VT100 emulation.
- One or more active BRI lines, if applicable.

  Note: Currently, MultiVoice for the MAX does not support BRI lines on the MAX 2000.
- Any expansion modules that were shipped separately.

Guidelines for installing MultiVoice Gateway units in a rack

Figure 3-1 shows an example of MultiVoice Gateway units installed in a rack.

Figure 3-1. MultiVoice Gateway units installed in a rack



- Leave approximately four inches of vertical space between MultiVoice Gateway units. The space allows for air flow between units and leaves room for handling the units if they need to be removed.
- Leave approximately 1 foot between the racks of MultiVoice Gateway units for air flow dissipation.
- Stair step MultiVoice Gateway in adjacent open racks, as shown in Figure 3-1, so that hot air from one unit is not being blown into an adjacent unit. The intake fans are on the right (as viewed from the front). The exhaust fans are on the left.
- Ensure adequate cooling in the room.
- You should install racks with open sides because the MultiVoice Gateway fans vent on the side of the unit. If you use enclosed racks:
  - Make sure that there are openings to the air conditioning system in the floor beneath each cabinet.
  - Exhaust fans at the top of the cabinet can provide substantial cooling. At a minimum, however, the cabinets should be ventilated at the top.

If you ordered MultiVoice Gateway expansion cards separately, as with the MAX 4000 and MAX 2000, continue with the next section. If all of your expansion cards are pre-installed, skip to "Setting up the hardware" on page 3-4.

Inserting an expansion card

Caution: When installing any equipment, be sure to follow proper procedures (such as using a grounding mat and a wrist strap) to prevent buildup of static electricity.

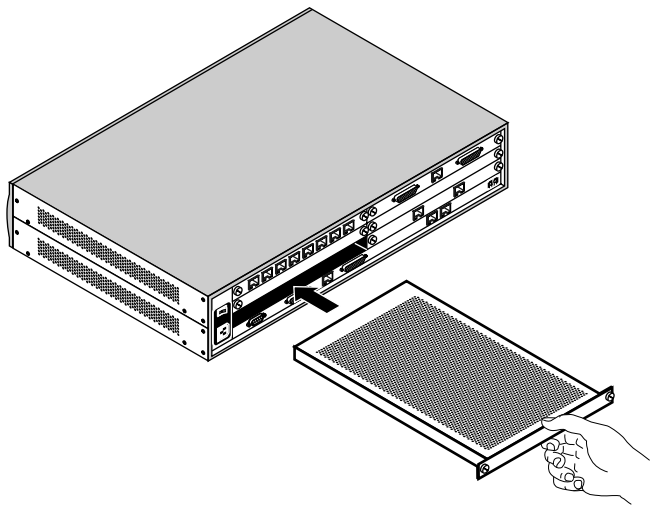
If your MultiVoice Gateway package includes expansion modules that are not already installed in your MultiVoice Gateway, insert the modules now. Perform the following steps:

1 Make sure that the MultiVoice Gateway power is off and the power cord is unplugged.

Warning: Failure to turn off the MultiVoice Gateway power and unplug the power cord could result in injury to you.

2 Hold the expansion card with the network ports facing you, and insert the card into a back panel slot as shown in Figure 3-2. Do not grab the slot cards from both ends. Be sure to insert the card into guides that are in the same plane.

Figure 3-2. Inserting an expansion card into a MultiVoice Gateway slot

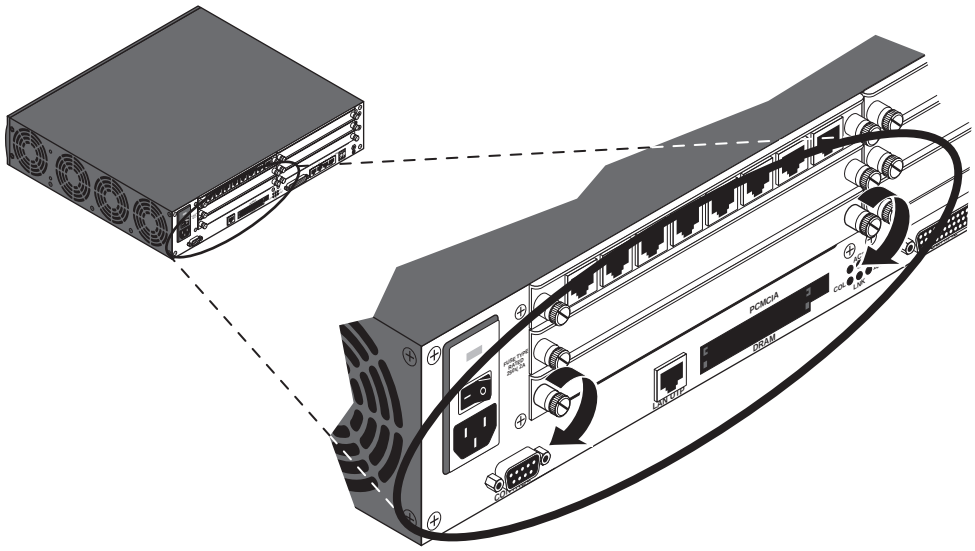


3 Push the card along the internal guides until it is secure. The face plate of the expansion card should touch the back panel of the MultiVoice Gateway.

Caution: Do not force the expansion card into the slot. Doing so can damage the card or slot connector.

4 Tighten the screws on either side of the module as shown in the Figure 3-3.

Figure 3-3. Tightening slot card thumbscrews



Now you are ready to set up the hardware.

Setting up the hardware

Before you set up the MultiVoice Gateway hardware, you need to make sure that you have the appropriate space. You can install the MultiVoice Gateway in a 19-inch or 23-inch rack.

The following illustrations show the dimensions of both base (MAX 6000/4000) MultiVoice Gateway units: the single power supply unit and the redundant power supply unit.

Figure 3-4. Dimensions of the MAX 6000 single power supply unit

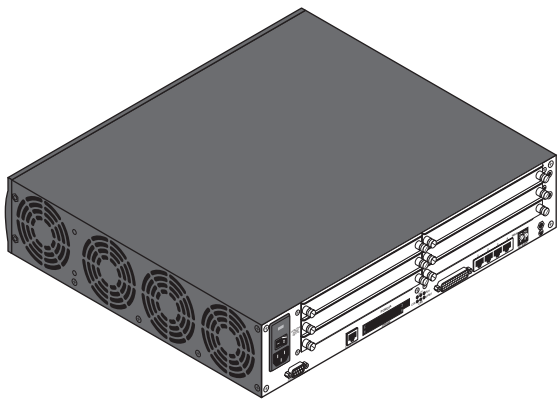
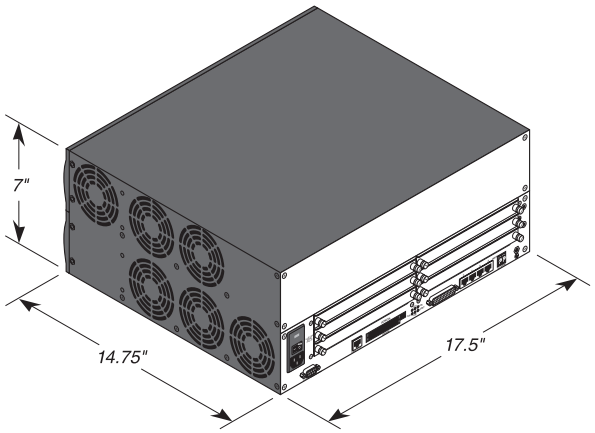


Figure 3-5. Dimensions of the redundant power supply unit

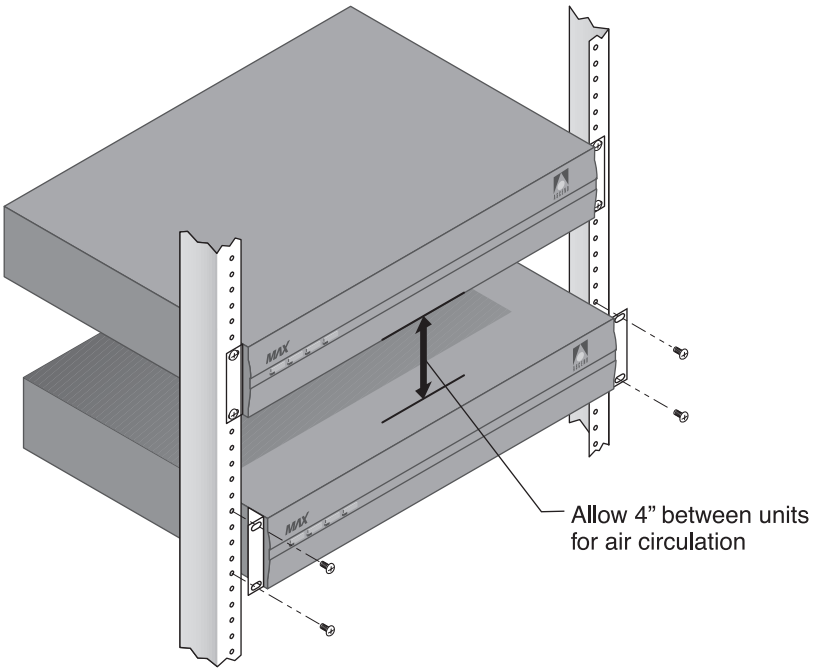


To set up the MultiVoice Gateway hardware, proceed as follows:

1 If you are installing the MultiVoice Gateway in a rack, insert the unit in the rack and secure it as shown in Figure 3-6.

2 If you are not rack-mounting the MultiVoice Gateway, place it where you can have full access to the front and back panels.

Figure 3-6. Mounting the MultiVoice Gateway in a rack



3 Connect a VT100 terminal or a workstation with VT100 terminal-emulation software to the MultiVoice Gateway Control port. Use the null-modem cable provided in your package.

Connecting to input power

Plug the power cord into your AC or DC power source. (Figure 3-4 and Figure 3-5 display the power sources, and Appendix C, “MultiVoice Gateway Technical Specifications,” lists input power requirements.)

Connecting to the LAN

To connect to the LAN:

1 Connect your Ethernet LAN cable to the Ethernet interface on the MultiVoice Gateway.

Note: The MultiVoice Gateway has a 10Base-T (LAN UTE) Ethernet port. For the MAX 6000 MultiVoice Gateway, you will need an adapter if you have another type of Ethernet LAN. On the MAX 4000 and MAX 2000, you may connect to a LAN using the Ethernet AUI port.

Connecting the MultiVoice Gateway to the T1 Line

1 Connect the MultiVoice Gateway either directly to the T1/PRI line or through other network interface equipment.

Note: To connect to the demarcation point, where the T1/PRI line’s metallic interface connects to other equipment, the MultiVoice Gateway T1/PRI ports must be equipped with internal CSUs. Otherwise, external CSUs or other network (WAN) interface equipment must be installed between the MultiVoice Gateway and the demarcation point.

2 Inform your T1/PRI service provider that your equipment is connected, so they can bring up the line.

Before you start up the MultiVoice Gateway, familiarize yourself with the LED indicator lights. (See “Interpreting the MultiVoice Gateway LEDs” on page 3-7.)

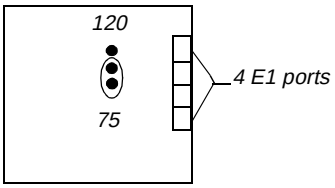
Connecting the MultiVoice Gateway to the E1 Line

The MultiVoice Gateway can connect to any DPNSS access point on a Private Branch Exchange (PBX) or directly to E1 digital services. Use a cable that is specifically constructed for transmission of E1/PRI signals (CCITT G700 series recommended). The MultiVoice Gateway can also connect to G.704 framed leased (non-switching) services for 75 Ohm lines. (Use cable 2510-0272-001 with 75 Ohm E1 lines.)

Grounding

The screen (shield) of the transmit and receive coaxial cable must be earthed at one end of the line only. Links (jumpers) inside the MultiVoice Gateway chassis earth the coaxial screens. The default position of the grounding links on the network line interface, when used with coaxial cable adapter, is on the transmit side (Tx) for 1680 Kbps network operations.

Figure 3-7. One set of links for each E1 port



For a daisy chain connection of the MultiVoice Gateway E1/PRI unit, only line 1 needs an earth link (jumper), as line 1 is the only port connected to the telecommunications network.

Connect your MultiVoice Gateway to the E1 PRI network interface (TA) equipment supplied by your PTT.

Cable length and characteristics

The maximum distance between the E1/PRI WAN interface equipment and the MultiVoice Gateway should not introduce attenuation of more than 6dB, when measured at half the maximum data rate (1024 Kbps). Also, the cable must have a root F characteristic.

Interpreting the MultiVoice Gateway LEDs

Before you start up the MultiVoice Gateway, you need to understand the LEDs on the front and back panels of the MultiVoice Gateway.

MultiVoice Gateway front panel

MAX 6000/4000

Figure 3-8 shows the location of LEDs on the MultiVoice Gateway front panel, for the MAX 6000 and MAX 4000, and Figure 3-9 shows the location of the LEDs on the Redundant MultiVoice Gateway front panel.

Figure 3-8. Location of the MultiVoice Gateway LEDs

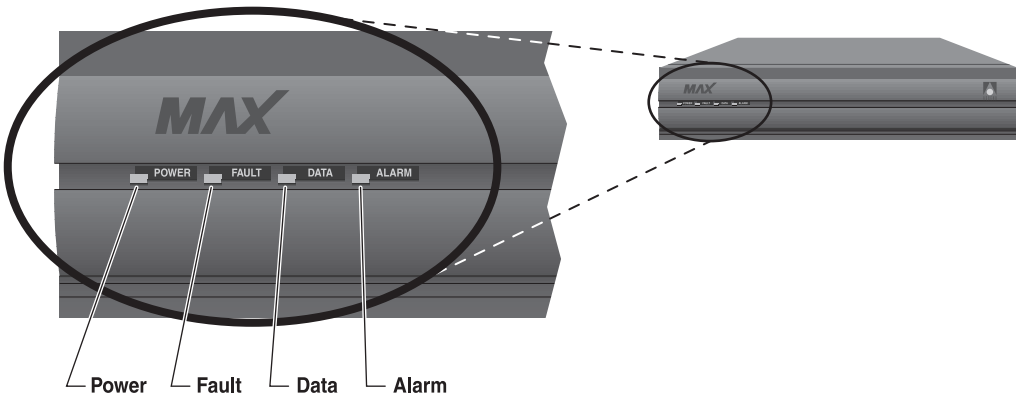


Table 3-1 lists the LEDs on the front panel of the MultiVoice Gateway and describes the function that each performs.

Table 3-1. MultiVoice Gateway front-panel LEDs

LED	Description
Power	On when the MultiVoice Gateway power is on.
Fault	On in one of two cases: Either a hardware self-test is in progress or there is a hardware failure. At system start-up, when the MultiVoice Gateway performs its Power On Self Test (POST), the LED is on. If any type of hardware failure occurs, the LED flashes. If the failure is isolated to an expansion card, the MultiVoice Gateway might continue to function without the expansion card.
Data	On when calls are active.
Alarm	On when there is a WAN alarm or a trunk is out of service (for example, during line loopback diagnostics). WAN alarms include Loss of Sync, Red Alarm, Yellow Alarm, and All Ones (or AIS).

Figure 3-9. Location of the LEDs on the Redundant MultiVoice Gateway

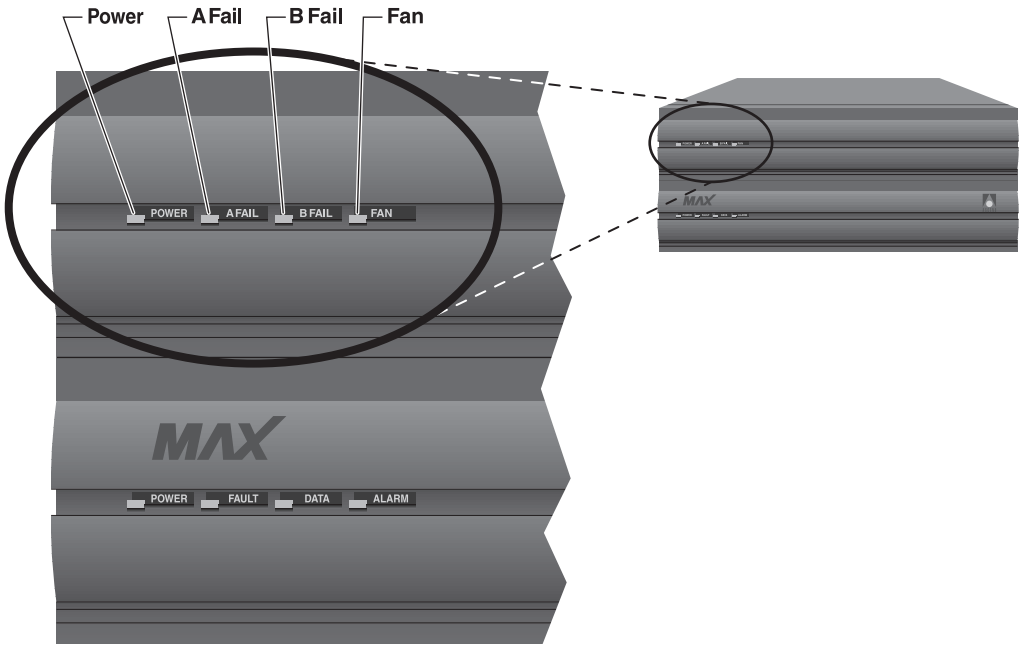


Table 3-2 lists and describes each LED on the front panel of the Redundant MultiVoice Gateway.

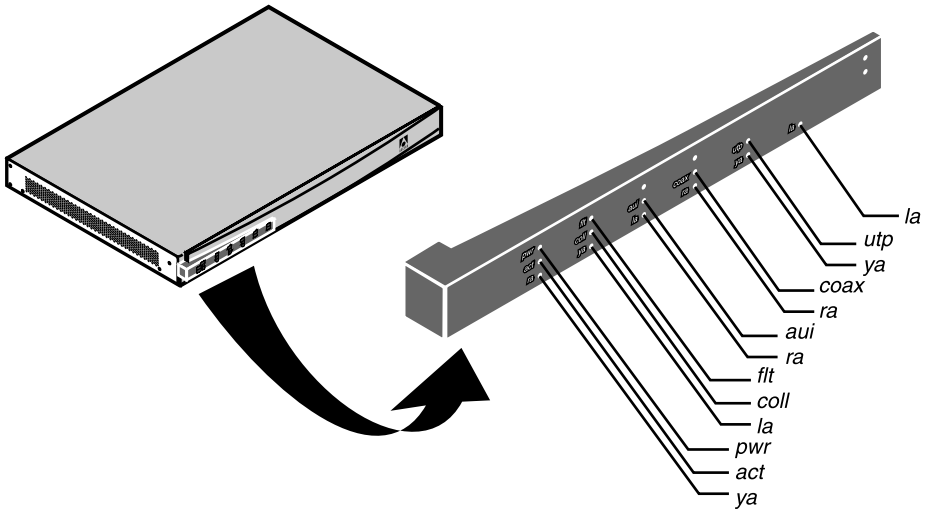
Table 3-2. Redundant MultiVoice Gateway LEDs

LED	Description
Power	On when the Redundant MultiVoice Gateway power supply is on.
A Fail	On only if there is a failure on power supply A. That is, if one or more of the voltages on the A side (+5, +3.3, +12, -12, -5) has failed.
B Fail	On only when there is a failure on power supply B, (if one or more of the voltages on the B side (+5, +3.3, +12, -12, -5) has failed.
Fan	On when the fans are functioning properly (if +12 VDC from either A or B is good.) If this LED is off, then a fan is not working.

MAX 2000

The following figure shows the location of LEDs on the MAX 2000 front panel.

Figure 3-10. Location of the MAX 2000 LEDs



Refer to the following table to understand each LED.

Table 3-3. MAX 2000 LEDs

LED	Description
pwr	This LED is on when the MAX power is on.
act	This LED is ON if there is activity on the Ethernet interface.

Table 3-3. MAX 2000 LEDs

LED	Description
ya (leftmost—for Line 1)	This LED is ON when the MAX is receiving a Yellow Alarm pattern, indicating that the other of the of the line cannot recognize signals transmitted from the MAX.
flt	This LED is ON in one of two cases—either a hardware self-test is in progress or there is a hardware failure. When a hardware self-test is in progress, the LED is ON. If any type of hardware failure occurs, the LED flashes. If the failure is isolated to an expansion card, the MAX may continue functioning without the expansion card.
coll	This LED is ON if there are collisions on the Ethernet.
la (leftmost—for Line 1)	This LED is ON when the link is active and there are no pending alarms or tests. If a PRI is active and using D-channel signaling, this LED blinks when the unit is unable to establish layer 2 and 3 protocol communications with the central office switch. This may indicate a configuration error.
aui	This LED is ON to reflect the AUI interface.
ra (leftmost—for Line 1)	This LED is ON when the MAX is receiving a Red Alarm pattern, indicating an improper receive signal or no receive signal. This condition can occur as a result of a high error rate or improper line configuration. When such a condition arises, this red LED is ON and a Yellow Alarm is transmitted toward the WAN.
coax	This LED is ON if the 10Base-2 interface is chosen.
utp	This LED is ON if the 10BaseT interface is chosen.
ra, ya, and la (righmost—for Line 2)	These LEDs have the same meanings as their leftmost counterparts, except they apply only to Line 2.

MultiVoice Gateway back panel

MAX 6000

The following Figures show the MultiVoice Gateway back-panel LEDs for the MAX 6000, which display the status of the Ethernet interface.

Figure 3-11. Ethernet interface LEDs on MultiVoice Gateway back panel

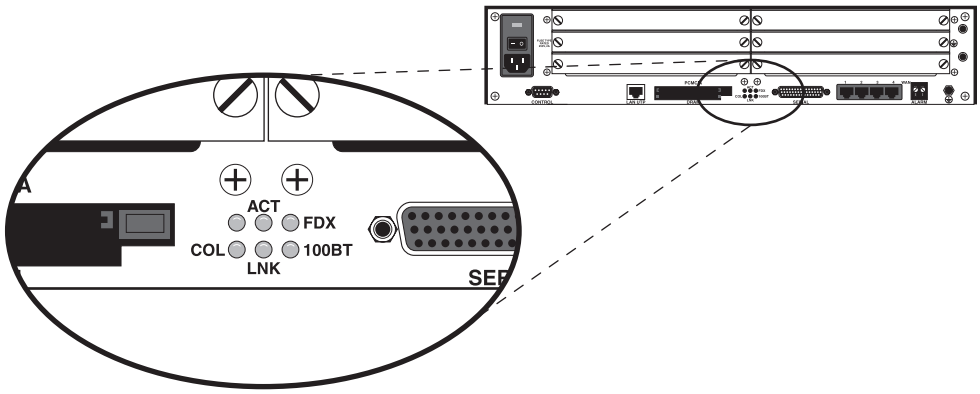


Table 3-4 describes the Ethernet interface LEDs.

Table 3-4. Ethernet interface LEDs on back panel

LED	Description
ACT (Activity)	On when the MultiVoice Gateway is detecting activity (network traffic) on its Ethernet interface.
COL (Collisions)	On when the MultiVoice Gateway detects packet collisions on the Ethernet.
FDX	On indicates full duplex on the Ethernet.
100ST	On, indicates 100BT. Off indicates 10BT.
LINK (Link integrity)	On when the Ethernet interface is functional.

MAX 4000

The following Figures show the MultiVoice Gateway back-panel LEDs for the MAX 4000, which display the status of the Ethernet interface.

Figure 3-12. Ethernet interface LEDs on the MAX 4000 MultiVoice Gateway back panel

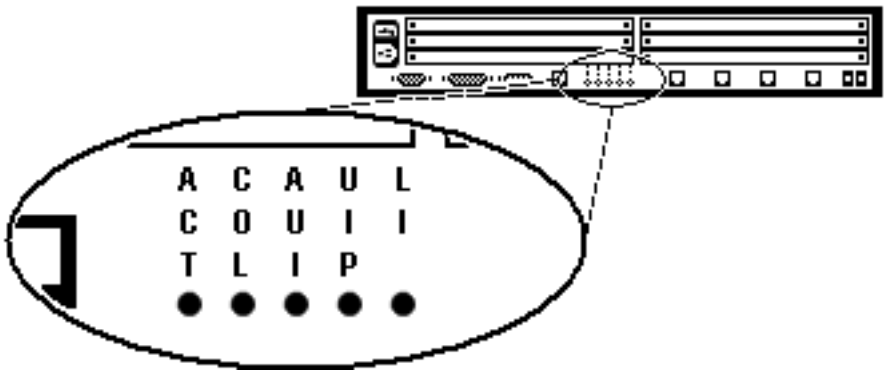


Table 3-5 describes the Ethernet interface LEDs for the MAX 4000.

Table 3-5. Ethernet interface LEDs on back panel

LED	Description
ACT (Activity)	On when the MultiVoice Gateway is detecting activity (network traffic) on its Ethernet interface.
COL (Collisions)	On when the MultiVoice Gateway detects packet collisions on the Ethernet.
AUI	On, indicates Ethernet interface on AUI port.
UIP	On, indicates Ethernet interface on LAN UTP port.
LI (Link integrity)	On when the Ethernet interface is functional.

Now that you know about the MAX LEDs, you are ready to start up the MAX.

Starting up the MultiVoice Gateway

To start up the MultiVoice Gateway, perform the following steps:

1 If you are using a PC, configure the terminal-emulation function in your communications software as follows:

- 9600 bps
- 8 data bits
- No parity
- 1 stop bit
- Direct connect

2 Make sure that you can see the LEDs on the front panel of the MultiVoice Gateway while you view the VT100 display.

3 Connect one end of the AC power cord to a power source and the other end to the MultiVoice Gateway.

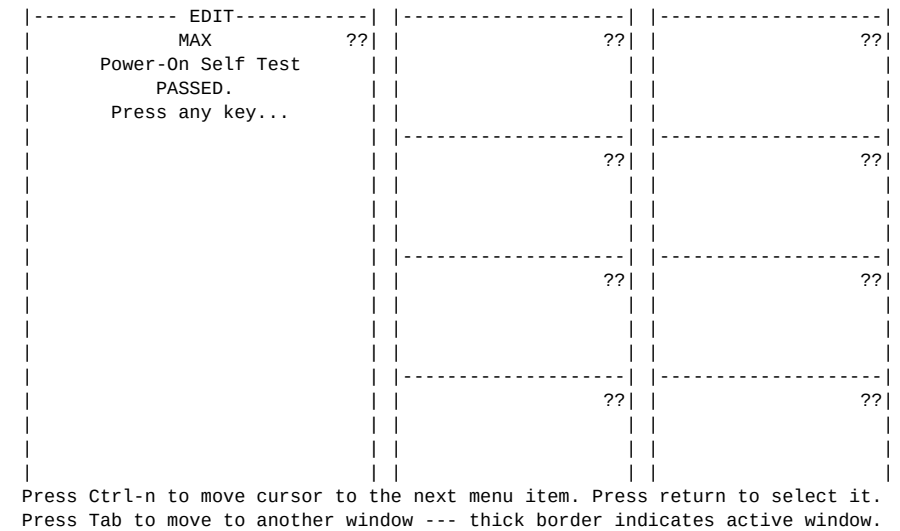
The power-on self-test (POST) begins and finishes within one minute.

4 While the POST is running, watch the LEDs.

If the Power LED is on and the Fault LED is off, the MultiVoice Gateway is operating properly. You can continue with the next step.

If either the Power LED is off or the Fault LED is on, remove the power cord and do not continue. Contact your Ascend distributor

5 Watch the VT100 display during the POST. When the POST is successful, the following screen appears:



6 Press any key. The following reminder screen appears, instructing you to edit your line configuration before you dial:

```
Edit Line Config
before dialing
Press any key...
```

Press any key again to display the MultiVoice Gateway Main Edit menu as shown.

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

For the MAX 2000, the following items are available from the MultiVoice Gateway `Main Edit menu:`

```
Main Edit Menu
>00-000 System
10-000 Net/T1
20-000 VOIP-16
30-000 VOIP-16
40-000 Serial Port T1-CSU
50-000 Ethernet
```

The next chapter explains how to use the VT100 interface and configure the MultiVoice Gateway.

Navigating the User Interface

4

Connections to the user interface

To configure the MultiVoice Gateway, you can access the user interface either through the unit's its control port or through a Telnet session.

Connecting via the MultiVoice Gateway Control port

You can connect a VT100 terminal or a workstation with VT100-emulation software to the control port of the MultiVoice Gateway. Use a serial cable. If using a workstation, set the terminal-emulation software as follows:

9600 bps
8 data bits
No parity
1 stop bit
No flow control
Direct connect

After the connection is established, the Control Monitor screen appears.

Connecting through TELNET

You can establish a Console session from any Telnet workstation by opening a Telnet session with the MultiVoice Gateway. In a Telnet session you can perform all of the configuration, diagnostic, management, and other functions that could be performed through the MultiVoice Gateway Control port.

To Telnet to the MultiVoice Gateway, you must know the:

- IP address of the MultiVoice Gateway.
- Telnet password, if configured.
- Password of a Security profile with Operations=Yes. (For complete information about Security profiles, see "The Main Edit menu" on page 4-2.)

The Main Edit menu

The configuration interface consists of the Main Edit menu and eight status windows. The left part of the screen is the Main Edit menu, which you use to configure the MultiVoice Gateway. The items listed in the Main Edit menu differ, depending on the system configuration. The Empty items represent expansion slots that do not contain a card.

Figure 4-1. MultiVoice Gateway Main Edit menu and Status windows for the MAX 6000 and MAX 4000

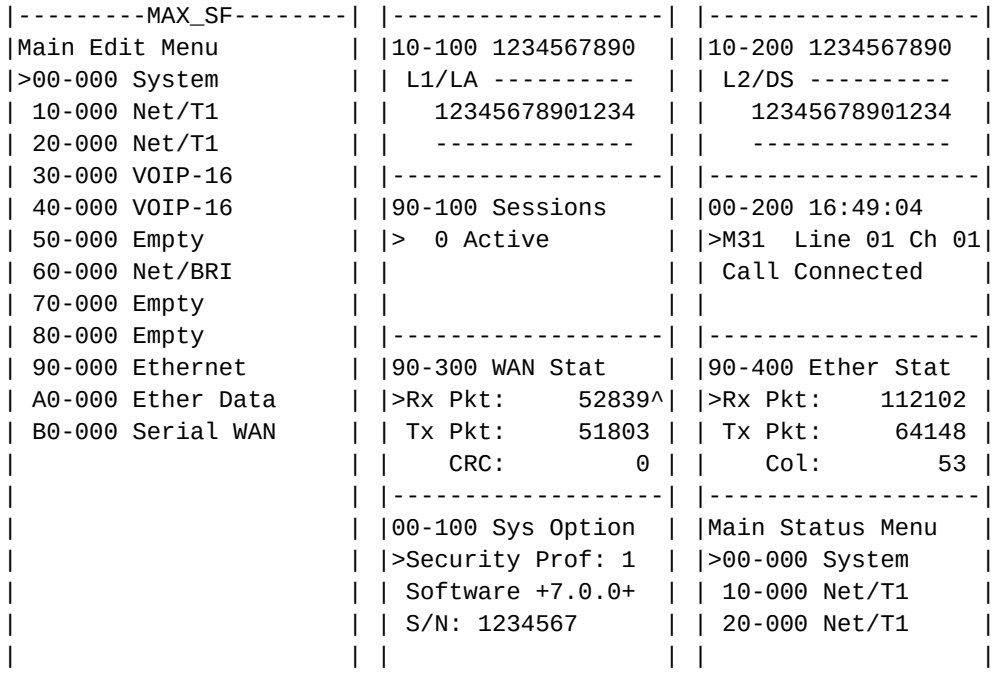


Figure 4-2. MultiVoice Gateway Main Edit menu and Status windows for the MAX 2000

```
|---MAX2000-110 EDIT-------| |----------------------| |----------------------|
|Main Edit Menu            | |10-100 1234567890     | |50-300 WAN Stat       |
|>00-000 System            | |  L1/RA ----------    | |  Rx Pkt:           0 |
| 10-000 Net/T1            | |    12345678901234    | |  Tx Pkt:           0 |
| 20-000 VOIP-16           | |                      | |     CRC:           0 |
| 30-000 VOIP-16           | |----------------------| |----------------------|
| 40-000 Serial Port T1-CSU| |50-100 Sessions       | |00-200 04:15:26       |
| 50-000 Ethernet          | |>  0 Active           | | >M31  Line 00 Ch 00  |
|                          | |                      | |  No Trunk Available  |
|                          | |                      | |                      |
|                          | |----------------------| |----------------------|
|                          | |50-500 DYN Stat       | |50-400 Ether Stat     |
|                          | |  Qual N/A  00:00:00  | | >Rx Pkt:     391668  |
|                          | |  0K     0 channels   | |  Tx Pkt:      42239  |
|                          | |  CLU  0%  ALU   0%   | |     Col:           0 |
|                          | |----------------------| |----------------------|
|                          | |00-100 Sys Option     | |Main Status Menu      |
|                          | | >Security Prof: 1    | | >00-000 System       |
|                          | |  Software +7.0.0+    | |  10-000 Net/T1       |
|                          | |  S/N: 7181672        | |  20-000 VOIP-16      |
|                          | |                      | |                      |
```

For an overview of how the MultiVoice Gateway menus and profiles are organized, see the MultiVoice Gateway *Reference Guide*.

Understanding menu numbering

The MultiVoice Gateway has four built-in T1 or E1 lines and a V.35 serial port for WAN access. It also has eight expansion slots, which supports multiple DSP slot cards and an 8-port BRI slot card, if desired.

Figure 4-3. Slot and port numbering in the MAX 6000/4000 MultiVoice Gateway

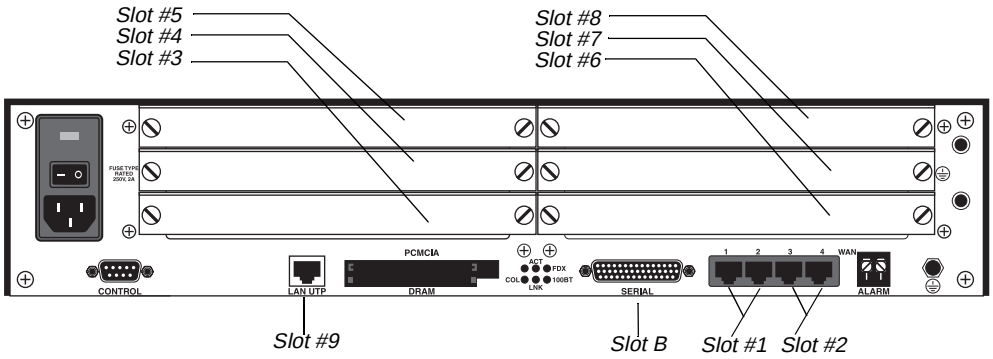
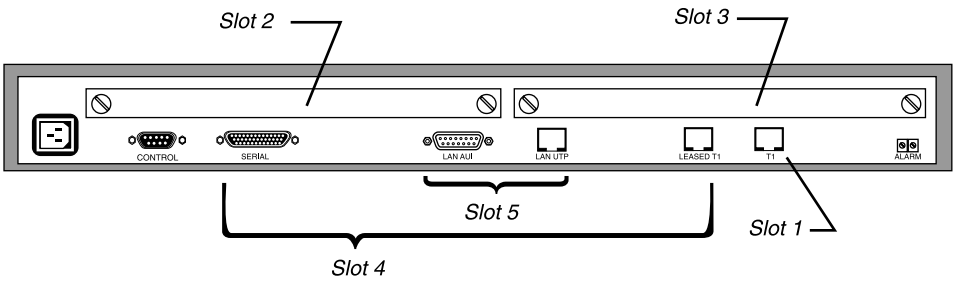


Figure 4-4. Slot and port numbering in the MAX 2000 MultiVoice Gateway



The numbers in the VT100 menus relate to slot numbers in the MultiVoice Gateway unit, which may be an actual expansion slot or a *virtual* slot on the MultiVoice Gateway unit's motherboard.

Common menu items

The system itself is assigned slot number 0 (menu 00-000) on the MAX 2000/4000/6000. The System menu contains the following profiles and submenus, which are all related to system-wide configuration and maintenance:

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

MAX 4000/6000 menu items

On the MAX 4000/6000 platforms, the menu numbers are associated with the following actual expansion slots or virtual slots:

- The built-in T1 or E1 lines are slot 1 and slot 2 (menu 10-000 and 20-000). Each T1 or E1 slot contains two lines. The menus for configuring and testing the lines are organized as follows:

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

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

- The six expansion slots are slots 3 through 8 (menus 30-000 through 80-000), with the numbering shown in Figure 4-3.
- The Ethernet is slot 9 (menu 90-000). The Ethernet menu contains submenus and profiles related to the local network, routing and bridging, and WAN connections.
- EtherData is slot A (menu A0-000). There is no menu for the EtherData slot.
- The serial WAN port is slot B (menu B0-000).

For example, the following Main Edit menu is for a MAX 6000 with two Net/T1 expansion modules, in slots 2 and 3, and a Net/BRI expansion module installed in slot 3. Expansion slots 4 through 8 are empty.

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

MAX 2000 menu items

On the MAX 2000 platform, the menu numbers are associated with the following actual expansion slots or virtual slots:

- The built-in T1 or E1 line is slot 1 and slot 2 (menu 10-000 and 20-000). Each T1 or E1 slot contains two lines. The menus for configuring and testing the lines are organized as follows:

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

- The two expansion slots are slots 2 and 3 (menus 20-000 through 30-000), with the numbering shown in Figure 4-4.
- The leased T1 port is slot 4 (menu 40-000). This menu contains parameters related to network nailed T1 trunks used for managed networks (e.g.,. frame relay connections).
- The Ethernet is slot 5 (menu 50-000). The Ethernet menu contains submenus and profiles related to the local network, routing and bridging, and WAN connections.

For example, the following Main Edit menu is for a MAX 2000 with a Net/T1 expansion module installed in slot 1 and a MXV-SL-DSP16 expansion module installed in slot 2. Expansion slot 3 is empty.

```
Main Edit Menu
   00-000 System
   10-000 Net/T1
   20-000 VOIP-16
   30-000 Empty
   40-000 Serial Port Ti-CSU
   50-000 Ethernet
```

Activating a menu or status window

Only the Edit window or one of the status windows can be active at one time. The active display has a thick, double line border on the left, right, and top sides. In Figure 4-1, the 10-100 status display is active (near the top-middle of the screen).

If you press the Tab key, the thick double lines move to 00-200, the next screen to the right. If you continue pressing the Tab key, you successively activate each window from left to right and down, until you reach the last display in the lower right-hand corner. Back-Tab or Ctrl-O moves you in the opposite direction.

Opening menus and profiles

The Main Edit menu contains a list of menus, each of which can contain profiles and submenus. In the menu that is currently open, the cursor character (>) points to one item in the menu. To move the cursor down, press Ctrl-N (next) or the Down-Arrow key. To move it up, press Ctrl-P (previous) or the Up-Arrow key. (Some VT100 emulators do not support the use of arrow keys.) For a complete list of key combinations used to navigate the interface, see Table 4-1 on page 4-8.) In the following example, for a MAX 6000, the cursor is at the second menu item:

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

To open a menu, move the cursor to the menu's name and press Enter. For example, on a MAX 6000, you press Ctrl-N until the cursor points to `90-000 Ethernet`, then press Enter. The Ethernet menu opens:

```
90-000 Ethernet
  >90-100 Connections
   90-200 Names / Passwords
   90-300 Bridge Adrs
   90-400 Static Rtes
   90-500 Filters
   90-600 Firewalls
   90-700 Frame Relay
   90-800 Answer
   90-900 SNMP Traps
   90-A00 IPX Routes
   90-B00 IPX SAP Filters
   90-C00 Mod Config
```

The Ethernet menu contains submenus and profiles related to network functions, such as bridging, routing, WAN connections, and so forth. The `Mod Config` Profile in this menu relates to the configuration of the Ethernet interface itself, as shown next:

```
90-B00 Mod Config
   Module Name=
   Ether options...
   WAN options...
   SNMP options...
   OSPF options...
   OSPF global options...
   Route Pref...
   TServ options...
   Bridging=No
   IPX Routing=No
   AppleTalk=No
   Shared Prof=No
   Telnet PW=
   RIP Policy=Poison Rvrs
   RIP Summary=Yes
   ICMP Redirects=Accept
   BOOTP Relay...
   DNS...
```

Note: With the exception of parameters designated N/A (not applicable), you can edit all parameters in any profile. A profile is a group of parameters listed under a particular menu entry. N/A means that a parameter does not apply within the context of how some other parameter(s) or profile has been set.

Opening edit fields

To open an edit field for a text-based parameter (such as a Telnet PW, for example), move the cursor to that parameter and press Enter. An edit field opens, delimited by brackets:

```
90-B00 Mod Config
   Module Name=
   Ether options...
   WAN options...
   SNMP options...
   OSPF options...
   OSPF global options...
   Route Pref...
   TServ options...
   Bridging=No
   Shared Prof=No
   Telnet PW:
   [ ]

   ICMP Redirects=Accept
   BOOTP Relay...
   DNS...
```

(For related information, see “Special display characters and keys” on page 4-8.)

A blinking text cursor appears in the brackets, indicating that you can start typing text. If the field already contains text, it is cleared when you type a character. To modify only a few characters of existing text, use the arrow keys to position the cursor, then delete or overwrite the characters.

To close the edit field and accept the new text, press Enter.

Setting enumerated parameters

An enumerated parameter is one that has a set of predefined values.You modify it by simply placing the cursor beside the parameter and pressing the Enter, Return, or Right-Arrow key until the proper value appears.

Saving your changes

When you exit a profile, you are prompted to confirm that you want to save changes:

```
EXIT?
>0=ESC (Don't exit)
 1=Exit and discard
 2=Exit and accept
```

You can save the profile values by choosing the Exit and Accept option and pressing Enter, or by pressing 2.

Special display characters and keys

The following characters have special meaning within the displays:

- The plus character (+) indicates that an input entry is too long to fit onto one line, and that the MultiVoice Gateway is truncating it for display purposes.
- An ellipsis (...) means that a submenu displays the details of a menu option.
  The MultiVoice Gateway displays the submenu when you select the menu option.

Table 4-1 lists the special-purpose keys and key combinations you can use in the Palmtop Controller and Control Monitor displays.

Table 4-1. Special keys for Palmtop Controller and Control Monitor displays

Palmtop Controller	Control Monitor	Operation
>	Right-Arrow, Return, Enter, Ctrl-Z, Ctrl-F	Enumerated parameter: Select the next value. String value: Move one character to the right or enter the current input. Menu: Open the current selection.

Table 4-1. Special keys for Palmtop Controller and Control Monitor displays (continued)

Palmtop Controller	Control Monitor	Operation
<	Left-Arrow, Ctrl-X, Ctrl-B	Enumerated parameter: Select the previous value. String value: Move left one character or exit the current input. Menu: Close the current selection.
v	Down-Arrow, Ctrl-N	Move down to the next selection.
^	Up-Arrow, Ctrl-U, Ctrl-P	Move up to the previous selection.
N/A	Ctrl-V	Move to the next page of the list.
N/A	Tab, Ctrl-I	Move to the next window.
	Back-Tab, Ctrl-O	Move to the previous window.
TOGGLE STAT	N/A	Toggle to a status menu from the edit menu and vice versa.
Shift->	Delete	Delete the character under the cursor.
Shift-<	Backspace	Delete the character to the left of the cursor.
Shift-^	none	Overwrite the character under the cursor with a space.
DO	Ctrl-D	Open the DO menu.
N/A	Ctrl-T	Return from or go to the Simplified Menus.
N/A	Ctrl-L	Refresh the VT100 screen.
N/A	Ctrl-C	Return from the MIF to the normal menus.
D	D	Dial the currently selected profile.

Note: You always use the Control and Shift keys in combination with other keys. This document represents key combinations as two characters separated by a hyphen, such as Shift-T, which types the capital letter T. On the Palmtop Controller, the main character associated with the key is large and white, and the Shift character associated with the key is small and yellow.

When you can successfully navigate the VT100 interface, you are ready to configure the MultiVoice Gateway.

Privileges and passwords

The MultiVoice Gateway has nine Security profiles. When shipped from the factory, none of the nine profiles have any restrictions defined. To see the list of Security Profiles, open the System menu in the Main Edit Menu, select Security, and press Enter. The following display appears:

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

The Default profile

Whenever the MultiVoice Gateway is powered on, it activates the first Security Profile in the list, which is always named Default and always has no password. For security reasons, you should reset the privileges in the Default profile to restrict what can be done by anyone accessing the MultiVoice Gateway configuration menus. Proceed as follows:

1 Open the System > Security > Default profile.

2 Set Operations to No.

Caution: If you reset or power-cycle the MultiVoice Gateway, it activates the new, restrictive Default profile. You will not be able to perform any configuration tasks until you activate the Full Access Profile.

Full Access and other administrative profiles

After you have restricted the access granted by the Default Security profile, you can gain full access by activating the Full Access profile. At the Main Edit menu, press Ctrl-D to display a context-sensitive menu (called a DO menu):

```
90-C00 Mod Config
DO...
  >0=Esc
  P=Password
  C=Close TELNET
  E=Termsrv
  D=Diagnostics
```

In the DO menu, press P (or select P=Password). The Edit window displays the list of Security profiles. Select Full Access and press Enter. The MultiVoice Gateway prompts for that profile's password:

```
00-300 Security
Enter Password:
 []
  Press > to accept
```

Enter `Ascend` (unless you have changed the default password.)

After you press Enter, a message states that the password was accepted and the MultiVoice Gateway is using the new security level. Or, if the password you entered is incorrect, you are prompted again to enter the password.

Note: For a Console session established through Telnet, the caller must first supply the Telnet password to establish a Telnet session. Then, the Default security level is set for that session. To configure the MultiVoice Gateway through Telnet, the caller must activate a Security profile that has Operations set to Yes.

Modifying the Full Access Profile

To ensure complete access when needed, you should leave the default settings in the FUll Access profile unchanged, except for the Password setting. TO prevent unauthorized access, you should change the default Password setting (`Ascend`) as soon as possible. Proceed as follows:

1 Open the System > Security > Full Access profile.

2 Set the Password parameter to a value only your system administrators know.

3 Exit and save your changes.

Other administrative profiles

To create customized profiles for individual administrators or groups of administrators, see Chapter 10, "MultiVoice Gateway System Administration."

Configuring the WAN Interfaces

5

Before you begin

Before configuring the MultiVoice Gateway for the MAX, make sure you have:

- Hardware installed as explained in the Chapter 3, “Setting Up the MultiVoice Gateway Hardware.”
- Familiarity with the VT100 user interface.
- One or more active T1 or E1 lines into the MultiVoice Gateway. To support the self-tests described in this chapter, the line(s) must provide switched data service on at least two channels. (For more information, see “Provisioning the Switch” on page B-1.)
- An active Ethernet LAN with appropriate cables and connectors.
- A local host or workstation that can Telnet or Ping to the MultiVoice Gateway.

Configuring T1 lines

Each built-in T1 line contains 24 channels, each of which can support one single-channel connection. Depending on the signalling mode used on the line, all 24 channels are available for user data, or 23 channels are available for data and the 24th is reserved for signalling. T1 line configuration parameters are in a Line Config profile, as shown in the following example for a MAX 4000/6000:

```
Net/T1
   Line Config
      Name=mytelco
      1st Line=Trunk
      2nd Line=Trunk
      Line N...
```

```
Sig Mode=Inband
NFAS ID num=N/A
Rob Ctl=Wink-Start
Switch Type=N/A
Framing Mode=D4
Encoding=AMI
FDL=N/A
Length=1-333
Buildout=N/A
Clock Source=Yes
Collect DNIS/ANI=No
Pbx Type=N/A
Delete Digits=N/A
Add Number=N/A
Call-by-Call=N/A
T1-PRI:PRI # Type=Unknown
T1-PRI:NumPlanID=ISDN
Ans #=N/A
Ans Service=N/A
Input Sample count=N/A
Send Disc=0
Overlap Receiving=N/A
PRI Prefix #=N/A
Trailing Digits=N/A
T302 Timer=N/A
Ch 1=Switched
Ch 1 #=12
Ch 1 Slot=3
Ch 1 Prt/Grp=1
Ch 1 TrnkGrp=5
```

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

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

You can set line 1 and line 2 to Trunk (indicating a standard T1 interface with signalling information) or Disabled.

Understanding the line interface parameters

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

T1 signalling mode

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

- Inband, robbed bit signalling—The MultiVoice Gateway uses the Rob Ctrl parameter for the Call Control mechanism.
- ISDN signalling—Designate the 24th channel of the T1 line as the D channel.

- ISDN NFAS (Non-Facility Associated signalling)—Enables two or more T1 lines to share a D channel. One of the lines must be configured as the primary D channel and one as the secondary (backup) D channel.

Assigning an interface ID to NFAS lines

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

Inband, robbed-bit call control mechanism

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

Carrier switch type

Switch Type specifies the network switch providing ISDN service on a T1 PRI line. The ISDN carrier supplies the information. For example, your carrier might support one of the following values:

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

T1 line framing and encoding

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

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

FDL for monitoring line quality

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

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

Cable length and the amount of attenuation required

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

The Buildout parameter specifies the amount of attenuation to apply to the T1 transceiver's internal CSU. The amount, if any, depends on the length of the cable between the MultiVoice Gateway and any repeater from which it might receive the signal. If the MultiVoice Gateway is too close to the Central Office (CO) or a repeater, you might need to specify some attenuation to reduce the strength of the signal. Valid values are 0 dB (decibels) through 22.5 dB. Check with your carrier to determine the correct value.

Clock source for synchronous transmission

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

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

Collecting DNIS and ANI

The Collect DNIS/ANI parameter enables the MultiVoice Gateway to collect the Automatic Number Identifier (ANI) and the Dialed Number Identification String (DNIS) signals. These signals are used to support ANI authentication of MultiVoice users and single-stage dialing, respectively. DNIS and ANI can be collected for three network signal types:

- DTMF tones in T1 inband.
- MF tones in E1 R2.
- D channel messages in T1/E1 PRI or BRI.

The collected DNIS is dialed by the MultiVoice Gateway

Note: To process DNIS and ANI signals, the telephone switch (or PBX) connected to the MultiVoice Gateway must support DNIS and ANI pass-through signalling. To test whether your switch supports DNIS and ANI pass-through signalling, use the `h323CallDisplay` command. (For information on performing this test see Appendix A, "Troubleshooting.")

Call-by-Call signalling values (MAX 4000/6000)

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

Understanding the channel configuration parameters

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

Use	Description
Switched (the default)	Supports switched connections. Can be robbed-bit or a B channel, depending on the line's signalling mode.
Nailed	A clear-channel 64k circuit.
D channel	The channel used for ISDN D-channel signalling. Assigned automatically to channel number 24 when ISDN signalling is in use.
NFAS-Prime	Primary D channel for two T1 lines that support NFAS signalling. Used as the D channel for both lines, unless it becomes unavailable.
NFAS-Second	Secondary D channel for two T1 lines that support NFAS signalling. Used as the secondary (backup) D channel.
Unused	Unavailable for use.

Examples of T1 configuration

This section provides examples of configuring T1 lines for ISDN PRI service, robbed-bit signalling, and NFAS signalling.

Configuring a line for ISDN PRI service

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

Example of configuring ISDN signalling

To configure ISDN signalling on Line 1 of the currently open T1 module:

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

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

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

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

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

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

4 Close the T1 profile.

Example of configuring Pre-T310 Timer

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

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

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

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

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

To configure the Pre-T310 timer:

1. Open the Net/T1 > Line Config > Line menu.
2. Set the Send Disc parameter to a value of from 0 to 60 seconds.

   The parameter must be set to a value less than the T310 timer value, so that it expires (and the MultiVoice Gateway sends its ISDN disconnect) before the T310 timer.
3. Open the Ethernet > Mod Config > Auth menu.
4. Set the Timeout Busy = Yes if you would like User Busy sent when the Send Disc timer expires. Set Timeout Busy = No if you would like Normal call clearing sent.

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

DNIS and ANI collection

DNIS/ANI are automatically collected when you set the signalling mode to ISDN. The Collect DNIS/ANI parameter will be set to N/A, and is ignored by the MAX when processing ISDN signalling.

Configuring a line for robbed-bit signalling

To configure a T1 line for robbed-bit signalling:

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

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

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

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

3 Specify the robbed-bit call control mechanism:

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

4 Close the T1 profile.

DNIS and ANI collection for T1 using robbed-bit signalling

To configure DNIS/ANI collection for a T1 using robbed-bit signalling:

1 Open `Net/T1 > Line Config` profile.

2 Open the Line subprofile and set the signalling mode to Inband:

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

3 configure Rob Ctl for either wink-inc-200 or wink-inc-400:

```
Rob Ctl=wink-inc-200
```

Note: If the value of Rob Ctl is set to Wink-Start, then Collect DNIS/ANI will be set to N/A, preventing caller ID collection.

4 Configure Collect DNIS/ANI to yes:

```
Collect DNIS/ANI=yes
```

5 Close the Line 1 subprofile.

6 Open the Line 2 subprofile and set the same values for these configuration values.

Using NFAS signalling

When you configure two T1 lines for NFAS signalling, they share a D channel. Configure one line with a primary D channel, and the other with a secondary D channel. The MultiVoice Gateway uses the secondary D channel only if the primary line goes down or if the MultiVoice Gateway receives from the carrier's switch a signal commanding a change to the other D channel.

Note: Both lines must reside in the same slot.

To configure two T1 lines for NFAS:

1 Open Net/T1 > Line Config and set both lines to Trunk service:

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

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

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

3 Keep the default NFAS ID:

```
NFAS ID num=1
```

4 Configure Channel 24 as the primary NFAS D channel:

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

5 Close the Line 1 subprofile.

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

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

7 Keep the default NFAS ID:

```
NFAS ID num=2
```

8 Configure Channel 24 as the secondary NFAS D channel:

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

9 Close the T1 profile.

Testing T1 connections

You can perform T1 line diagnostics to test line configuration from the MultiVoice Gateway user interface. Also, you can use the terminal-server Test command to validate connectivity by placing and answering test phone calls.

Performing T1 line diagnostics

The MultiVoice Gateway provides the following T1 diagnostic commands:

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

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

Validating connectivity

To test whether the MultiVoice Gateway line is functioning normally, use the Test command from the MultiVoice Gateway terminal server. The command causes the MultiVoice Gateway to place a call to itself over the WAN, and to send a number of packets over the connection. This procedure tests the MultiVoice Gateway unit's ability to initiate and receive calls, and demonstrates whether the connection over the digital access line is functional.

Note: The terminal-server Test command uses one channel to dial out and another channel to answer. Consequently, you must set the T1/PRI line is set for bidirectional calling.

To perform a self test:

1 From the Main Edit Menu, select System.

The System menu appears:

```
00-200 System
  00-100 Sys Config
  >00-200 Sys Diag
```

```
  00-300 Security
  00-400 Destinations
  00-500 Dial Plan
```

2 Select Sys Diag.

The Sys Diag menu appears:

```
00-200 Sys Diag
  >00-201 Restore Cfg
  00-202 Save Config
  00-203 Use MIF
  00-204 Sys Reset
  00-205 Term Serv
  00-206 Upd Rem Cfg
```

3 Select Term Serv.

The Terminal Server screen appears:

```
** Ascend Pipeline Terminal Server **

ascend%
```

4 Type **`test`** ***`phone-number`***

where *`phone-number`* is the phone number of the MultiVoice Gateway T1 line.

Note: The most frequent reason for failing to connect is an incorrect phone number.

5 If the test is unsuccessful, verify that you have entered all the T1 line parameters correctly and that your line is correctly provisioned as explained in Appendix B, “Provisioning the Switch.”

6 Enter **`quit`** to exit the terminal server interface.

7 Press the Left-Arrow or the Escape key to return to the Main Edit Menu.

Configuring E1 lines

Each built-in E1 line contains 32 channels, each of which can support one single-channel connection. Depending on the signalling mode used on the line, all 32 channels are available for user data, or 31 channels are available for data with the 32nd is reserved for signalling. E1 line configuration parameters are in a Line Config profile, as shown in the following example for a MAX 4000/6000:

```
Net/E1
   Line Config
      Name=myPTT_line1
      1st Line=Trunk
      2nd Line=Trunk
      Back-to-Back=No
      Line 1...
         Sig Mode=DPNSS
         Switch Type=Net 5
         Framing Mode=G.703
         # Complete=N/A
         Grp B Answer Signal=N/A
         Grp B Busy Signal=N/A
         Grp B No Signal=N/A
         Grp II Signal=N/A
         Answer Delay=N/A
         Caller ID=N/A
         L3 End=X END
         L2 End=B END
         NL Value=64
         LoopAvoidance=7
         Clock Source=Yes
         Overlap Receiving=No
         PRI Prefix #=N/A
         Trailing Digits=N/A
         T302 Timer=N/A
         Ch 1=Switched
         Ch 1 #=1212
         Ch 1 Slot=3
         Ch 1 Prt/Grp=1
         Ch 1 TrnkGrp=5
```

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

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

You can set line 1 and line 2 to Trunk (indicating a standard E1 interface with signalling information) or Disabled.

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

incoming calls to the MultiVoice Gateway. If you need to disable incoming calls, contact your carrier.

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

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

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

Understanding the line interface parameters

This section provides background information about the E1 line interface parameters. (For complete information, see *MAX Reference Guide*.)

E1 signalling mode

An E1 line's signalling mode (Sig Mode) is typically country-specific and can be NONE (leased) or one of the following:

- ISDN—ISDN signalling using the D channel. You must designate the 32nd channel of the E1 line as the D channel.
- DPNSS—The interface supports DPNSS or DASS 2 signalling.
- R2—R2 signalling. This is the R2 signalling protocol specific by ITU-T Recommendation Q.464 (1988) - *(Signalling System R2) Signalling between the outgoing international R2 register and the last incoming R2 register.*
- Argentinian—A version of the R2 signalling protocol supported in Argentina.
- Brazil—A version of the R2 signalling protocol supported in Brazil.
- Czech—A version of the R2 signalling protocol supported in Czech Republic and surrounding states.
- Indian—A version of the R2 signalling protocol supported in India.
- Korean—A version of the R2 signalling protocol supported in Korea.
- Malaysian—A version of the R2 signalling protocol supported in Malaysia.
- Metered—Metered R2 signalling protocol, for use in Brazil and South Africa.
- Chinese—A version of the R2 signalling protocol supported in China.

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

Note: R2 signalling and country-specific signalling options are not supported for MultiVoice Gateways using the MAX 2000

Carrier switch type

Switch Type is the type of network switch providing ISDN service on an E1 PRI line. Like E1 signalling mode, Switch Type is typically a country-specific parameter.

Carrier switch types for E1/PRI lines include:

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

E1 framing

The physical layer of the E1 line uses a type of G.703 framing, which is the standard framing mode used by some E1 ISDN providers and by DASS 2, or 2DS, a variant of G.703 required by most European telecommunications providers.

Specifying digits received on an incoming R2 call

The Number Complete parameter specifies how many digits complete the number of an incoming call using R2 signalling. You can specify end-of-pulsing to indicate that the MultiVoice Gateway should keep on receiving digits until the caller stops sending them, or you can specify a fixed number of digits (up to 10).

Group signalling

Group B signalling and Group II signalling specify the group signal to send before answering a call.

Collecting Caller ID

The Caller ID parameter enables the MultiVoice Gateway to collect the ANI signals for country-specific R2 signalling sets (i.e., `Sig Mode=CZECH`). This parameter must be enabled (`Caller ID=Yes`) in order to support ANI authentication of MultiVoice users on networks processing localized E1 R2 signals.

Required settings for DPNSS or DASS 2 switches

- L3 End and L2 End—Specify CCITT Layer 3 and CCITT Layer 2, respectively.
- NL value—Default value is 64.
- Loop Avoidance—Default value is 7.

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

Clock source for synchronous transmission

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

Understanding the channel configuration parameters

This section provides background information about the E1 channel configuration parameters. (For complete information, see the *MAX Reference Guide*.)

Specifying how to use the channel

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

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

Phone number assignments

Ch *N* # is the add-on number associated with each switched channel.

Examples of E1 configuration

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

Using ISDN signalling

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

1 Open Net/E1 > Line Config > Line 1 and specify ISDN signalling:

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

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

```
         Switch Type=Net 5
```

3 Specify Framing Mode.

```
         Framing Mode=2DS
```

```
2DS is a variant of G.703 required by most European telecommunica-
tions providers. Check with your carrier about which framing mode
to specify.
```

4 Close the E1 profile.

Note: When `Sig Mode=ISDN`, DNIS and ANI are automatically collected.

Example of DPNSS signalling configuration

To configure the E1 line for DPNSS signalling:

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

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

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

Mercury is a variant of DPNSS.

3 Set the framing mode. For example:

```
Framing Mode=2DS
```

2DS is a variant of G.703 required by most European telecommunications providers. Check with your carrier about which framing mode to specify.

4 Make sure that the following parameters are set to their default values, as shown:

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

5 Close the E1 profile.

Setting up a nailed connection

For example, if there are 5 nailed channels at the local end, there must be 5 nailed channels at the remote end, but Channel 1 could be the number of nailed channels must be the same at both ends of the connection, but the channel assignments do not have to match.

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

The following example shows the cursor poised for opening the Line 1 profile:

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

```
Net/E1
   Line Config
      Name=
      1st Line=Trunk
      2nd Line=Disabled
     >Line 1...
```

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

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

3 Close the E1 profile.

Configuring DNIS and ANI collection for E1 R2

Configuration for systems using ITU-T Q.464 standard E1 R2 signalling

To configure DNIS/ANI collection for the ITU standard E1 R2 signalling:

1 Open Net/E1 > Line Config and set both lines to Trunk service:

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

2 Open the Line 1 subprofile and set the signalling mode to R2:

```
Line 1...
   Sig Mode=R2
```

Note: When `Sig Mode=R2`, DNIS and ANI are automatically collected.

3 Close the Line 1 subprofile.

4 Open the Line 2 subprofile and set the same values for these configuration values.

Configuration for systems using localized E1 R2 signalling

To configure ANI collection for localized (country-specific) E1 R2 signalling:

1 Open Net/E1 > Line Config and set both lines to Trunk service:

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

2 Open the Line 1 subprofile and set the signalling mode to appropriate localized R2 signalling option, for example CZECH:

```
Line 1...
   Sig Mode=CZECH
```

3 Set the caller ID mode to enable ANI collection

```
Caller ID=Yes
```

4 Close the Line 1 subprofile.

5 Open the Line 2 subprofile and set the same values for these configuration values.

Testing E1 connections

You can perform E1 line diagnostics to test line configuration from the MultiVoice Gateway, user interface. Also, you can use the terminal-server Test command to validate connectivity by placing and answering test phone calls.

Performing E1 line diagnostics

The MultiVoice Gateway provides the following E1 diagnostic commands:

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

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

Validating the E1 connection

To test whether the MultiVoice Gateway line is functioning normally, use the Test command from the MultiVoice Gateway terminal server. The command causes the MultiVoice Gateway to place a call to itself over the WAN, and to send a number of packets over the connection. This procedure tests the MultiVoice Gateway's ability to initiate and receive calls, and demonstrates whether the connection over the digital access line is functional.

Note: The terminal-server Test command uses one channel to dial out and another channel to answer. Consequently, you must set the E1/PRI line for bidirectional calling.

To perform a self test:

1 From the Main Edit Menu, select System.

The System menu appears:

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

2 Select Sys Diag.

The Sys Diag menu appears:

```
00-200 Sys Diag
  >00-201 Restore Cfg
  00-202 Save Config
```

```
00-203 Use MIF
00-204 Sys Reset
00-205 Term Serv
00-206 Upd Rem Cfg
```

3 Select Term Serv.

The Terminal Server screen appears:

```
** Ascend Pipeline Terminal Server **

ascend%
```

4 Type **`test`** ***`phone-number`***

where *`phone-number`* is the phone number of the MultiVoice Gateway E1 line.

The most frequent cause for failing to connect is an incorrect phone number.

5 If the test is unsuccessful, verify that you have entered all the E1 line parameters correctly and that your line is correctly provisioned as explained in Appendix B, "Provisioning the Switch."

6 Enter **`quit`** to exit the terminal server interface.

7 Press the Left-Arrow or the Escape key to return to the Main Edit Menu.

ISDN call information

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

```
ascend% show calls
```

The command displays statistics about current calls. For example:

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

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

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

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

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

Configuring the serial WAN port

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

The following example shows the serial WAN configuration parameters:

```
Serial WAN
   Mod Config
      Module Name=serial
      Nailed Grp=3
      Activation=Static
      Ext. Clock * 1K=56
```

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

Understanding the serial WAN parameters

This section provides some background information about the serial WAN configuration.

Assigning a group number to the serial WAN bandwidth

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

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

Signals to control the serial WAN data flow

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

Example of a serial WAN configuration

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

1. Open Serial WAN > Mod Config.
2. Assign a module name and a group number.
3. Set the Activation parameter to Static:

```
Serial WAN
   Mod Config
```

```
Module Name=wan-serial
Nailed Grp=3
Activation=Static
```

4 Close the Serial WAN profile.

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

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

(For more information about Frame Relay, see Chapter 7, “Configuring Frame Relay.”)

Configuring ISDN BRI network cards

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

```
Net/BRI
   Line Config
      Name=bri-net
      Switch Type=AT&T
      BRI Analog Encode=Mu-Law
      Line N...
         Enabled=Yes
         Link Type=P_T_P
         B1 Usage=Switched
         B1 Slot=3
         B2 Prt/Grp=1
         B1 Trnk Grp=5
         B2 Usage=Switched
         B2 Slot=3
         B2 Prt/Grp=2
         B2 Trnk Grp=5
         Pri Num=555-1212
         Pri SPID=01555121200
         Sec Num=555-1213
         Sec SPID=01555121300
```

(For more information about each parameter, see the *MAX Reference Guide*.) MultiVoice on the MAX 2000 does not support the use of BRI lines.

Note: After you have configured the line, you might need to configure the card for outbound calls as described in “Configuring the Net BRI line for outbound calls” on page 5-22.

Understanding the Net BRI parameters

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

Assigning a profile name

You can configure several profiles and activate a profile when it is needed. Each profile's name should indicate its usage.

Carrier switch type and how it operates

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

BRI Analog Encode

If you are going to receive modem calls, you can set the BRI Analog Encode parameter to specify the encoding type. (For more information about this parameter, see the *MAX Reference Guide*.)

Link Type

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

Using the BRI line for switched or nailed connections

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

Associating the channel with a slot/port in the MultiVoice Gateway

In the B *N* Slot and B *N* Prt/Grp parameters, you can assign a switched channel to a slot or slot/port combination for a digital modem, AIM port, or Ethernet. This configuration affects both inbound call routing and outbound calls. In effect, it reserves the channel for calls to and from the specified slot or port.

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

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

Assigning the channel to a trunk group

You can assign trunk-group numbers 4 through 9 to channels to make them available for outbound calls. You cannot combine PRI channels with BRI channels in the same trunk group.

Phone number and Service Profile Identifier (SPID) assignments

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

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

Pri SPID and Sec SPID are the SPIDs associated with the Primary and Secondary numbers, respectively.

Examples of Net BRI configurations

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

Configuring incoming switched connections

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

1 Open Net/BRI > Line Config.

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

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

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

```
      Line 1...
         Enabled=Yes
         Link Type=NI-1
```

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

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

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

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

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

7 Close the Net BRI profile.

Configuring the Net BRI line for outbound calls

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

1 Open System > Sys Config and enable trunk groups system-wide:

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

2 Close the System profile.

3 Open Net/BRI > Line Config > Line 1:

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

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

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

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

6 Close the Net BRI profile.

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

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

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

8 Close the Ethernet profile.

To specify that a connection uses a BRI line:

9 Open the Connection profile.

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

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

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

11 Close the Connection profile.

Displaying information about BRI calls

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

```
ascend% show calls
```

The command displays statistics about current calls, for example:

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

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

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

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

Configuring MultiVoice

6

MultiVoice call configuration

To enable MultiVoice calling, you must configure each MultiVoice Gateway with the following information:

- The IP address of the MultiVoice Access Manager
- Whether or not the MultiVoice Access Manager requires users to enter a Personal Identification Number (PIN) for authentication.
- The type of voice compression and coding to use for MultiVoice calls.

Additionally, you may improve MultiVoice call performance by:

- Entering an IP address for a secondary MultiVoice Access Manager.
- Adjusting the frequency and time intervals when a MultiVoice Gateway must register with the MultiVoice Access Manager.
- Enabling use of a fixed or dynamic Jitter Buffer.
- Enabling silence detection and comfort noise generation.
- Modifying the Type of Service (ToS) byte for UDP packet processing.
- Modifying the maximum number of calls a MultiVoice Gateway processes.
- Enabling single-stage dialing.
- Disabling PSTN progress tone cut-through on the local MultiVoice Gateway.

Configuration options

The MultiVoice call configuration options are located in the VOIP Options submenu of the Ethernet profile:

```
Ethernet
   VOIP Options
      GK IP Adrs=192.16.15.2
      2nd GK IP=0.0.0.0
      Keepalive Timer=120
      Reg Retries=5
      Reg Retry Timer=5
      Pri GK Retries=1
      VPN Mode=Yes
      Pkt Audio Mode=G.729
      Frames/Packet=4
      Silence Detect/CNG=No
      Enable Adaptive Jtr Buf=Yes
      Max Jtr Buf Size=19
      Initial Jtr Buf Size=2
      TOS Enabled=No
      Precedence=N/A
      TOS=N/A
      Max VOIP Calls=16
      Near End Cut Through=Yes
      Single Dial Enable=No
```

You must provide an IP address for the GK IP Adrs parameter for the MultiVoice Gateway to process voice calls. This address points to the computer running the MultiVoice Access Manager that will perform all of the Gatekeeper functions for this Gateway. The MultiVoice Gateway can process calls over must IP networks using the factory defaults for the remaining VOIP Options parameters.

Understanding the VOIP parameters

This section provides background information about the VOIP Options parameters. (For complete information, see the *MAX reference Guide*.)

The Gatekeeper IP address

The GK IP Adrs parameter identifies the computer running MultiVoice Access Manager that will perform all the H.323 Gatekeeper functions for this Gateway. Since MultiVoice implements the H.323 direct call model for Voice over IP networks, each Gateway must communicate with an Gatekeeper for processing of call registration, admission and status (RAS) messages. The MultiVoice Gateway will send all call request messages and call processing information to the IP address specified by GK IP Adrs.

The secondary Gatekeeper IP address

The 2nd GK IP parameter identifies the computer running MultiVoice Access Manager that will perform all the H.323 Gatekeeper functions for this Gateway, when it can't register with MVAM on the system identified by GK IP Adrs. This allows a MultiVoice Gateway to continue initiating new calls over the IP network.

When an IP address is not assigned to 2nd GK IP, then the MultiVoice Gateway goes into a *slow poll mode* with the MultiVoice Access Manager at GK IP Adrs. The MultiVoice Gateway attempts registrations with the MVAM at GK IP Adrs at 30-second intervals. During the time the Gateway is unregistered, new calls are *blocked*, which means the MultiVoice Gateway will reject any new calls.

Note: Anytime a MultiVoice Gateway is attempting to register with a Gatekeeper, the Gateway is effectively unregistered with any Gatekeeper. During this period calls are blocked. However, existing calls continue to operate normally.

Controlling keep-alive registration

Once registered with a Gatekeeper, a MultiVoice Gateway re-registers with its currently registered Gatekeeper every 120 seconds. This is called the keep-alive registration. The Keepalive Timer parameter sets the time interval between attempts to reregister with a system running the MultiVoice Access Manager following the initial registration. This value equals the wait time, in seconds, between each attempt to re-register.

You may enter any value between 1 and 65535. Changes to the Keepalive Timer parameter become effective with the next registration cycle.

When the keep-alive registration fails, a MultiVoice Gateway does the following:

- If valid IP addresses (non-null) are configured for both GK IP Adrs and 2nd GK IP, the MultiVoice Gateway attempts to register with the MultiVoice Access Manager at the 2nd GK IP address. Once it successfully registers with the secondary Gatekeeper, the MultiVoice Gateway is operating in *backup mode*.
- If the IP address for 2nd GK IP is null, then the MultiVoice Gateway goes into a slow poll mode with the MultiVoice Access Manager at GK IP Adrs.

Reregistration policy parameters

After a MultiVoice Gateway registers with the MultiVoice Access Manager at 2nd GK IP, it periodically attempts to reregister with the MultiVoice Access Manager at GK IP Adrs. These attempts to reregister with the primary Gatekeeper are initiated after every cycle of five successful registrations with the secondary Gatekeeper. If the Gateway cannot register with the primary Gatekeeper in this mode, it performs keep-alive registration with the secondary Gatekeeper.

The Reg Retries parameter sets the number of attempts a MultiVoice Gateway will make each time it executes keep-alive registration. Since a Gateway may not successfully register on its first attempt, the value for this parameter represents the number of repeated registration attempts a Gateway makes during a registration cycle, until it either registers successfully or until all attempts have failed. You may enter any value between 1 and 200 for Reg Retries. Changes to this value become effective with the next registration cycle. This value defaults to 5 attempts.

The Reg Retry Timer parameter sets the time interval between each registration attempt with a MultiVoice Access Manager. This sets the pause, in seconds, between each registration attempt specified by the Reg Retries parameter. You may specify a time between 1 and 200 seconds. Changes to this value become effective with the next registration cycle. This value defaults to 5 seconds.

The Pri GK Retries parameter sets the number of attempts a MultiVoice Gateway will make whenever it tries to reregister with the MultiVoice Access Manager at GK IP Adrs. Since a Gateway may not successfully register on its first attempt, the value for this parameter represents the number of repeated registration attempts a Gateway makes during a reregistration cycle, until it either registers successfully with the MultiVoice Access Manager at GK IP Adrs or until all attempts have failed. Setting Pri GK Retries to zero (0) disables this feature.You may enter any value between 0 and 200. Changes to this value become effective with the next registration cycle. This value defaults to 1.

PIN collection

The VPN Mode parameter enables/disables collection of a MultiVoice user's Personal Identification Number (PIN). This parameter controls whether a user must enter a separate PIN code when placing a MultiVoice call. If you set `VPN Mode=No` (default), the MultiVoice Gateway prompts callers for their PIN before they enter the destination phone number.

When callers dial into the MultiVoice Gateway, it presents them either with a dial tone or with prompts indicating that MultiVoice Access Manager requires PIN authentication.

The MultiVoice Access Manager creates user PINs automatically when you create user records.

Note: This parameter has no effect on Automatic Number Identification (ANI) authentication.

Voice compression and coding

Voice is transmitted across an IP network as compressed audio frames, which are compressed/uncompressed by the MultiVoice Gateway.

The Pkt Audio Mode parameter is used to select the default audio codec (coder/decoder) used to pack (and unpack) analog speech into digital audio frames. The MultiVoice Gateway supports the following audio codecs:

- G.711 U Law
- G.711 A Law
- G.729(A)
- G.723.1

This parameter defaults to G.711 U Law. Changes to this parameter become effective when you reset the MultiVoice Gateway.

The Frames/Packet parameter sets the number of compressed audio frames assigned to each RTP packet for the audio codec defined by the Pkt Audio Mode parameter. You may assign a value ranging from 1 to 10 packets; the default is 4.

Lowering the value for this parameter reduces the delay and distortion introduced into any given voice call. But a lower value can also degrade performance, because it results in more IP packets per voice call.

Silence detection and comfort noise generation

The MultiVoice Gateway can be configured to detect periods of silence during voice calls, suppress transmission of voice packets during silent periods, and generate white (comfort) noise to assure the user that a call is still connected during silent periods.

The Silence Detect/CNG parameter is used to enable/disable the silence detection and suppression, and noise generation feature on the MultiVoice Gateway. Enabling this feature prevents silence frames from being passed over the network, reducing the effective bandwidth of the MultiVoice call. During those silent periods, the local Gateway will generate background (comfort) noise to assure the caller that the call is still connected during these silent periods. You may toggle between `Yes` and `No`, to enable/disable this feature. This value defaults to No. Changes to this value become effective with the next MultiVoice call.

Note: This parameter is ignored (`Silence Detect/CNG=N/A`) when the MultiVoice Gateway uses the G.723.1 audio codec (`Pkt Audio Mode=G.723`).

Dynamic jitter buffer control

MultiVoice calls are processed using packet-based jitter buffering. As the MultiVoice Gateway processes each voice call, the jitter buffer size is automatically adjusted to a length of time appropriate for processing a fixed number of RTP packets, regardless of which audio codec is used to process those packets. A unique jitter buffer is opened for each call, which dynamically adjusts its size to accommodate network conditions, such as:

- low latency as a result of high network throughput
- increased latency as a result of reduced network throughput

The Enable Adaptive Jtr Buf parameter changes the jitter buffer mode to either adaptive or fixed for the MultiVoice calls. When the adaptive mode is selected, the jitter buffer size will increase or decrease, depending on the number of late or out-of-sequence packets received, between the values set for Max Jtr Buf Size and Initial Jtr Buf Size. You may toggle between `Yes` and `No`, to enable/disable this feature. This value defaults to Yes. Changes to this value become effective with the next MultiVoice call.

The Max Jtr Buf Size parameter sets the maximum jitter buffer size for a call. When using adaptive mode, the jitter buffer may increase to accommodate the entered number of audio packets, based on the in-coming audio packet volume. You may enter a value between 1 and 19 (packets). This allows the MultiVoice Gateway to expand the length of a call's jitter buffer to a size proportionate to the selected number of audio packets. This value defaults to 19. Changes to this value become effective with the next MultiVoice call.

The Initial Jtr Buf Size parameter sets the initial jitter buffer size for a call. When using adaptive mode, the MultiVoice Gateway will open a jitter buffer to accommodate the entered number of audio packets, based on the in-coming audio packet volume. In either adaptive or fixed mode, the jitter buffer is built-up to Initial Jtr Buf Size at start-up. You may enter a value between 1 and 19 (packets). This value defaults to 2. Changes to this value become effective with the next MultiVoice call.

Note: Under certain circumstances, the minimum jitter buffer size may be less then the initial jitter buffer set through the MAX menu. The initial jitter buffer size and minimum jitter buffer will be the same when the initial jitter buffer size configured is 1.

Type of Service (TOS) management

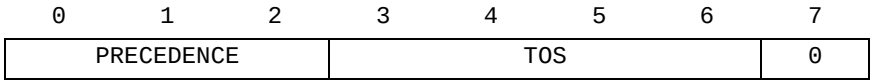
This group of parameters allows you to change the Precedence bits (bit0 - bit2) and the TOS bits (bit3 - bit6) for the Type of Service (TOS) byte use by UDP voice packets. In networks which support processing IP packets based on precedence, the Type of Service byte is used to attain a certain level of UDP packet processing by manipulating values for delay, throughput and reliability.

Type of Service is an eight (8) bit parameter found in the header of an IP datagram. It is divided into three fields, containing the following values:

Bits 0-2: Precedence.

Bits 3-6: TOS (performance cost).

Bit 7: Reserved for Future Use.



The TOS Enabled parameter enables/disables user configuration of the Type of Service byte. By setting the value for TOS Enable to Yes, you may change TOS byte by assigning values to the Precedence and TOS parameters. You may toggle the value for TOS Enabled between Yes, to enable operator configuration of the ToS byte, or No, to disable this feature. This value defaults to Yes. Changes to this value become effective with the next call.

The Precedence parameter sets the importance or priority of the UPD packet, bit0 through bit2 of the Type of Service octet. This is represented by a Hexadecimal value, which defines how the network will process the UDP packets.

These are requested values. The impact of a selected value on UDP packet processing is network dependent (see RFC791). This value defaults to 101. Changes to this parameter take effect the next MultiVoice call.

The TOS parameter controls processing attribute management, bit3 through bit6 of the Type of Service octet. These bits denote how the network should make trade-offs between throughput, delay, reliability and cost when processing the UDP packets.

These are requested values. The impact of a selected value on UDP packet processing is network dependent (see RFC1349). This value defaults to Minimize Delay. Changes to this parameter take effect the next MultiVoice call.

Limiting the Gateway's call volume

The Max VOIP Calls parameter is used to reduce the maximum number of MultiVoice calls a Gateway can process, by reducing the number of available Digital Signal Processors (DSPs). Any number between 1 and the maximum number of DSPs installed on the MultiVoice Gateway may be assigned to this parameter. This value defaults to the maximum call volume for the installed MAX platform. Changes to this value become effective with the next call. This feature is useful when continued high call volumes on a network affect the call quality. Adjusting the value for Max VOIP Calls will allow a MultiVoice Gateway to allocate more system resources to processing fewer calls, resulting in improved call quality.

Note: When active calls exceed the Max VOIP Calls limit, the caller will hear a busy signal from the MultiVoice Gateway.

Controlling call-progress tones on a local Gateway

The Near End Cut Through parameter enables the call-progress tones from the distant PSTN to be heard by the caller connected to the local MultiVoice Gateway. This provides answer supervision support for MultiVoice Gateways using non-PRI trunks, by processing the call progress tones from the distant PSTN.

Setting this value to Yes will enable passing the PSTN-generated call progress tones across the IP network, using RTP packets between Gateways. These audio signals from distant PSTN are compressed by the distant Gateway for transmission across the IP network, then uncompressed by the local Gateway and played for the caller. Setting this value to No will cause the Gateway to generate local progress tones in response to Q.931 messages.

Changes to this value become effective with the next call. This value defaults to Yes. Network capacity and voice quality are the determining factors as to when this parameter should be modified.

Single-stage dialing

The Single Dial Enable parameter is used to enable/disable single stage dialing of MultiVoice calls. Setting this value to Yes enables the MultiVoice Gateway to extract the Dialed Number Identification Service (DNIS) string from a single dialed entry. Setting this value to No disables DNIS string collection, requiring users to dial the MultiVoice Gateway, first, wait for a dial tone form the MultiVoice Gateway, then dial the called telephone number. This value defaults to No. Changes to this value become effective with the next VoIP call.

Single stage dialing will work with MultiVoice Gateways under the following conditions:

- You are using T1 inband trunks, and the switch (or PBX) can relay DTMF signals to the MultiVoice Gateway.
- You are using T1 PRI trunks.
- You have enable collection of DNIS on the MultiVoice Gateway. (For information on configuring DNIS collection see “Collecting DNIS and ANI” on page 5-4.)

MultiVoice configuration examples

Configuring Gatekeepers

To configure MultiVoice communications with a primary Gatekeeper:

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

2 Press Enter to open the edit field for GK IP Adrs:

```
GK IP Adrs:
     [0.0.0.0]
```

3 Enter the IP address of the MultiVoice Access Manager. For example:

```
GK IP Adrs = 10.10.10.10
```

The MultiVoice Gateway must be able to send packets to and receive packets from the MultiVoice Access Manager. You can verify connectivity by Pinging the IP address of the MultiVoice Access Manager from the MultiVoice Gateway terminal server. If the Pings fail, see your network administrator about possible routing problems.

To configure MultiVoice communications with both a primary and secondary Gatekeeper:

1. Open the Ethernet > Mod Config > VOIP Options menu.
2. Set GK IP Adrs to the IP address of the primary MultiVoice Access Manager. For example:

   ```
   GK IP Adrs = 10.10.10.10
   ```

3. Set 2nd GK IP to the IP address of the secondary MultiVoice Access Manager. For Example:

   ```
   2nd Gk IP = 11.11.11.11
   ```

   Verify connectivity by Pinging the IP address of both MultiVoice Access Managers from the MultiVoice Gateway terminal server. If the Pings fail, see your network administrator about possible routing problems.

Configuring Gateway registration policy

To configure registration policy for a MultiVoice Gateway:

1. Open the Ethernet > Mod Config > VOIP Options menu.
2. Set the Keepalive Timer by pressing Enter to open the edit field, and entering a value between 1 and 65535 (seconds). For example:

   ```
   Ethernet
      Mod Config
        Keepalive Timer:
          [120]
   ```

3. Press Enter to save your change.

   Note: If you change this parameter, you should also change the `registrationDuration` parameter on the MultiVoice Access Manager. A Gateways's registration with MVAM will automatically expire within that time frame.

4. Set the Reg Retries by pressing Enter to open the edit field, and entering a value between 0 and 200 (attempts). For Example:

   ```
   Ethernet
      Mod Config
        Reg Retries:
          [5]
   ```

5. Press Enter to save your change.
6. Set the Reg Retry Timer by pressing Enter to open the edit field, and entering a value between 0 and 200 (seconds). For Example:

   ```
   Ethernet
      Mod Config
        Reg Retry Timer:
          [5]
   ```

7. Press Enter to save your change.
8. Set the Pri GK Retries by pressing Enter to open the edit field, and entering a value between 0 and 200 (attempts). For Example:

   ```
   Ethernet
      Mod Config
        Pri GK Retries:
          [5]
   ```

9 Press Enter to save your change.

Gatekeeper registration policy and failure detection

At H.323 stack initialization time, the MultiVoice Gateway attempts to register with the primary Gatekeeper. The H.323 stack will not initialize when the primary Gatekeeper is not configured. Registration with a primary Gatekeeper fails when the Gateway cannot register with the primary gatekeeper after all attempts have been made. By default, the MultiVoice Gateway makes five (5) registration attempts at 5-second intervals.

When registration with the primary Gatekeeper fails:

- If there is a valid address (non-null) configured for the 2nd GK IP, a MultiVoice Gateway will attempt to register with the secondary Gatekeeper; applying the same registration policy (five (5) registration attempts at 5-seconds intervals).
- If there is no valid address (null) configured for the 2nd GK IP, then the MultiVoice Gateway goes into a slow poll mode.

Configuring PIN authentication

To configure PIN authentication on a MultiVoice Gateway:

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

2 Set the VPN mode parameter by pressing Enter to toggle between Yes and No. For Example:

```
Ethernet
   Mod Config
     VPN Mode=Yes
```

If the MultiVoice Access Manager requires user PIN authentication, set `VPN Mode=No`.

If you set `VPN Mode=No`, the MultiVoice Gateway prompts callers for their PIN before they enter the destination phone number.

Configuring ANI authentication

To configure ANI authentication on a MultiVoice Gateway:

To configure DNIS/ANI collection for a T1 using robbed-bit signaling:

1 Open `Net/T1 > Line Config` profile.

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

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

3 configure Rob Ctl for either wink-inc-200 or wink-inc-400:

```
Rob Ctl=wink-inc-200
```

Note: If the value of Rob Ctl is set to Wink-Start, then Collect DNIS/ANI will be set to N/A, preventing caller ID collection.

4 Configure Collect DNIS/ANI to yes:

```
Collect DNIS/ANI=yes
```

5 Close the Line 1 subprofile.

Caution: If you elect to use both ANI and PIN authentication, entry of an invalid PIN will cause the call to be rejected. If you enter a valid PIN, but the ANI of the calling number does not match the information in the user database, the call will be rejected.

Configuring audio compression

To configure the default audio compression scheme for a MultiVoice Gateway:

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

2 Set the Pkt Audio Mode parameter by pressing Enter to toggle through the list of supported audio compression and coding methods. For Example:

```
Ethernet
   Mod Config
     Pkt Audio Mode=G.711 U Law
```

The default value for this parameter is G.711 U law. You may toggle through and select values representing these supported audio codecs:

Parameter value	Audio codec
G.711 U Law	G.711 U Law
G.711 A Law	G.711 A Law
G.729	G.729(A)
G.723	G.723.1

3 Set the Frames/Packet parameter by pressing Enter to open the edit field, and entering a value between 1 and 10 (packets). For Example:

```
Ethernet
   Mod Config
     Frames/Packet=1
```

The default is 4.

Note: When a different audio codec is dynamically selected during call setup, the MultiVoice Gateway uses the default value of 4 frames per RTP packet to process that call,

4 Press Enter to save your change.

5 Set the Silence Detect/CNG parameter by pressing Enter to toggle between Yes and No, enabling or disabling silence detection and suppression and comfort noise generation. For Example:

```
Ethernet
   Mod Config
     Silence Detect/CNG=Yes
```

6 Press Enter to save your change.

You must set `Silence Detect/CNG=Yes` on both the local Gateway and distant Gateway. Comfort noise is generated by a MultiVoice Gateway only when using the G.729 codec (`Pkt Audio Mode=G.729`). This parameter defaults to N/A when `Pkt Audio Mode=G.723`. When this parameter is enabled, `Silence Detect/CNG=Yes`, the dynamic jitter buffer is not used (`Enable Adaptive Jtr Buf=N/A` and `Max Jtr Buf Size=N/A`).

Impact of configurable voice frames on IP packet size

The size of each IP packet is determined by the number of audio frames contained in each RTP packet plus the size of the respective headers required to construct the frame.

The RTP packet header contains a time stamp and sequence number used to reconstruct the voice message. The header size is fixed at 12 bytes. The size of the packet data will vary, depending upon the type of audio codec defined for Pkt Audio Mode:

Table 6-1. Impact of configurable voice frames on IP packet size

Audio codec	Number of voice frames	RTP packet size	Ethernet frame size
G.729	1 @ 10ms ea.	22 bytes	64 bytes
	2 @ 10ms ea.	32 bytes	74 bytes
	3 @ 10ms ea.	42 bytes	84 bytes
	4 @ 10ms ea.	52 bytes	94 bytes
	5 @ 10ms ea.	62 bytes	104 bytes
	6 @ 10ms ea.	72 bytes	114 bytes
	7 @ 10ms ea.	82 bytes	124 bytes
	8 @ 10ms ea.	92 bytes	134 bytes
	9 @ 10ms ea.	102 bytes	144 bytes
	10 @ 10ms ea.	112 bytes	154 bytes
G.723.1	1 @ 30ms ea.	32 Bytes	74 Bytes
	2 @ 30ms ea.	52 Bytes	94 Bytes
	3 @ 30ms ea.	72 Bytes	114 Bytes
	4 @ 30ms ea.	92 Bytes	134 Bytes
	5 @ 30ms ea.	112 Bytes	154 Bytes
	6 @ 30ms ea.	132 Bytes	174 Bytes
	7 @ 30ms ea.	152 Bytes	194 Bytes
	8 @ 30ms ea.	172 Bytes	214 Bytes
	9 @ 30ms ea.	192 Bytes	234 Bytes
	10 @ 30ms ea.	212 Bytes	254 Bytes

Table 6-1. Impact of configurable voice frames on IP packet size

Audio codec	Number of voice frames	RTP packet size	Ethernet frame size
G.711	1 @ 5ms ea.	52 Bytes	94 Bytes
	2 @ 5ms ea.	92 Bytes	134 Bytes
	3 @ 5ms ea.	132 Bytes	174 Bytes
	4 @ 5ms ea.	172 Bytes	214 Bytes
	5 @ 5ms ea.	212 Bytes	254 Bytes
	6 @ 5ms ea.	252 Bytes	294 Bytes
	7 @ 5ms ea.	292 Bytes	334 Bytes
	8 @ 5ms ea.	332 Bytes	374 Bytes
	9 @ 5ms ea.	372 Bytes	414 Bytes
	10 @ 5ms ea.	412 Bytes	454 Bytes

Configuring the dynamic jitter buffer

To configure the dynamic jitter buffer for a MultiVoice call:

1. Open the Ethernet > Mod Config > VOIP Options menu.
2. Set the Enable Adaptive Jtr Buf parameter by pressing Enter to toggle between `Yes` and `No`, enabling or disabling the dynamic jitter buffer feature. For Example:

   ```
   Ethernet
      Mod Config
        Enable Adaptive Jtr Buf=Yes
   ```

   This parameter defaults to `Yes`. If this parameter is changed to `No`, the MultiVoice Gateway will use the value set for Initial Jtr But Size to create static jitter buffers for calls.
3. Set the Max Jtr Buf Size parameter by pressing Enter to open the edit field, and entering a value between 1 and 19 (packets). For Example:

   ```
   Ethernet
      Mod Config
        Max Jtr Buf Size=19
   ```
4. Press Enter to save your change.

   This parameter defaults to `19`. This parameter is ignored if the Enable Adaptive Jtr Buf parameter is set to `No`.
5. Set the Initial Jtr Buf Size parameter by pressing Enter to open the edit field, and entering a value between 1 and 19 (packets). For Example:

   ```
   Ethernet
      Mod Config
        Initial Jtr Buf Size=2
   ```
6. Press Enter to save your change.

This parameter defaults to 2. This parameter is ignored if the Packet Audio Mode parameter is set to G.723.

Note: For certain MultiVoice Gateway configurations, dynamic jitter buffer support is not available. Table 6-2 summarizes those configuration items which affect jitter buffer operations.

Table 6-2. Configuration dependencies affecting jitter buffer processing

Configured mode	Enable Adaptive Jtr Buf	Max Jtr Buf Size	Initial Jtr Buf Size
Pkt Audio Mode=G.723	N/A	N/A	N/A
Silence Detect/CNG=Yes	N/A	N/A	Active
Fixed Jtr Buf Mode	No	N/A	Active
Adaptive Jtr Buf Mode	Yes	Active	Active

Determining jitter buffer size

The dynamic jitter buffer size is a function of the following:

- The RTP packet duration (in milliseconds) for the selected audio codec,
- The number of RTP packets defined for the jitter buffer.

The dynamic jitter buffer size is determined by multiplying the number of RTP packets entered for the initial and maximum jitter buffer parameters and packet duration, the total speech in milliseconds contained in one RTP packet:

Initial Jtr Buf Size x *Packet Duration (ms)*

Max Jtr Buf Size x *Packet Duration (ms)*

For example, in fixed mode, if the Initial Jtr Buf Size=5, and an in-coming call used the G.711 codec with one audio frame per packet, and has a packet duration of 5ms, then:

5 (Packets) x 5ms/packet = 25ms (jitter buffer length)

The instantaneous jitter buffer size within the call is 25ms. If a second in-coming call used the G.729(A) codec, and had five audio frames per packet, with a packet duration of 50ms, then the instantaneous jitter buffer size within this call would be 250ms.

Table 6-3 and Table 6-4 contain the supported per call jitter buffer lengths:

Table 6-3. Jitter buffer length (in milliseconds) for the G.711 audio codec

Jitter[a] buffer packets	Packet duration (ms), for one to 10 audio frames per RTP packet using the G.711 codec									
	1 frame @5ms	2 frames @10ms	3 frames @15ms	4 frames @20ms	5 frames @25ms	6 frames @30ms	7 frames @35ms	8 frames @40ms	9 frames @45ms	10 frames @50ms
1	5	10	15	20	25	30	35	40	45	50
2	10	20	30	40	50	60	70	80	90	100

Table 6-3. Jitter buffer length (in milliseconds) for the G.711 audio codec

Jitter[a] buffer packets	Packet duration (ms), for one to 10 audio frames per RTP packet using the G.711 codec									
	1 frame @5ms	2 frames @10ms	3 frames @15ms	4 frames @20ms	5 frames @25ms	6 frames @30ms	7 frames @35ms	8 frames @40ms	9 frames @45ms	10 frames @50ms
3	15	30	45	60	75	90	105	120	135	150
4	20	40	60	80	100	120	140	160	180	200
5	25	50	75	100	125	150	175	200	225	250
6	30	60	90	120	150	180	210	240	270	300
7	35	70	105	140	175	210	245	280	315	350
8	40	80	120	160	200	240	280	320	360	400
9	45	90	135	180	225	270	315	360	405	450
10	50	100	150	200	250	300	350	400	450	500
11	55	110	165	220	275	330	385	440	495	550
12	60	120	180	240	300	360	420	480	540	600
13	65	130	195	260	325	390	455	520	585	650
14	70	140	210	280	350	420	490	560	630	700
15	75	150	225	300	375	450	525	600	675	750
16	80	160	240	320	400	480	560	640	720	800
17	85	170	255	340	425	510	595	680	765	850
18	90	180	270	360	450	540	630	720	810	900
19	95	190	285	380	475	570	665	760	855	950

a. This is the value entered for either Max Jtr Buf Size and/or Initial Jit Buf Size.

Table 6-4. Jitter buffer length (in milliseconds) for the G.729(A) audio codec

Jitter[a] buffer packets	Packet duration (ms), for one to 10 audio frames per RTP packet using the G.729(A) codec									
	1 frames @10ms	2 frames @20ms	3 frames @30ms	4 frames @40ms	5 frames @50ms	6 frames @60ms	7 frames @70ms	8 frames @80ms	9 frames @90ms	10 frames @100ms
1	10	20	30	40	50	60	70	80	90	100
2	20	40	60	80	100	120	140	160	180	200

Table 6-4. Jitter buffer length (in milliseconds) for the G.729(A) audio codec

Jitter[a] buffer packets	Packet duration (ms), for one to 10 audio frames per RTP packet using the G.729(A) codec									
	1 frames @10ms	2 frames @20ms	3 frames @30ms	4 frames @40ms	5 frames @50ms	6 frames @60ms	7 frames @70ms	8 frames @80ms	9 frames @90ms	10 frames @100ms
3	30	60	90	120	150	180	210	240	270	300
4	40	80	120	160	200	240	280	320	360	400
5	50	100	150	200	250	300	350	400	450	500
6	60	120	180	240	300	360	420	480	540	600
7	70	140	210	280	350	420	490	560	630	700
8	80	160	240	320	400	480	560	640	720	800
9	90	180	270	360	450	540	630	720	810	900
10	100	200	300	400	500	600	700	800	900	1000
11	110	220	330	440	550	660	770	880	990	1100
12	120	240	360	480	600	720	840	960	1080	1200
13	130	260	390	520	650	780	910	1040	1170	1300
14	140	280	420	560	700	840	980	1120	1260	1400
15	150	300	450	600	750	900	1050	1200	1350	1500
16	160	320	480	640	800	960	1120	1280	1440	1600
17	170	340	510	680	850	1020	1190	1360	1530	1700
18	180	360	540	720	900	1080	1260	1440	1620	1800
19	190	380	570	760	950	1140	1330	1520	1710	1900

a. This is the value entered for either Max Jtr Buf Size and/or Initial Jit Buf Size.

Configuring the Type of Service (ToS) priority

To configure the IP Type of Service (ToS) byte for UDP voice packets:

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

2 Set the TOS Enabled parameter by pressing Enter to toggle between `Yes` and `No`, enabling or disabling the ToS byte configuration. For Example:

```
Ethernet
   Mod Config
     TOS Enabled=Yes
```

This parameter defaults to `Yes`. If this parameter is changed to `No`, MultiVoice will request the network's default processing priority for UDP voice packets.

3 Set the Precedence parameter by pressing Enter to toggle through the list of hexadecimal values which set the bit0 through bit2 of the ToS byte. For Example:

```
Ethernet
   Mod Config
     Precedence=100
```

The default is 101. You may toggle through and select values (Hexadecimal) representing these processing priorities, as defined by RFC791:

Parameter value	Processing priority
000	Routine
001	Priority
010	Immediate
011	Flash
100	Flash Override
101	CRITIC/ECP (default)
110	Internetwork Control
111	Network Control

4 Set the TOS parameter by pressing Enter to toggle through a list of processing cost options for bit3 through bit6 of the ToS byte. For Example:

```
Ethernet
   Mod Config
     TOS=Minimize Delay
```

This parameter defaults to `Minimize Delay`. You may toggle through and select from the following values (assigning the associated bit values to the ToS byte) for this parameter, as defined by RFC1349:

Parameter value	Bit values
Minimize Delay	1000
Maximize Throughput	0100
Maximize Reliability	0010
Minimize Cost	0001
Normal (network control)	0000

Configuring Gateway call volumes

To configure the call volume for a MultiVoice Gateway:

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

2 Set the Max VOIP calls parameter by pressing Enter to open the edit field, and entering a value between 1 and the built-in maximum call volume for the MultiVoice Gateway. For Example:

```
Ethernet
   Mod Config
     Max VOIP Calls=64
```

This parameter defaults to the built-in maximum call volume. TAOS Release 7.0, supports the following maximum number of voice calls for the MAX gateway.

MAX platform	Maximum call volume
MAX 2000	16
MAX 400x	16
MAX 6000	64

Note: The built-in maximum call volumes used by this feature for each MAX platform is defined (hardcoded) into the MultiVoice for the MAX software. These values do not reflect actual call volumes achieved in either a testing or production environment.

Configuring local call progress tone processing

To configure local call progress tone processing on a MultiVoice Gateway:

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

2 Set the Near End Cut Through parameter by pressing Enter to toggle between `Yes` and `No`. For Example:

```
Ethernet
   Mod Config
     Near End Cut Through=Yes
```

This value defaults to `Yes`. Setting this value to `No` will cause the near end Gateway to generate call progress tones, rather than passing the network tones from the PSTN.

Note: When NO is selected, callers may hear silence if no Q.931 messages are received by the local MultiVoice Gateway

Using Near-end cut through

This feature provides answer supervision support for MAX gateways using non-PRI trunks, by processing the call progress tones from the distant PSTN as either:

- Audio frames passed between two MAX gateways using RTP packets,
- Locally generating call progress tones from the Near End Gateway, based upon Q.931 call processing messages.

This feature provides the following functionality:

- Pass-through of country specific call progress tones between MAX gateways using RTP packets.

  When a Far End Gateway receives call progress tones from the PSTN, the tones are stored as audio frames, then transmitted across the IP network in RTP packets. Upon receiving the RTP packets, the Near End Gateway decodes and sends these tones to the calling end-point.

- The ability to enable/disable network tone cut-through on the Near End Gateway.

  Network tone cut-through may be toggled on/off through the MAX menu. Disabling this feature will cause the MAX gateway to ignore RTP audio signaling and have the Near End

Gateway generate local progress tones in response to Q.931 messages received from the Far End Gateway.

Note: In TAOS Release 7.0, the fast H.245 (start H.245 before Q.931 CONNECT) is always used and has no impact on this feature.

Configuring single-stage dialing

To configure single-stage dialing on a MultiVoice Gateway:

1. From the Net/T1 or Net/E1 line menu, enable DNIS collection. (For information see "Collecting DNIS and ANI" on page 5-4.)
2. Open the Ethernet > Mod Config > VOIP Options menu.
3. Set the Single Dial Enable parameter by pressing Enter to toggle between Yes and No. For Example:

```
Ethernet
   Mod Config
     Single Dial Enable=Yes
```

This value defaults to `No`. You will still be prompted to enter a separate PIN if you set VPN Mode=No, before the call is connected.

Using single-stage dialing without PIN authentication

In this configuration, users do not need to enter a PIN authentication to complete a MultiVoice call (`VPN Mode=Yes`) or users are authenticated using ANI. Callers enter only the MultiVoice access number followed by the destination phone number (DNIS). For example they can enter 997325551212:

99	The access number. This may be either single or multiple digits, configurable by the service provider. This number is not forwarded to the destination Gateway.
7325551212	The destination phone number. This is a real destination number (DNIS) which must be sent to destination Gateway. This number could be a PBX extension (ie.3103 in company private phone network) or a full public phone number as used here.

Using use single-stage dialing with PIN authentication

In this configuration, users will enter the access number, followed by the destination phone number, and are prompted to enter their PIN to complete a MultiVoice call (`VPN Mode=No`). Callers enter the MultiVoice access number and destination phone number (DNIS) all at-one-time, then hear the Personal Identification Number (PIN) prompt (three short beeps). (In future releases a caller will hear a voice announcement "please enter you PIN number".) The user must enter the PIN to initiate call processing.

For information on configuring DNIS collection see "Collecting DNIS and ANI" on page 5-4.

Using authentication

When callers dial into the MultiVoice Gateway:

- If PIN authentication is enabled, the Gateway presents the caller either with a dial tone or with a prompt indicating that the MultiVoice Access Manager requires PIN authentication.
- If ANI authentication is enabled, the Gateway collects the ANI information from the caller's telephone, passes it to MVAM for verification, then presents the caller either with second dial tone, from the Gateway, or a fast-busy tone when it rejects a call.

When you do not require PIN authentication

When you do not configure PIN authentication, the MultiVoice Gateway processes calls as follows:

1 The caller dials the local MultiVoice Gateway.

2 The local MultiVoice Gateway presents a dial tone to the caller.

3 The caller enters the destination phone number, followed by the pound sign (#).

4 The local MultiVoice Gateway initiates a session with the MultiVoice Access Manager, passing the destination phone number to it.

5 The MultiVoice Access Manager sends the local MultiVoice Gateway the IP address of the destination MultiVoice Gateway, selected on the basis of configured coverage areas.

If the MVAM finds no MultiVoice Gateway with a coverage area that supports the called number, the local MultiVoice Gateway disconnects the call.

6 The local MultiVoice Gateway initiates a session with the destination MultiVoice Gateway.

7 The destination MultiVoice Gateway initiates a session with the MVAM to determine if it approved the call. The MultiVoice Access Manager acknowledges the call request from the distant Gateway.

If the MVAM rejects the call request, the destination MultiVoice Gateway disconnects the call.

8 The destination MultiVoice Gateway dials the destination phone number, and the connection is complete.

If the caller does not press the pound sign after entering a string of digits, the MultiVoice Gateway waits for a timer to expire, then sends the string to the MultiVoice Access Manager. Initially set to 16 seconds, the timer starts running when the caller enters the first digit, but restarts after each subsequent digit. However, each restart decrements the timer by one seconds, up to a maximum of 14. If the caller enters 15 or more digits, the MultiVoice Gateway waits two seconds before sending the string.

If the call is not established in several seconds, the local MultiVoice Gateway sends a *tick-tock* sound to the caller which indicates that the call is still proceeding.

Note: Unless your T1 or E1 line supports ISDN signaling, callers might not receive some call information, such as busy signals.

When you require PIN authentication

If you configure PIN authentication, the MultiVoice Access Manager processes calls as follows:

1 The caller dials the local MultiVoice Gateway.

2 The local MultiVoice Gateway presents three quick tones to the caller.

3 The caller enters a PIN, followed by the pound sign (#).

If the pound sign is omitted, the MultiVoice Gateway sends the user's input after a few seconds.

4 The caller enters the destination phone number, followed by the pound sign (#).

5 The local MultiVoice Gateway initiates a session with the Gatekeeper running the MultiVoice Access Manager and passes the PIN and destination phone number to it.

If the caller enters an incorrect PIN the MultiVoice Gateway prompts for a new PIN by sending the caller a single long tone followed by three quick tones. The MultiVoice Gateway allows three incorrect PINs before disconnecting the caller.

6 If the caller enters a correct PIN the MultiVoice Access Manager selects the IP address of the destination MultiVoice Gateway, on the basis of configured coverage areas, and sends it to the local MultiVoice Gateway.

If MVAM finds no MultiVoice Gateway with a coverage area that supports the called number, the local MultiVoice Gateway disconnects the call.

7 The local MultiVoice Gateway initiates a session with the destination MultiVoice Gateway.

8 The destination MultiVoice Gateway initiates a session with the MVAM to determine if it approved the call. The MultiVoice Access Manager acknowledges the call request from the distant Gateway.

If the MVAM rejects the call request, the destination MultiVoice Gateway disconnects the call.

9 The destination MultiVoice Gateway dials the destination phone number to complete the connection.

Note: If you require PIN authentication, you must set the Ethernet > Mod Config > VOIP Options > VPN Mode to No on all registered MultiVoice Gateways. Otherwise, callers will not be prompted for their PINs, and their calls will fail.

When callers dial into the MultiVoice Gateway, it presents them either with a dial tone or with prompts indicating that MultiVoice Access Manager requires PIN authentication.

If the caller does not press the pound sign after entering a string of digits, the MultiVoice Gateway waits for a timer to expire, then sends the string to the Gatekeeper running the MultiVoice Access Manager. Initially set to 16 seconds, the timer starts running when the caller enters the first digit, but restarts after each subsequent digit. However, each restart decrements the timer by half a second, up to 14.5 seconds. If the caller enters 30 or more digits, the MultiVoice Gateway waits two seconds before sending the string.

If the call is not established within several seconds, the local MultiVoice Gateway sends a *tick-tock* sound to the caller to indicate that the call is still proceeding.

When you require ANI authentication

If you configure ANI authentication, the MultiVoice Gateway processes calls as follows:

1 The caller dials the local MultiVoice Gateway.

2 The local MultiVoice Gateway presents a dial tone to the caller.

3 The caller enters the destination phone number, followed by the pound sign (#).

Note: The caller may experience up to 10 seconds of silence after dialing during ANI processing.

4 The local MultiVoice Gateway collects the ANI for the calling phone number.

5 The MultiVoice Gateway initiates a session with the Gatekeeper running MultiVoice Access Manager and passes the ANI and destination phone number to it.

6 MultiVoice Access Manager compares the ANI to the User Alias information in the user database.

If the ANI does not match a User Alias, MultiVoice Access Manager disconnects the caller.

7 If the ANI matches a User Alias, MultiVoice Access Manager selects the IP address of the destination MultiVoice Gateway, on the basis of configured coverage areas, and sends it to the local MultiVoice Gateway.

If MVAM finds no MultiVoice Gateway with a coverage area that supports the called number, the local MultiVoice Gateway disconnects the call.

8 The local MultiVoice Gateway initiates a session with the destination MultiVoice Gateway.

9 The destination MultiVoice Gateway initiates a session with the MVAM to determine if it approved the call. The MultiVoice Access Manager acknowledges the call request from the distant Gateway.

If the MVAM rejects the call request, the destination MultiVoice Gateway disconnects the call.

10 The destination MultiVoice Gateway dials the destination phone number to complete the connection.

The MultiVoice Gateway collects the caller's ANI and forwards it, in the Acknowledge Request (ARQ) message, along with the destination phone number, to the MultiVoice Access Manager. If the ANI matches the information in the user database, call setup continues.

Note: Since the MultiVoice Gateway collects both ANI and DNIS as a single operation, callers may experience a delay of up to 10 seconds for processing before hearing a dial tone, fast-busy, or other call progress tones.

For information on configuring ANI collection see "Collecting DNIS and ANI" on page 5-4

Caution: ANI authentication does not work across WANs or behind PBXs that do not support delivery of DNIS/ANI.

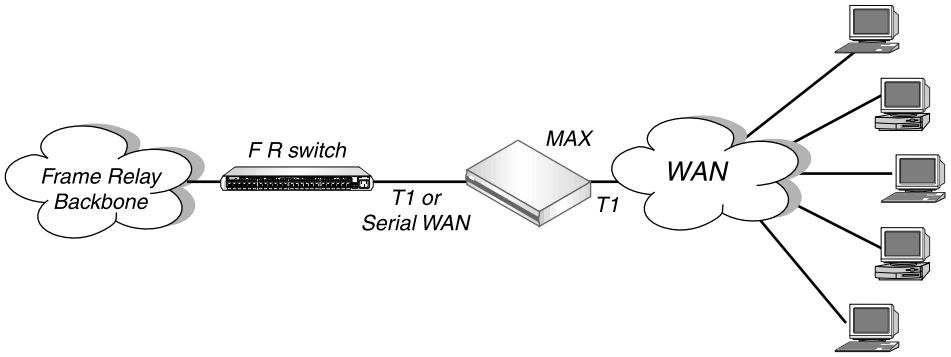
Configuring Frame Relay

7

Using the MultiVoice Gateway as a Frame Relay concentrator

In a Frame Relay backbone, every access line connects directly to a Frame Relay (FR) switch. In the past, most connections to the Frame Relay network were relatively high speed, (full T1 or E1 lines, for example). With recent changes in Frame Relay pricing, many sites now want to concentrate many low-speed dial-in connections into one high-speed nailed connection to a Frame Relay switch. If you configure the MultiVoice Gateway as a Frame Relay concentrator, it accepts incoming dial-in connections as usual and forwards them out to a Frame Relay switch, as shown in Figure 7-1.

Figure 7-1. The MultiVoice Gateway operating as a Frame Relay concentrator



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

Configuration of the MultiVoice Gateway as a Frame Relay concentrator involves configuring the following elements:

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

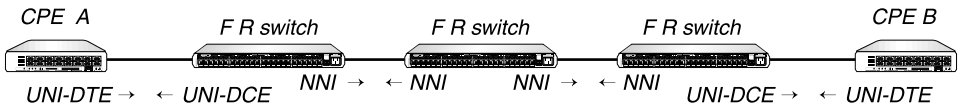
Kinds of physical network interfaces

The MultiVoice Gateway typically uses serial WAN, nailed T1, or nailed E1 to connect to a Frame Relay switch. For details of configuring these interfaces, see Chapter 5, "Configuring the WAN Interfaces."

Kinds of logical interfaces to a Frame Relay switch

Figure 7-2 shows the types of Frame Relay interfaces supported in the MultiVoice Gateway.

Figure 7-2. Types of logical interfaces to Frame Relay switches

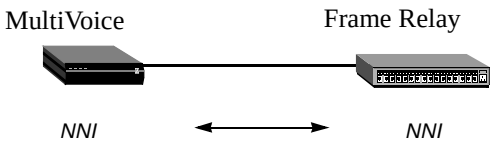


As a Frame Relay concentrator, the MultiVoice Gateway can operate as a Customer Premise Equipment (CPE) device or as a FR switch, or both. In Figure 7-2, all of the elements could be Ascend units, but are not necessarily so.

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

Network to Network Interface (NNI)

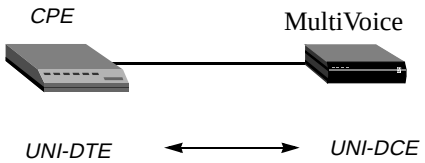
Figure 7-3. Network to Network interface (NNI) in a MultiVoice Gateway unit



An NNI interface connection enables the MultiVoice Gateway to appear as a Frame Relay network interface on the basis of the NNI specifications. The MultiVoice Gateway performs both DTE and DCE link management and allows two separate Frame Relay networks to connect by means of a common protocol. (For more information, see "Configuring an NNI interface" on page 7-6.)

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

Figure 7-4. User to Network Interface-Data Communications Equipment (UNI-DCE)

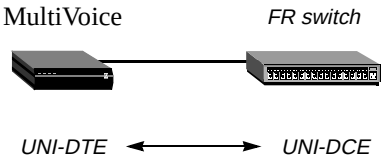


UNI is the interface between an end-user and a network end point (a router or a switch) on the Frame Relay network. In a UNI-DCE connection, the MultiVoice Gateway operates as a Frame Relay router communicating with a DTE device. To the DTE devices, it appears as a Frame Relay network end point. (For more information, see “Configuring a UNI-DCE interface” on page 7-7.)

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

In a UNI-DTE connection, configure the MultiVoice Gateway as a UNI-DTE communicating with a Frame Relay switch. It acts as a Frame Relay *feeder* and performs the DTE functions specified for link management. (For more information, see “Configuring a UNI-DTE interface” on page 7-7.)

Figure 7-5. User to Network Interface - Data Terminal Equipment (UNI-DTE)



Types of Frame Relay connections

For Frame Relay connections, the MultiVoice Gateway supports gateway connections and Frame Relay circuits:

Gateway connections

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

Frame Relay circuits

A Frame Relay *circuit* is a permanent virtual circuit (PVC) segment that consists of two DLCI end points and possibly two Frame Relay profiles. It requires two and only two DLCI numbers. If the circuit has only one DLCI, the MultiVoice Gateway drops the data. If you configure more than two DLCIs, Frame Relay only uses two DLCI numbers. You define a circuit in two

Connection profiles. Data coming in on the DLCI specified in the first Connection profile switches to the DLCI configured in the second one.

Configuring the logical link to a Frame Relay switch

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

```
Ethernet
   Frame Relay
      Name=NNI
      Active=Yes
      Call Type=Nailed
      FR Type=NNI
      Nailed Grp=1
      Data Svc=64k
      PRI # Type=N/A
      Dial #=N/A
      Bill #=N/A
      Call-by-Call=N/A
      Transit #=N/A
      Link Status Dlci=0
      Link Mgmt=Q.933A
      N391=6
      DTE N392=3
      DTE N393=4
      DCE N392=3
      DCE N393=4
      T391=10
      T392=15
      MRU=1532
```

Understanding the Frame Relay parameters

This section provides some background information about the Frame Relay parameters. For more information about each of the parameters, see the *MAX Reference Guide*.

Specifying a profile name and activating the profile

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

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

Bringing down the datalink when DLCIs are not active

The LinkUp parameter (MAX 4000 platforms) specifies whether the data link comes up automatically and stays up even when the last DLCI has been removed. If you set this

parameter to No, the data link does not come up unless a Connection profile (DLCI) brings it up, and it shuts down after the last DLCI has been removed.

Note: You can start and drop Frame Relay data-link connections the DO Dial and DO Hangup commands. DO DIAL brings up a data-link connection. DO Hangup closes the link and any DLCIs on it. If LinkUp=Yes, DO Hangup brings the link down, but it automatically restarts. A restart also occurs if a Connection profile (DLCI) invokes the data link.

Defining the nailed connection to the switch

Nailed is the default for Frame Relay connections. When you define the call type as nailed, dial numbers and other telco options are N/A. You can specify Switched if the Frame Relay switch allows dial-in. However, Frame Relay networks currently have no dial-out connection capability. The two types of data service available are 64K and 56K.

Specifying the type of Frame Relay interface

You can set the FR Type parameter to NNI (for an NNI interface to the switch), DCE (for a UNI-DCE interface), or DTE (for a UNI-DTE interface). For more information, see “Kinds of logical interfaces to a Frame Relay switch” on page 7-2.

Link management protocol

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

Frame Relay timers and event counts

Frame Relay timers and event counts are as follows:

- N391 specifies the interval at which the MultiVoice Gateway requests a Full Status Report (between 1 and 255 seconds). Is N/A if FR Type is DCE.
- DCE N392 specifies the number of errors, during DCE N393 monitored events, that causes the network side to declare the user side procedures inactive. The value should be less than that of DCE N393 (between 1 and 10). DCE N392 is N/A when FR Type is DTE.
- DCE N393 specifies the maximum value for the DCE monitored event count (between 1 and 10). It is N/A when FR Type is DTE.
- DTE N392 specifies the number of errors, during DTE N393 monitored events, that which cause the user side to declare the network side procedures inactive. The value should be less than that of DTE N393 (between 1 and 10). DTE N392 is N/A when FR Type is DCE.
- DTE N393 specifies the maximum value for the DTE monitored event count (between 1 and 10). It is N/A when FR Type is DCE.
- T391 specifies the Link Integrity Verification polling timer (between 5 and 30 seconds). The value should be less than that of T392. T391 is N/A when FR Type is DCE.
- T392 specifies the time for Status Enquiry messages (between 5 and 30 seconds). The MultiVoice Gateway records an error message if it does not receive a Status Enquiry message within T392 seconds. This parameter is N/A when FR Type is DTE.

MRU (Maximum Receive Units)

The MRU parameter specifies the maximum number of bytes the MultiVoice Gateway can receive in a single packet across this link. Usually the default of 1532 is the right setting, unless the far end device requires a lower number.

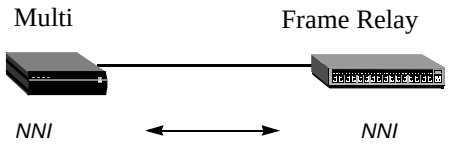
Examples of Frame Relay profile configuration

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

Configuring an NNI interface

In this example, the MultiVoice Gateway has a nailed connection to another Frame Relay switch, and the connection uses an NNI interface configuration. Figure 7-6 shows the connection.

Figure 7-6. Example of NNI connection to another switch



To configure the Frame Relay profile for this NNI interface:

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

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

3. Set the FR Type to NNI:

```
FR Type=NNI
```

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

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

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

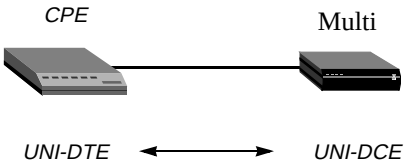
```
Link Mgmt=T1.617D
N391=6
T391=10
T392=15
MRU=1532
```

6. Close the Frame Relay profile.

Configuring a UNI-DCE interface

In this example, the MultiVoice Gateway has a nailed connection to customer premises equipment (CPE), and the connection uses a UNI-DCE configuration, Figure 7-7 shows the connection.

Figure 7-7. Example of UNI-DCE connection to an end-point (DTE)



To configure the Frame Relay profile for this connection:

1 Open a Frame Relay profile.

2 Assign the profile a name and activate it:

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

3 Set the FR Type to DCE:

```
FR Type=DCE
```

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

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

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

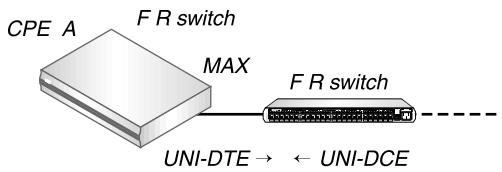
```
Link Mgmt=T1.617D
DCE N392=3
DCE N393=4
T392=15
```

6 Close the Frame Relay profile.

Configuring a UNI-DTE interface

In this example, the MultiVoice Gateway has a nailed connection to a Frame Relay switch configured as a DCE, and the connection uses a UNI-DTE configuration. Figure 7-8 shows the connection.

Figure 7-8. UNI-DTE connection to a Frame Relay switch



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

1 Open a Frame Relay profile.

2 Assign the profile a name and activate it:

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

3 Set the FR Type to DTE:

```
      FR Type=DTE
```

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

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

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

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

6 Close the Frame Relay profile.

Configuring Connection profiles for Frame Relay

All connections that use Frame Relay must specify the name of a configured Frame Relay profile as the data link between the MultiVoice Gateway and the Frame Relay network. Forwarded or routed connections over the Frame Relay link use the parameters shown in the following examples:

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

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

For gateway connections:

```
Ethernet
   Connections
      Encaps=FR
      Encaps options...
         FR Prof=pacbell
         DLCI=16
         Circuit=N/A

      Route IP=Yes

      Ip options...
         LAN Adrs=10.2.3.4/24
```

For Frame Relay circuits:

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

Understanding the Frame Relay connection parameters

This section provides some background information about the Frame Relay connection parameters. For more information about each parameter, see the *MAX Reference Guide*.

Gateway connections (Encaps=FR)

Gateway connections require FR encapsulation, a Frame Relay profile name, and a DLCI. Your Frame Relay provider tells you the DLCI to assign to each connection.

A Connection profile that specifies Frame Relay encapsulation must include a DLCI to identify the first hop of a Permanent Virtual Circuit (PVC). The MultiVoice Gateway does not allow you to enter duplicate DLCIs, except when they are carried by separate physical links specified in different Frame Relay profiles.

Frame Relay circuits (Encaps=FR_CIR)

A circuit is a PVC segment configured in two Connection profiles. Data coming in on the DLCI configured in one Connection profile is switched to the DLCI configured in the other. Data gets dropped if the circuit has only one DLCI. If more than two Connection profiles specify the same circuit name, the MultiVoice Gateway uses only two DLCIs.

In a circuit, both Connection profiles must specify FR_CIR encapsulation and the same circuit name. Each profile must specify a unique DLCI. The MultiVoice Gateway does not allow you to enter duplicate DLCIs, except when separate physical links specified in different Frame Relay profiles carry duplicate DLCIs.

Examples of connection configuration

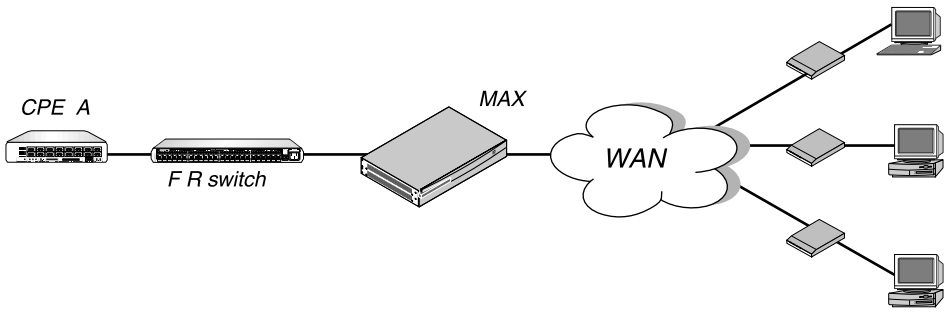
This section shows examples of Connection profile configuration for Frame Relay gateway, circuit, and redirect configurations.

Configuring a Frame Relay gateway connection

This example shows how to configure a Frame Relay gateway connection. It presumes that dial-in users who need to reach the distant IP network have valid Connection profiles (or

RADIUS user profiles). This example shows the Connection profile that assigns a DLCI and passes the data stream out to a Frame Relay switch. Figure 7-9 shows the network.

Figure 7-9. Gateway connections



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

1 Open a Connection profile.

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

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

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

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

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

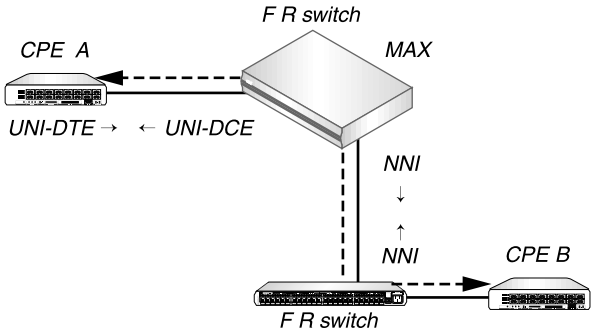
```
      Encaps options...
         FR Prof=ATT-NNI
         DLCI=55
         Circuit=N/A
```

5 Close the Connection profile.

Configuring a Frame Relay circuit

This example shows how to configure a Frame Relay circuit between a UNI-DCE and NNI data links. Configure a circuit between any two interfaces within the MultiVoice Gateway in the same way. Figure 7-10 shows an example of a Frame Relay circuit network:

Figure 7-10. A Frame Relay circuit



In this example, ATT-DCE is the Frame Relay profile for the UNI-DCE interface in the MultiVoice Gateway. ATT-NNI is the Frame Relay profile for the NNI interface. To configure this circuit:

1 Open the first Connection profile.

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

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

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

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

4 Close the Connection profile.

5 Open the second Connection profile.

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

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

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

```
      Encaps options...
         FR Prof=ATT-NNI
```

```
DLCI=23
Circuit=Circuit-1
```

8 Close the second Connection profile.

Monitoring Frame Relay connections

The terminal-server command-line interface includes Show FR commands for monitoring Frame Relay in the MultiVoice Gateway. To display the options, invoke the terminal-server interface (System > Sys Diag > Term Serv) and then enter the Show FR command with the ? option. For example:

```
ascend% show fr ?

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

Displaying Frame Relay statistics

To display Frame Relay statistics, enter the Show FR command with the `stats` option. For example:

```
ascend% show fr stats

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

The output includes the following fields:

Field	Description
Name	Name of the Frame Relay profile associated with the interface.
Type	Type of interface.
Status	Status of the interface. Up means the interface is functional, but is not necessarily handling an active call. Down means the interface is not functional.
Speed	Data rate in bits per second.
MTU	Maximum packet size allowed on the interface.
InFrame	Number of frames the interface has received.
OutFrame	Number of frames transmitted.

Displaying link management information

To display Link Management Information (LMI) for each link activated by a Frame Relay profile, use the `lmi` option. For example:

```
ascend% show fr lmi

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

LMI is not on for fr1-temp

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

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

Displaying DLCI status

To display the status of each DLCI, use the `dlci` option. For example:

```
ascend% show fr dlci

DLCIs for fr1

DLCIs for fr1-temp

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

DLCIs for fr1-temp-9

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

DLCIs not assigned
```

The MultiVoice Gateway reports DLCI information using these fields:

Field	Description
`DLCI`	DLCI number.
`Status`	ACTIVE if the connection is up or INACTIVE if not.
`input pkts`	Number of frames the interface has received.
`output pkts`	Number of frames the interface has transmitted.

Field	Description
`input octets`	Number of bytes the interface has received.
`output octets`	Number of bytes the interface has transmitted.
`in FECN pkts`	Number of packets received with the FECN (Forward Explicit Congestion Notification) bit set. This field always contains a 0 (zero), because congestion management is not currently supported.
`in BECN pkts`	Number of packets received with the BECN (Backward Explicit Congestion Notification) bit set. This field always contains a 0 (zero), because congestion management is not currently supported.
`in DE pkts`	Number of packets received with the DE (Discard Eligibility) indicator bit set.
`last time status changed`	Time at which the DLCI state last changed.

Displaying circuit information

Entering the Show FR command with the `circuits` option shows the Frame Relay profile name, the DLCI, and the status of configured circuits. For example:

```
ascend% show fr circuits

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

Turning off a circuit without disabling its endpoints

The Set Circuit command enables you to turn off traffic going through a Frame Relay circuit without disabling the circuit end points. This command prevents traffic from going between end points, but does not disrupt the state of the DLCI. To display the support options, use the ? option:

```
ascend% set circuit ?

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

To allow data to flow through a circuit, use the Active option. For example:

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

- To turn off data flow without disrupting the state of the DLCIs, use the inactive option. For example:

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

Configuring IP Routing

8

Introduction to IP routing and interfaces

The first task described in this chapter, setting up the IP network, involve setting parameters in the MultiVoice Gateway for the MAX Ethernet profile. The parameters define the unit's Ethernet IP interface, network services (such as DNS), and routing policies.

For configuring IP routes and preferences and configuring the MultiVoice Gateway for dynamic route updates, you configure the Static Routes profile to set up the IP routing table, which determines the paths over which IP packets are forwarded.

To perform the tasks described in this chapter, you have to understand how the MultiVoice Gateway uses IP addresses and subnet masks, IP routes, and IP interfaces.

IP addresses and subnet masks

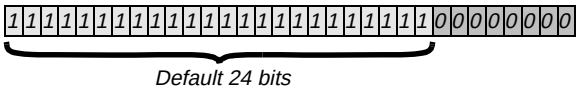
In the MultiVoice Gateway, you specify IP addresses in dotted decimal format. If you specify no subnet mask, the MultiVoice Gateway assumes that the address contains the default number of network bits for its class. In other words, in Table 8-1, the number of network bits for each class corresponds to the default subnet mask for that class.

Table 8-1. IP address classes and number of network bits

Class	Address range	Network bits
Class A	0.0.0.0 — 127.255.255.255	8
Class B	128.0.0.0 — 191.255.255.255	16
Class C	192.0.0.0 — 223.255.255.255	24

For example, a class C address such as 198.5.248.40 has 24 network bits, so its default mask is *24*. The 24 network bits leave 8 bits for the host portion of the address. So one class C network can support up to 253 hosts.

Figure 8-1. A class C IP address



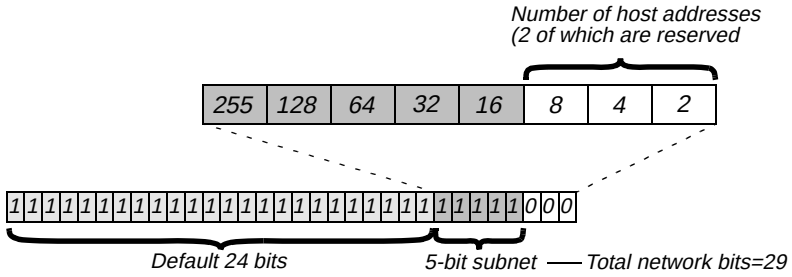
As shown in Table 8-1, a mask has a binary 1 in each masked position. Therefore, the default, 24-bit, subnet mask for a class C address can be represented in dotted decimal notation as 255.255.255.0.

For specifying a different subnet mask, the MultiVoice Gateway supports a modifier that specifies the total number of network bits in the address. For example:

```
IP address = 198.5.248.40
Mask = 255.255.255.248
```

In this example, the mask specification indicates that 29 bits of the address specify the network. This is commonly referred to as a 29-bit subnet. The three remaining bits specify unique hosts.

Figure 8-2. A 29-bit subnet mask and number of supported hosts



Three available bits allow eight possible bit combinations. Of the eight possible host addresses, two are reserved, as follows:

000 — Reserved for the network (base address)
001
010
100
110
101
011
111 — Reserved for the broadcast address of the subnet

Ascend notation

When you display a MultiVoice Gateway routing table, entry, the subnet mask follows the IP address, and a slash separates the two values. For example, if the address 198.5.248.40 has a 29-bit mask, it appears in the routing table as 198.5.248.40/29.

Zero subnets

Early implementations of TCP/IP did not allow zero subnets. That is, subnets could have the same base address that a class A, B, or C network would have. For example, the subnet 192.168.8.0/30 was illegal because it had the same base address as the class C network 192.168.8.0/24, while 192.168.8.4/30 was legal (192.168.8.0/30 is called a zero subnet, because like a class C base address, its last octet is zero). Modern implementations of TCP/IP allow subnets to have base addresses that might be identical to the class A, B, or C base addresses. Ascend's implementations of RIP 2 and OSPF treat these so-called zero subnetworks the same as any other network. You should decide whether or not to support and configure zero subnetworks for your environment. If you configure them in some cases and treat them as unsupported in other cases, you will encounter routing problems.

Table 8-2 shows how the standard subnet address format relates to Ascend notation for a class C network number.

Table 8-2. Standard subnet masks

Subnet mask	Ascend notation	Number of host addresses
255.255.255.0	/24	254 hosts + 1 broadcast, 1 network (base)
255.255.255.128	/25	126 hosts + 1 broadcast, 1 network (base)
255.255.255.192	/26	62 hosts + 1 broadcast, 1 network (base)
255.255.255.224	/27	30 hosts + 1 broadcast, 1 network (base)
255.255.255.240	/28	14 hosts + 1 broadcast, 1 network (base)
255.255.255.248	/29	6 hosts + 1 broadcast, 1 network (base)
255.255.255.252	/30	2 hosts + 1 broadcast, 1 network (base)
255.255.255.254	/31	invalid netmask (no hosts)
255.255.255.255	/32	1 host — a host route

The broadcast address of any subnet has the host portion of the IP address set to all ones. The network address (or base address) represents the network itself, with the host portion of the IP address set to all zeros. Therefore, these two addresses define the address range of the subnet. For example, if the MultiVoice Gateway configuration assigns the following address to a remote router:

```
IP address = 198.5.248.120
Mask = 255.255.255.248
```

The Ethernet attached to that router has the following address range:

```
198.5.248.120 – 198.5.248.127
```

A host route is a special case IP address with a subnet mask of 32 bits. It has a subnet mask of 255.255.255.255.

IP routes

At system start-up, the MultiVoice Gateway builds an IP routing table that contains configured routes. When the system is up, it can use routing protocols such as RIP or OSPF to learn additional routes dynamically.

In each routing table entry, the Destination field specifies a destination network address that may appear in IP packets, and the Gateway field specifies the address of the next-hop router to reach that destination.

How the MultiVoice Gateway uses the routing table

The MultiVoice Gateway relies on the routing table to forward IP packets, as follows:

- If the MultiVoice Gateway finds a routing table entry whose Destination field matches the destination address in a packet, it routes the packet to the specified next-hop router, through its Ethernet interface.
- If the MultiVoice Gateway does not find a matching entry, it looks for the Default route, which is identified in the routing table by a destination of 0.0.0.0. If that route has a specified next-hop router, it forwards the packet to that router.
- If the MultiVoice Gateway does not find a matching entry and does not have a valid Default route, it drops the packet.

Static and dynamic routes

A static route is a manually configured path from one network to another. It specifies the destination network and the gateway (router) to use to get to that network. If a path to a destination must be reliable, the administrator often configures more than one static route to the destination. In that case, the MultiVoice Gateway chooses the route on the basis of assigned metrics and availability. Each static route has its own Static Rtes profile.

The Ethernet > Mod Config profile specifies a static connected route, which states “to reach system A, send packets out this interface to system A.”

A dynamic route is a path, to another network, that is learned from another IP router rather than configured in one of the MultiVoice Gateway unit’s local profiles. Routers that use RIP broadcast their entire routing table every 30 seconds, updating other routers about the usability of particular routes. Hosts that run ICMP can also send ICMP Redirects to offer a better path to a destination network. OSPF routers propagate link-state changes as they occur. Routing protocols such as RIP and OSPF all use some mechanism to propagate routing information and changes through the routing environment.

Route preferences and metrics

The MultiVoice Gateway supports route preferences, because different protocols have different criteria for assigning route metrics. For example, RIP is a distance-vector protocol, which uses a virtual hop count to select the shortest route to a destination network. OSPF is a link-state protocol, which means that OSPF can take into account a variety of link conditions, such as the reliability or speed of the link, when determining the best path to a destination network.

When choosing a route to put into the routing table, the router first compares preference values, preferring the lowest number. If the preference values are equal, the router compares

the metric fields and uses the route with the lowest metric. Following are the preference values for the various types of routes:

Route	Default Preference
OSPF	10
ICMP redirects	30
RIP	100
Static	100
ATMP, PPTP	100

MultiVoice Gateway Ethernet interface

The following example shows the routing table for a MultiVoice Gateway configured to enable IP routing:

```
** Ascend MultiVoice Gateway Terminal Server **

ascend% iproute show
Destination        Gateway   IF       Flg   Pref   Met     Use     Age
10.10.0.0/16       -         ie0      C        0     0       3     222
10.10.10.2/32      -         local    CP       0     0       0     222
127.0.0.0/8        -         bh0      CP       0     0       0     222
127.0.0.1/32       -         local    CP       0     0       0     222
127.0.0.2/32       -         rj0      CP       0     0       0     222
224.0.0.0/4        -         mcast    CP       0     0       0     222
224.0.0.1/32       -         local    CP       0     0       0     222
224.0.0.2/32       -         local    CP       0     0       0     222
224.0.0.5/32       -         local    CP       0     0       0     222
224.0.0.6/32       -         local    CP       0     0       0     222
224.0.0.9/32       -         local    CP       0     0       0     222
255.255.255.255/32 -         ie0      CP       0     0       0     222
```

The Ethernet interface has the IP address 10.10.10.2 (with a subnet mask of 255.255.0.0). No Connection profiles or static routes are configured.

The MultiVoice Gateway creates the following interfaces at start-up:

Interface	Description
Ethernet IP	Always active, because it is always connected. Its IP address is assigned in Ethernet > Mod Config > Ether Options. The MultiVoice Gateway creates two routing table entries: one with a destination of the network (`ie0`), and the other with a destination of the MultiVoice Gateway (`local`).
Black-hole (`bh0`)	Always up. The black-hole address is 127.0.0.3. Packets routed to this interface are discarded silently.
Loopback (`local`)	Always up. The loopback address is 127.0.0.1/32.
Reject (`rj0`)	Always up. The reject address is 127.0.0.2. Packets routed to this interface are sent back to the source address with an ICMP *host unreachable* message.

Interface	Description
Multi-cast	Have a destination address with a value of 224 for the first octet. The MultiVoice Gateway does not support Multi-casting, and the MultiVoice Gateway ignores Multi-cast entries in its routing table.

Configuring the local IP network setup

The Ethernet profile contains system-global parameters that affect all IP interfaces in the MultiVoice Gateway. The following example shows the related parameters:

```
Ethernet
   Mod Config
      Ether options…
         IP Adrs=10.2.3.1/24
         2nd Adrs=0.0.0.0/0
         RIP=Off
         Ignore Def Rt=Yes
         Proxy Mode=Off

      Shared Prof=No
      Telnet PW=Ascend

      BOOTP Relay...
         BOOTP Relay Enable=No
         Server=N/A
         Server=N/A

      DNS...
         Domain Name=abc.com
         Sec Domain Name=
         Pri DNS=10.65.212.10
         Sec DNS=12.20 7.23.51
         Allow As Client DNS=Yes
         Pri WINS=0.0.0.0
         Sec WINS=0.0.0.0
         List Attempt=No
         List Size=N/A
         Client Pri DNS=0.0.0.0
         Client Sec DNS=0.0.0.0

      SNTP Server...
         SNTP Enabled=Yes
         Time zone-UTC+0000
         SNTP host#1=0.0.0.0
         SNTP host#2=0.0.0.0
         SNTP host#3=0.0.0.0

      UDP Cksum=No
      Adv Dialout Routes=Always
```

Understanding the IP network parameters

This section provides some background information about the IP network configuration. The information is organized by functionality rather than by parameter. For more information about each parameter, see the *MAX Reference Guide*.

Primary IP address for the Ethernet interface

The IP Address parameter specifies the MultiVoice Gateway unit's IP address for the local Ethernet interface. When specifying IP addresses for the MultiVoice Gateway's Ethernet interfaces, you must specify the subnet mask. IP address and subnet mask are required settings for the MultiVoice Gateway to operate as an IP router.

Second IP address for the Ethernet interface

The MultiVoice Gateway can assign two unique IP addresses to the physical Ethernet port and route between them. This feature, referred to as *dual IP*, can give the MultiVoice Gateway a logical interface on each of two networks or subnets on the same backbone.

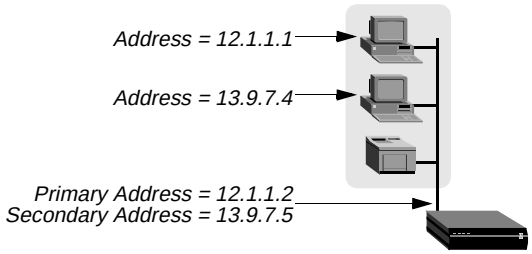
Usually, devices connected to the same physical wire all belong to the same IP network. With dual IP, a single wire can support two separate IP networks, with devices on the wire assigned to one network or the other and communicating by routing through the MultiVoice Gateway.

Dual IP is also used to distribute the load of routing traffic to a large subnet, by assigning IP addresses on that subnet to two or more routers on the backbone. When the routers have a direct connection to the subnet as well as to the backbone network, they route packets to the subnet and include the route in their routing table updates.

Dual IP also enables you to make a smooth transition when changing IP addresses. That is, a second IP address can act as a place holder while you are making the transition in other network equipment.

Figure 8-3 shows an example of an IP network to connected a MultiVoice Gateway.

Figure 8-3. Sample IP network



Two IP addresses, 12.1.1.2 and 13.9.7.5, are assigned to the MultiVoice Gateway's Ethernet interface. The MultiVoice Gateway routes between both networks. The MultiVoice Gateway enables the host assigned 12.1.1.1 to communicate with the host assigned 13.9.7.4.

The host assigned 12.1.1.1 and the host assigned 13.9.7.4 share a physical cable segment, but cannot communicate unless the MultiVoice Gateway routes between the 12.0.0.0 network and the 13.0.0.0 network.

Enabling RIP on the Ethernet interface

You can configure the IP interface to send RIP updates (inform other local routers of its routes), receive RIP updates (learn about networks that can be reached through other routers on the Ethernet), or both.

Note: Ascend recommends that you run RIP version 2 (RIP-v2) if possible. You should not run RIP-v2 and RIP-v1 on the same network in such a way that the routers receive each other's advertisements. RIP-v1 does not propagate subnet mask information, and the default-class network mask is assumed, while RIP-v2 handles subnet masks explicitly. Running the two versions on the same network can result in RIP-v1 class subnet mask assumptions overriding accurate subnet information obtained via RIP-v2.

Ignoring the default route

You can configure the MultiVoice Gateway to ignore default routes advertised by routing protocols. This configuration is recommended, because you typically do not want the default route changed by a RIP update. The default route specifies a static route to another IP router, which is often a local router such as an Ascend GRF400 or other kind of LAN router. When the MultiVoice Gateway is configured to ignore the default route, RIP updates do not modify the default route in the MultiVoice Gateway routing table.

Proxy ARP and inverse ARP

The MultiVoice Gateway can be configured to respond to ARP requests for remote devices that have dynamically assigned addresses. It responds to the ARP request with its own MAC address while bringing up the connection to the remote device. This feature is referred to as Proxy ARP.

The MultiVoice Gateway also supports Inverse Address Resolution Protocol (Inverse ARP). Inverse ARP allows the MultiVoice Gateway to resolve the protocol address of another device when the hardware address is known. The MultiVoice Gateway does not issue any Inverse ARP requests, but it does respond to Inverse ARP requests that have the protocol type of IP (8000 hexadecimal), or in which the hardware address type is the two-byte Q.922 address (Frame Relay). All other types are discarded. The Inverse ARP response packet sent by the MultiVoice Gateway includes the following information:

- ARP source-protocol address (the MultiVoice Gateway unit's IP address on Ethernet)
- ARP source-hardware address (the Q.922 address of the local DLCI)

(For the details of Inverse ARP, see RFCs 1293 and 1490.)

Telnet password

The Telnet password is required from all users attempting to access the MultiVoice Gateway unit by Telnet. Users are allowed three tries to enter the correct password, after which the connection attempt fails.

BOOTP Relay

By default, a MultiVoice Gateway does not relay BOOTP (Bootstrap Protocol) requests to other networks. It can do so if BOOTP is enabled, but SLIP BOOTP must be disabled in

Ethernet > Mod Config > TServ Options. SLIP BOOTP makes it possible for a computer connecting to the MultiVoice Gateway over a SLIP connection to use the Bootstrap Protocol. A MultiVoice Gateway can support BOOTP on only one connection. If both SLIP BOOTP and BOOTP relay are enabled, you will receive an error message.

You can specify the IP address of one or two BOOTP servers, but you are not required to specify a second BOOTP server.

If you specify two BOOTP servers, the MultiVoice Gateway that relays the BOOTP request determines when each server is used. The order of the BOOTP servers in the BOOTP Relay menu does not necessarily determine which server is tried first.

Local domain name

The Domain Name is used for DNS lookups. When the MultiVoice Gateway is given a host name to look up, it tries various combinations, including the appending of the configured domain name to the host name. The secondary domain name (Sec Domain Name) can specify another domain that the MultiVoice Gateway can search. The MultiVoice Gateway searches the secondary domain only after the domain specified by the Domain Name parameter.

DNS or WINS name servers

When the MultiVoice Gateway is informed about DNS (or WINS), Telnet and Rlogin users can specify host names instead of IP addresses. If you configure a primary and secondary name server, the secondary server is accessed only if the primary one is inaccessible.

DNS lists

DNS can return multiple addresses for a hostname in response to a DNS query, but it does not include information about availability of those hosts. Users typically attempt to access the first address in the list. If that host is unavailable, the user must try the next host, and so forth. However, if the access attempt occurs automatically as part of immediate services, the physical connection is torn down when the initial connection fails. To avoid tearing down physical links when a host is unavailable, you can set the List Attempt parameter to Yes. The List Size parameter specifies the maximum number of hosts listed (up to 35).

SNTP service

The MultiVoice Gateway can use Simple Network Time Protocol (SNTP)—RFC 1305 to set and maintain its system time by communicating with an SNTP server. SNTP must be enabled for the MultiVoice Gateway to communicate by means of that protocol. In addition, you must specify your time zone as an offset from the Universal Time Coordination (UTC). UTC is in the same time zone as Greenwich Mean Time (GMT). Specify the offset in hours, using a 24-hour clock. Because some time zones, such as Newfoundland, do not have an even hour boundary, the offset includes four digits and is stated in half-hour increments. For example, in Newfoundland the time is 1.5 hours ahead of UTC, which is represented as follows:

```
UTC +0130
```

For San Francisco, which is 8 hours ahead of UTC, the time would be:

```
UTC +0800
```

For Frankfurt, which is 1 hour behind UTC, the time would be:

```
UTC -0100
```

Specifying SNTP server addresses

The Host parameter lets you specify up to three server addresses. The MultiVoice Gateway attempts to communicate with the first address. It attempts the second only if the first is inaccessible, and the third only if the second is inaccessible.

UDP checksums

If data integrity is of the highest concern for your network, and having redundant checks is important, you can turn on UDP checksums to generate a checksum whenever a UDP packet is transmitted. UDP packets are transmitted for queries and responses related to ATMP, SYSLOG, DNS, ECHOSERV, RADIUS, TACACS, RIP, SNTP, and TFTP.

Setting UDP checksums to Yes could cause a slight decrease in performance, but in most environments the decrease is not noticeable.

Poisoning dialout routes in a redundant configuration

If you have another Ascend unit backing up the MultiVoice Gateway in a redundant configuration on the same network, you can use the Adv Dialout Routes parameter to instruct the MultiVoice Gateway to stop advertising IP routes that use dial services if its trunks experience an alarm condition. If you do not set the parameter, the MultiVoice Gateway continues to advertise its dialout routes, which prevents the redundant unit from taking over the routing responsibility.

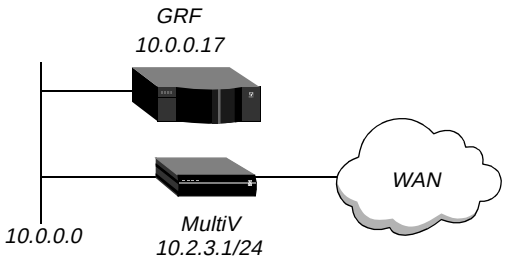
Examples of IP network configuration

This section shows some examples of Ethernet profile IP configuration.

Configuring the MultiVoice Gateway IP interface on a subnet

On a large corporate backbone, many sites configure subnets to increase the network address space, segment a complex network, and control routing in the local environment. For example, Figure 8-4 shows the main backbone IP network (10.0.0.0) supporting an Ascend GRF router (10.0.0.17).

Figure 8-4. Creating a subnet for the MultiVoice Gateway



You can place the MultiVoice Gateway on a subnet of that network by entering a subnet mask in its IP address specification. For example:

1 Open Ethernet > Mod Config > Ether Options.

2 Specify the IP subnet address for the MultiVoice Gateway on Ethernet. For example:

```
Ethernet
   Mod Config
      Ether options…
         IP Adrs=10.2.3.1/24
```

3 Configure the MultiVoice Gateway to receive RIP updates from the local GRF router:

```
      RIP=Recv=v2
```

4 Close the Ethernet profile.

With this subnet address, the MultiVoice Gateway requires a static route to the backbone router on the main network. Otherwise, it can only communicate with devices on the subnets to which it is directly connected. To create the static route and make the backbone router the default route:

1 Open the Default IP Route profile.

2 Specify the IP address of a backbone router in the Gateway parameter. For example:

```
Ethernet
   Static Rtes
      Name=Default
      Active=Yes
      Dest=0.0.0.0/0
      Gateway=10.0.0.17
      Preference=100
      Metric=1
      DownPreference=140
      DownMetric=7
      Private=Yes
```

3 Close the Default IP Route profile.

For more information about IP Route profiles, see “Configuring IP routes and preferences” on page 8-16. To verify that the MultiVoice Gateway is up on the local network, invoke the terminal-server interface and Ping a local IP address or hostname. For example:

```
ascend% ping 10.1.2.3
```

You can terminate the Ping exchange at any time by pressing Ctrl-C.

Configuring DNS

The DNS configuration enables the MultiVoice Gateway to use local DNS or WINS servers for lookups. In this example of a DNS configuration, client DNS is not in use. To configure the local DNS service:

1 Open Ethernet > Mod Config > DNS.

2 Specify the local domain name.

3 If appropriate, specify a secondary domain name.

4 Specify the IP addresses of a primary and secondary DNS server, and turn on the DNS list attempt feature:

```
Ethernet
   Mod Config
      DNS...
         Domain Name=abc.com
         Sec Domain Name=
         Pri DNS=10.65.212.10
         Sec DNS=12.20 7.23.51
         Allow As Client DNS=Yes
         Pri WINS=0.0.0.0
         Sec WINS=0.0.0.0
         List Attempt=Yes
         List Size=35
         Client Pri DNS=0.0.0.0
         Client Sec DNS=0.0.0.0
         Enable Local DNS Table=No
         Loc.DNSTab Auto Update=No
```

5 Close the Ethernet profile.

You can create a local DNS table to provide a list of IP addresses for a specific host name when the remote DNS server fails to resolve the host name. If the local DNS table contains the host name for the attempted connection, it provides the list of IP addresses.

You create the DNS table from the terminal server by entering the hostnames and their IP addresses. A table can contain up to eight entries, with a maximum of 35 IP addresses for each entry. If you specify automatic updating, you only have to enter the first IP address of each host. Any others are added automatically.

Automatic updating replaces the existing address list for a host each time the remote DNS server succeeds in resolving a connection to a host that is in the table. You specify how many of the addresses returned by the remote server can be included in the new list.

On the MultiVoice Gateway, the table provides additional information for each table entry. The information is in the following two fields, which are updated when the system matches the table entry with a hostname that was not found by the remote server:

- # Reads—the number of reads since entry was created. This field is updated each time a local name query match is found in the local DNS table.
- Time of Last Read

You can check the list of host names and IP addresses in the table by entering the terminal-server command Show Dnstab. Figure 8-5 shows an example of a DNS table on a MultiVoice Gateway. Other terminal-server commands show individual entries, with a list of IP addresses for the entry.

Figure 8-5. Example of a local DNS table

```
Local DNS Table
Name                     IP Address      # Reads Time of last read
_____________________ _______________ _______ ___________________
1: ""                    ------          ------
2: "server.corp.com."    200.0.0.0       2       Feb 10 10:40:44
3: "boomerang"           221.0.0.0       2       Feb 10  9:13:33
4: ""                    ------          -------
5: ""                    ------          -------
6  ""                    ------          -------
7: ""                    ------          -------
```

Additional terminal-server commands

The terminal-server interface includes Show and DNStab commands to help you view, edit, and make entries to the DNS table.

Show commands

- show ? displays a list that includes dnstab help.
- show dnstab displays the local DNS table.
- show dnstab ? displays help for the dnstab editor.
- show dnstab entry displays the local DNS table entry (all IP addresses in the list).

DNStab commands

The terminal server dnstab command has the following variations:

DNStab Command	Description
dnstab	Displays help information about the DNS table.
dnstab show	Displays the local DNS table.
dnstab entry *N*	Displays a list for entry *n* in the local DNS table. The list displayed includes the entry and all the IP addresses stored for that entry up to a maximum number of entries specified in the List Size parameter. If List Attempt=No, no list is displayed.
dnstab edit	Start editor for the local DNS table.

Configuring the local DNS table

To enable and configure the local DNS table:

1. Open the Ethernet > Mod Config > DNS menu.
2. Select a setting for the List Attempt parameter.
3. Specify the list size by setting the List Size parameter.
4. Select Enable Local DNS Table=Yes.
   The default is No.
5. Select a setting for the Loc.DNS Tab Auto Update parameter.

Criteria for valid names in the local DNS table

Each name in the local DNS table:

- Must be unique in the table.
- Must start with an alphabetic character, which may be either uppercase or lowercase.
- Must be less than 256 characters
- Can be a local name or a fully qualified name that includes the domain name.

Periods at the ends of names are ignored.

Entering IP addresses in the local DNS table

To enter IP addresses in a local DNS table, you use the DNS table editor from the terminal server. While the editor is in use, the system cannot look up addresses in the table or perform automatic updates. A table *entry* is one of the eight table indexes. It includes the host name, IP address (or addresses), and information fields. To place the initial entries in the table:

1. At the terminal-server interface, type **`dnstab edit`**.

   Before you make any entries, the table is empty. The editor initially displays zeros for each of the eight entries in the table. To exit the table editor without making an entry, press Enter.

2. Type an entry number and press Enter.

   A warning appears if you type an invalid entry number. If the entry exists, the current name for that entry appears in the prompt.

3. Type the name for the current entry.

   If the system accepts the name, it places the name in the table and prompts you for the IP address for the name that you just entered. (For the characteristics of a valid name, see “Criteria for valid names in the local DNS table” on page 8-14.)

   If you enter an invalid name, the system prompts you to enter a valid name.

4. Type the IP address for the entry.

   If you enter an address in the wrong format, the system prompts you for the correct format. If your format is correct, the system places the address in the table and the editor prompts you for the next entry.

5. When you are finished making entries, type the letter **`0`** and press Enter when the editor prompts you for another entry.

Editing the local DNS table

To edit the DNS table entries, you access the DNS table editor from the terminal server. While the editor is in use, the system cannot look up addresses in the table or perform automatic updates. A table *entry* is one of the eight table indexes. It includes the host name, IP address (or addresses), and information fields. To edit one or more entries in the local DNS table:

1 At the terminal-server interface, type **`dnstab edit`**.

If the table has already been created, the number of the entry last edited appears in the prompt.

2 Type an entry number, or press Enter to edit the entry number currently displayed.

A warning appears if you type an invalid entry number. If the entry exists, the current value for that entry appears in the prompt.

3 Replace, accept, or clear the displayed name, as follows:

- To replace the name, type a new name and press Enter.
- To accept the current name, press Enter.
- To clear the name, press the spacebar and then Enter.

If you enter a valid name, the system places it in the table (or leaves it there if you accepted the current name) and prompts you for the corresponding IP address. (For the characteristics of a valid name, see "Criteria for valid names in the local DNS table" on page 8-14)

If you clear an entry name, all information in all fields for that entry is discarded.

4 Either type a new IP address and press Enter, or leave the current address and just press Enter.

- To change the IP address, type the new IP address
- If you are changing the name of the entry but not the IP address, just press Enter.

If the address is in the correct format, the system places it in the table and prompts you for another entry.

5 When you are finished making entries, type the letter **`0`** and press Enter when the editor prompts you for another entry.

Deleting an entry from the local DNS table

To delete an entry from the local DNS table:

1 At the terminal server interface, type **`dnstab edit`** to display the table.

2 Type the number of the entry you want to delete, and press Enter.

3 Press the spacebar, then press Enter.

Configuring IP routes and preferences

The IP routing table contains routes that are configured (static routes) and routes that are learned dynamically from routing protocols such as RIP or OSPF. The following example shows the parameters for configuring static routes:

```
Ethernet
   Static Rtes
      Name=route-name
      Active=Yes
      Dest=10.2.3.0/24
      Gateway=10.2.3.4
      Metric=2
      Preference=100
      Private=No
      Ospf=Cost=1
      ASE-type=Type1
      ASE=tag=c0000000

Ethernet
   Mod Config
      Ether options…
         IP Adrs=10.2.3.1/24
         2nd Adrs=0.0.0.0/0
         RIP=Off

      Route Pref…
         Static Preference=100
         Rip Preference-100
         RipAseType-Type2
         Rip Tag=c8000000
         OSPF Preference=10
         OSPF ASE Preference=150
```

Understanding the static route parameters

This section provides some background information about static routes. For more information about each parameter, see the *MAX Reference Guide.*

Route names

IP routes are indexed by name. You can assign any name of less than 31 characters.

Activating a route

A route must be active to affect packet routing. If Active = No, the route is ignored.

Route's destination address

The destination address of a route is the target network (the destination address in a packet). Packets destined for that host will use this static route to bring up the right connection. The zero address (0.0.0.0) represents the default route (the destination to which packets are forwarded when there is no route to the packet's destination).

Route's gateway address

The Gateway parameter specifies the IP address of the router or interface through which to reach the target network.

Metrics, costs, and preferences

The Metric parameter specifies the hop count (a number of from 1 to 15) for this route. Hop count refers to the number of routers that have to be crossed to reach the destination. For example, reaching a destination with a hop count of 10 requires (theoretically) crossing 10 routers. A route with a shorter hop count to a destination is more desirable than one with a larger hop count, since it most likely is a shorter, faster route.

You can configure the Metric parameter as *virtual* hop count. To define which routes are more desirable, regardless of the actual number of routers the route crosses. The higher the metric, the less likely is the MultiVoice Gateway to use the route.

The Cost parameter specifies the cost of an OSPF link. Cost is a configurable metric that can take into account the speed of the link and other issues. The lower the cost, the more likely is the interface to be used to forward data traffic. (For details, see Chapter 9, "Configuring OSPF Routing.")

The Preference parameter specifies a route preference. Zero is the default for connected routes (such as the Ethernet). When choosing which route to use, the router first compares the preference values, preferring the lowest number. If the preference values are equal, the router compares the metric values, and uses the route with the lowest metric. The value of 255 means "Do not use this route." (For details, see "Route preferences and metrics" on page 8-4.)

Tagging routes learned from RIP

The Rip-Tag field is *attached* to all routes learned from RIP in OSPF updates. The tag is a hexadecimal number that can be used by border routers to filter the record.

Type-1 or type-2 metrics for routes learned from RIP

The Rip Ase Type parameter can be set to Type-1 or Type-2. Type-1 is a metric expressed in the same units as the link-state metric (the same units as interface cost). Type-2 is considered larger than any link-state path. It assumes that routing between autonomous systems is the major cost of routing a packet, and eliminates the need for conversion of external costs to internal link-state metrics.

Making a route private

Private routes are used internally but are not advertised.

Note: Typically, default routes should not be advertised to other routers. They are designed for the internal use of the specific router on which they are configured.

A connected route for the Ethernet IP interface

The IP Adrs parameter specifies the MultiVoice Gateway unit's IP address on the local Ethernet. The MultiVoice Gateway creates a route for this address at system startup.

Static route preferences

By default, static routes and RIP routes have the same preference, so they compete equally. ICMP redirects take precedence over both, and OSPF take precedence over everything. If a dynamic route's preference is lower than that of the static route, the dynamic route can overwrite (hide) a static route to the same network. In the IP routing table, the hidden static route has an *h* flag, indicating that it is inactive. The active, dynamically learned route is also in the routing table. However, dynamic routes age and, if no updates are received, eventually expire. In that case, the hidden static route reappears in the routing table.

RIP and OSPF preferences

Because OSPF typically involves a complex environment, its router configuration is described in Chapter 9, "Configuring OSPF Routing."

Tagging routes learned from RIP

The RIP Tag field is *attached* to all routes learned from RIP in OSPF updates. The tag is a hexadecimal number that can be used by border routers to filter the record.

Metrics for routes learned from RIP

The RipAseType parameter can specify Type-1 or Type-2. Type-1 is a metric expressed in the same units as the link-state metric (the same units as interface cost). Type-2 is considered larger than any link-state path. It assumes that routing between autonomous systems is the major cost of routing a packet, and it eliminates the need for conversion of external costs to internal link-state metrics.

Examples of static route configuration

The section provides information about configuring the IP default route and configuring a static route to a remote subnet. For an example of the Ethernet profile configuration of the MultiVoice Gateway unit's local IP interface, see "Configuring the MultiVoice Gateway IP interface on a subnet" on page 8-10.

Configuring the default route

If no routes exist for the destination address of a packet, the MultiVoice Gateway forwards the packet to the default route. Most sites use the default route to specify a local IP router (such as a Cisco router or a UNIX host running the route daemon) to off-load routing tasks to other devices.

Note: If the MultiVoice Gateway does not have a default route, it drops packets for which it has no route.

1 Open the first IP Route profile (the route named Default) and activate it:

```
Ethernet
   Static Rtes
      Name=Default
```

```
Active=Yes
Dest=0.0.0.0/0
```

Note: The name of the first IP Route profile is always Default, and its destination is always 0.0.0.0 (you cannot change these values).

2 Specify the router to use for packets with unknown destinations. For example:

```
Gateway=10.9.8.10
```

3 Specify a metric for this route, the route's preference, and whether the route is private. For example:

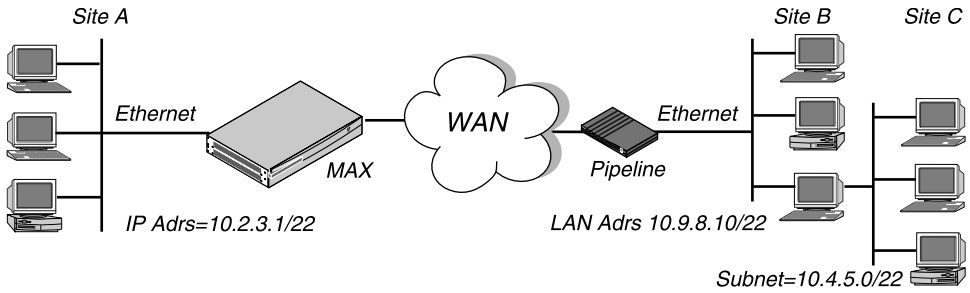
```
Metric=1
Preference=100
Private=Yes
```

4 Close the IP Route profile.

Defining a static route to a remote subnet

If the connection does not enable RIP, the MultiVoice Gateway does not learn about other networks or subnets that might be reachable through the remote device, such as the remote network shown in Figure 8-6.

Figure 8-6. Two-hop connection that requires a static route when RIP is off



To enable the MultiVoice Gateway to route to site C without using RIP, you must configure an IP Route profile similar to the following example:

```
Ethernet
   Static Rtes
      Name=SITEBGW
      Active=Yes
      Dest=10.4.5.0/22
      Gateway=10.9.8.10
      Metric=2
      Preference=100
      Private=Yes
      Ospf=Cost=1
      ASE-type=Type1
      ASE=tag=c0000000
```

Example of route preferences configuration

The following example increases the preference value of RIP routes, instructing the router to use a static route first if one exists.

1 Open Ethernet > Mod Config > Route Pref.

2 Set Rip Preference to 150:

```
Ethernet
   Mod Config
      Route Pref…
         Rip Preference=150
```

3 Close the Ethernet profile.

Configuring the MultiVoice Gateway for dynamic route updates

The Ethernet interface can be configured to send or receive RIP updates, send or receive OSPF updates, and accept or ignore ICMP redirects. All of these routing mechanisms modify the IP routing table dynamically.

The following example shows the parameters that enable the MultiVoice Gateway to receive updates from RIP or ICMP. (For information about OSPF updates, see Chapter 9, “Configuring OSPF Routing.”)

```
Ethernet
   Mod Config
      Ether options…
         RIP=On
         Ignore Def Rt=Yes
      RIP Policy=Poison Rvrs
      RIP Summary=Yes
      ICMP Redirects=Accept
```

Understanding the dynamic routing parameters

This section provides some background information about the dynamic routing options. For complete information, see the *MAX Reference Guide*.

RIP (Routing Information Protocol)

The RIP parameter enables the MultiVoice Gateway to send or receive RIP updates (or both) on the Ethernet interface. You can also choose between RIP-v1 and RIP-v2 on the Ethernet interface.

Note: The IETF has voted to move RIP-v1 into the *historic* category and its use is no longer recommended. Ascend recommends that you upgrade all routers and hosts to RIP-v2. If you must maintain RIP-v1, Ascend recommends that you create a separate subnet and place all RIP-v1 routers and hosts on that subnet.

Ignoring the default route

You can configure the MultiVoice Gateway to ignore default routes advertised by routing protocols. This configuration is recommended, because you typically do not want the default route changed by a RIP update. The default route specifies a static route to another IP router, which is often a local router such as a Cisco router or another kind of LAN router. When the MultiVoice Gateway is configured to ignore the default route, RIP updates will not modify the default route in the MultiVoice Gateway routing table.

RIP Policy and RIP Summary

The RIP Policy and RIP Summary parameters have no affect on RIP-v2.

If the MultiVoice Gateway is running RIP-v1, the RIP Policy parameter specifies a split horizon or poison reverse policy to handle update packets that include routes that were received on the same interface on which the update is sent. Split-horizon means that the MultiVoice Gateway does not propagate routes back to the subnet from which they were received. Poison-reverse means that it propagates routes back to the subnet from which they were received, but with a metric of 16.

The RIP Summary parameter specifies whether to summarize subnet information when advertising routes. If the MultiVoice Gateway summarizes RIP routes, it advertises a route to all the subnets in a network of the same class. For example, the route to 200.5.8.13/28 (a class C address subnetted to 28 bits) would be advertised as a route to 200.5.8.0. When the MultiVoice Gateway does not summarize information, it advertises each route in its routing table as-is. In the example just given, the MultiVoice Gateway would advertise a route only to 200.5.8.13.

Ignoring ICMP Redirects

ICMP was designed to dynamically find the most efficient IP route to a destination. ICMP Redirect packets are one of the oldest route discovery methods on the Internet. They are also ne of the least secure methods, because it is possible to counterfeit ICMP Redirects and change the way a device routes packets.

Examples of RIP and ICMP configurations

The following sample configuration instructs the router to ignore ICMP redirect packets, and to receive (but not send) RIP updates on the Ethernet interface.

1 Open Ethernet > Mod Config > Ether Options.

2 Configure the router to receive (but not send) RIP updates on Ethernet:

```
Ethernet
   Mod Config
      Ether options…
         RIP=Recv-v2
```

Receiving RIP updates on Ethernet means that the router will learn about networks that are reachable through other local routers. However, it will not propagate information about all of its remote connections to the local routers.

3 Close the Ether Options subprofile, and set ICMP Redirects to Ignore.

```
ICMP Redirects=Ignore
```

4 Close the Ethernet profile.

Managing IP routes and connections

This section describes how to monitor TCP/IP/UDP and related information in the terminal-server command-line interface. To invoke the terminal-server interface, select System > Sys Diag > Term Serv and press Enter.

Working with the IP routing table

The terminal-server IProute commands display the routing table and enable you to add or delete routes. The changes you make to the routing table by using the IProute command last only until the MultiVoice Gateway unit resets. To display the IProute commands:

```
ascend% iproute ?

iproute ?       Display help information
iproute add     iproute add <destination/size> <gateway> [ pref ] [ m
iproute delete  iproute delete <destination/size> <gateway> [ proto ]
iproute show    displays IP routes (same as "show ip routes" command)
```

Displaying the routing table

Note that the IProute Show command and the Show IP Routes command have identical output. For example, to view the IP routing table:

```
ascend% iproute show

Destination        Gateway        IF       Flg Pref  Met   Use   Age
127.0.0.1/32       -              lo0      CP   0     0     0     20887
10.1.2.0/24        -              ie0      C    0     0     19775 20887
10.1.2.1/32        -              lo0      CP   0     0     389   20887
255.255.255.255/32 -              ie0      CP   0     0     0     20887
```

The columns in the table display the following information:

Column	Description
Destination	Target address of a route. To send a packet to this address, the MultiVoice Gateway will use this route. Note that the router will use the most specific route (having the largest mask) that matches a given destination.
Gateway	Address of the next hop router that can forward packets to the given destination. Direct routes (without a gateway) do not show a gateway address in the gateway column.
IF	Name of the interface through which a packet addressed to this destination will be sent: • `ie0` is the Ethernet interface • `lo0` is the loopback interface

Column	Description
Flg	One or more of the following flag values: • C—A directly connected route such as Ethernet • I—ICMP Redirect dynamic route • N—Placed in the table via SNMP MIB II • O—A route learned from OSPF • R—Route learned from RIP • r—RADIUS route • S—Static route • ?—Route of unknown origin, which indicates an error • G—Indirect route via a gateway • P—Private route • T—Temporary route • *—Hidden route that will not be used unless another better route to the same destination goes down
Pref	Preference value of the route. Note that all routes that come from RIP have a preference value of 100, while the preference value of each individual static route can be set independently.
Metric	RIP-style metric for the route, with a valid range of 0-16. Routes learned from OSPF show a RIP metric of 10. OSPF Cost infinity routes show a RIP metric of 16.
Use	Count of the number of times the route was referenced since it was created. (Many of these references are internal, so this is not a count of the number of packets sent over this route.)
Age	Age of the route in seconds. Used for troubleshooting, to determine when routes are changing rapidly or flapping.

Continuing the example, the first route shown is the loopback route:

```
127.0.0.1/32        -               lo0       CP   0     0     0     20887
```

The loopback route says that packets sent to this special address will be handled internally. The C flag indicates a Connected route, while the P flag indicates that the router will not advertise this route.

The loopback route is followed by a connection to the Ethernet interface. It is directly connected, with a Preference and Metric of zero.

```
10.1.2.0/24         -               ie0       C    0     0     19775 20887
```

The last two routes are a private loopback route, and a private route to the broadcast address:

```
10.1.2.1/32         -               lo0       CP   0     0     389   20887
255.255.255.255/32 -                ie0       CP   0     0     0     20887
```

The private loopback route shown is a host route with the Ethernet address. It is private, so it will not be advertised. The private route to the broadcast address is used in cases where the router wants to broadcast a packet but is otherwise unconfigured with a route to the broadcast

address. This route is typically used when the MultiVoice Gateway is trying to locate a server on a client machine to handle challenges for a token security card.

Adding an IP route

To add to the MultiVoice Gateway unit's routing table a static route that will be lost when the unit resets, enter the IProute Add command in the following format:

iproute add *destination gateway [metric]*

where ***destination*** is the destination network address, ***gateway*** is the IP address of the router that can forward packets to that network, and ***metric*** is the virtual hop count (default 8) to the destination network. For example:

```
ascend% iproute add 10.1.2.0 10.0.0.3/24 1
```

This sample command adds a route to the 10.1.2.0 network and all of its subnets. The new route is through the IP router located at 10.0.0.3/24. The metric to the route is 1 (it is one hop away).

If you try to add a route to a destination that already exists in the routing table, the MultiVoice Gateway replaces the existing route, but only if it has a higher metric than the new route. If you get the message `Warning: a better route appears to exist`, the MultiVoice Gateway has rejected your attempt to add a route because the routing table already contained the same route with a lower metric. Note that RIP updates can change the metric for the route.

Deleting an IP route

To remove a route from the MultiVoice Gateway unit's routing table, enter the IProute Delete command in the following format:

iproute delete *destination gateway*

For example:

iproute delete 10.1.2.0 10.0.0.3/24

Note: RIP updates can add back any route you remove with IProute Delete. Also, the MultiVoice Gateway restores all routes listed in the Static Route profile after a system reset.

Displaying route statistics

The Traceroute command is useful for locating slow routers or diagnosing IP routing problems. It traces the route an IP packet follows, by launching UDP probe packets with a low Time-To-Live (TTL) value and then listening for an ICMP *time exceeded* reply from a router. The Traceroute command uses the following syntax:

```
traceroute [-n] [-v] [-m max_ttl] [-p port] [-q nqueries]
[-w waittime] host [datasize]
```

All flags are optional. The only required parameter is the destination host name or IP address.

The elements of the syntax are as follows:

Syntax element	Description
`-n`	Prints hop addresses numerically rather than symbolically and numerically (this eliminates a name server address-to-name lookup for each gateway found on the path).
`-v`	Verbose output. Lists all received ICMP packets other than Time Exceeded and ICMP Port Unreachable.
`-m` *`max_ttl`*	Set the maximum time-to-live (maximum number of hops) for outgoing probe packets. The default is 30 hops.
`-p` *`port`*	Set the base UDP port number used in probes. Traceroute hopes that nothing is listening on any of the UDP ports from the source to the destination host (so an ICMP Port Unreachable message will be returned to terminate the route tracing). If something is listening on a port in the default range, this option can be used to pick an unused port range. The default is 33434.
`-q` *`nqueries`*	Set the maximum number of queries for each hop. The default is 3.
`-w` *`waittime`*	Set the time to wait for a response to a query. The default is 3 seconds.
`host`	The destination host by name or IP address.
`datasize`	Set the size of the data field of the UDP probe datagram sent by Traceroute. The default is 0. This results in a datagram size of 38 bytes (a UDP packet carrying no data).

For example, to trace the route to the host Techpubs:

```
ascend% traceroute techpubs

traceroute to techpubs (10.65.212.19), 30 hops MultiVoice Gateway,
0 byte packets
 1  techpubs.eng.ascend.com (10.65.212.19)  0 ms  0 ms  0 ms
```

Probes start with a TTL of one and increase by one until one of the following conditions occurs:

1 The MultiVoice Gateway receives an ICMP *port unreachable* message.

The UDP port in the probe packets is set to an unlikely value, such as 33434, because the target host is not intended to process the packets. A *port unreachable* message indicates that the packets reached the target host and were rejected.

2 The TTL value reaches the maximum value.

By default, the maximum TTL is set to 30. You can specify a different TTL by using the –`m` option; for example:

```
traceroute -m 60 techpubs

traceroute to techpubs (10.65.212.19), 60 hops MultiVoice Gateway, 0
byte packets
 1  techpubs.eng.abc.com (10.65.212.19)  0 ms  0 ms  0 ms
```

Three probes are sent at each TTL setting. The second line of command output shows the address of the router and round trip time of each probe. If the probe answers come from different gateways, the address of each responding system is shown. If there is no response

within a three second timeout interval, the command output is an asterisk. The following annotations can appear after the time field in a response:

- !H—Host reached.
- !N—Network unreachable.
- !P—Protocol unreachable.
- !S—Source route failed. Might indicate a problem with the associated device.
- !F—Fragmentation needed. Might indicate a problem with the associated device.
- !h—Communication with the host is prohibited by filtering.
- !n—Communication with the network is prohibited by filtering.
- !c—Communication is otherwise prohibited by filtering.
- !?—An ICMP subcode detected. This event should not occur.
- !??—Reply received with inappropriate type. This event should not occur.

Pinging other IP hosts

The terminal-server Ping command is useful for verifying that the transmission path is open between the MultiVoice Gateway and another station. It sends an ICMP echo_request packet to the specified station. If the station receives the packet, it returns an ICMP echo_response packet. For example, to ping the host Techpubs:

```
ascend% ping techpubs

PING techpubs (10.65.212.19): 56 data bytes
64 bytes from 10.65.212.19: icmp_seq=0 ttl=255 time=0 ms
64 bytes from 10.65.212.19: icmp_seq=3 ttl=255 time=0 ms
^C
--- techpubs ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/MultiVoice Gateway = 0/0/0 ms
```

You can terminate the Ping exchange at any time by pressing Ctrl-C. When you press Ctrl-C, the command reports the number of packets sent and received, the percentage of packet loss, any duplicate or damaged echo_response packets, and round-trip statistics. In some cases, round-trip times cannot be calculated.

During the Ping exchange, the MultiVoice Gateway displays information about the packet exchange, including the TTL (Time-To-Live) of each ICMP echo_response packet.

Note: The maximum TTL for ICMP Ping is 255, but the maximum TTL for TCP is often 60 or lower, so you might be able to Ping a host but not be able to run a TCP application (such as Telnet or FTP) to that station. If you Ping a host running a version of Berkeley UNIX earlier than 4.3BSD-Tahoe, the TTL report is 255 minus the number of routers in the round-trip path. If you Ping a host running the current version of Berkeley UNIX, the TTL report is 255 minus the number of routers in the path from the remote system to the station performing the Ping.

The Ping command sends an ICMP mandatory echo_request datagram, which asks the remote station *Are you there?* If the echo_request reaches the remote station, the station sends back an ICMP echo_response datagram, which tells the sender *Yes, I am alive*. This exchange verifies that the transmission path is open between the MultiVoice Gateway and a remote station.

Configuring Finger support

You can configure the MultiVoice Gateway to respond to Finger requests, as specified in RFC 1288, *The Finger User Information Protocol*.

To enable the MultiVoice Gateway to respond to Finger requests:

1. Open the Ethernet > Mod Config.
2. Set Finger to Yes.
3. Exit and save the changes.

Displaying information

The following Show commands are useful for monitoring IP routing and related protocols:

```
show arp            Display the Arp Cache
show icmp           Display ICMP information
show if             Display Interface info. Type 'show if ?' for help.
show ip             Display IP information. Type 'show ip ?' for help.
show udp           Display UDP information. Type 'show udp ?' for help.
show tcp           Display TCP information. Type 'show tcp ?' for help.
show pools          Display the assign address pools.
```

Displaying the ARP cache

To display the ARP cache, enter the Show ARP command. For example:

```
ascend% show arp

entry typ ip address      ether addr    if rtr pkt   insert
    0 DYN 10.65.212.199  00C07B605C07   0   0   0   857783
    1 DYN 10.65.212.91   0080C7C4CB80   0   0   0   857866
    2 DYN 10.65.212.22   080020792B4C   0   0   0   857937
    3 DYN 10.65.212.3    0000813DF048   0   0   0   857566
    4 DYN 10.65.212.250  0020AFF80F1D   0   0   0   857883
    5 DYN 10.65.212.16   0020AFEC0AFB   0   0   0   857861
    6 DYN 10.65.212.227  00C07B5F14B6   0   0   0   857479
    7 DYN 10.65.212.36   00C07B5E9AA5   0   0   0   857602
    8 DYN 10.65.212.71   0080C730041F   0   0   0   857721
    9 DYN 10.65.212.5    0003C6010512   0   0   0   857602
   10 DYN 10.65.212.241  0080C72ED212   0   0   0   857781
   11 DYN 10.65.212.120  0080C7152582   0   0   0   857604
   12 DYN 10.65.212.156  0080A30ECE6D   0   0   0   857901
   13 DYN 10.65.212.100  00C07B60E28D   0   0   0   857934
   14 DYN 10.65.212.1    00000C065D27   0   0   0   857854
   15 DYN 10.65.212.102  08000716C449   0   0   0   857724
   16 DYN 10.65.212.33   00A024AA0283   0   0   0   857699
   17 DYN 10.65.212.96   0080C7301792   0   0   0   857757
   18 DYN 10.65.212.121  0080C79BF681   0   0   0   857848
   19 DYN 10.65.212.89   00A024A9FB99   0   0   0   857790
   20 DYN 10.65.212.26   00A024A8122C   0   0   0   857861
   21 DYN 10.65.212.6    0800207956A2   0   0   0   857918
   22 DYN 10.65.212.191  0080C75BE778   0   0   0   857918
   23 DYN 10.65.212.116  0080C72F66CC   0   0   0   857416
```

```
24 DYN 10.65.212.87   0000813606A0   0   0   0   857666
25 DYN 10.65.212.235  00C07B76D119   0   0   0   857708
26 DYN 10.65.212.19   08002075806B   0   0   0   857929
```

The ARP table displays the following information:

- `entry`—A unique identifier for each ARP table entry.
- `typ`—How the address was learned, dynamically (DYN) or statically (STAT).
- `ip address`—The address contained in ARP requests.
- `ether addr`—The MAC address of the host with that IP address.
- `if`—The interface on which the MultiVoice Gateway received the ARP request.
- `rtr`—The next-hop router on the specified interface.

Displaying ICMP packet statistics

To display the numbers of ICMP packets received intact, received with errors, and transmitted, enter the Show ICMP command. For example:

```
show icmp

3857661 packet received.
20 packets received with errors.
   Input histogram: 15070
2758129 packets transmitted.
0 packets transmitted due to lack of resources.
   Output histogram: 15218
```

The Input and Output histograms show the number of ICMP packets received and transmitted, respectively:

Displaying interface statistics

To display the supported interface-statistics commands:

```
ascend% show if ?

show if ?           Display help information
show if stats       Display Interface Statistics
show if totals      Display Interface Total counts
```

To display the status and packet count of each active WAN link and of as local and loopback interfaces, enter the Show IF Stats command. For example:

```
ascend% show if stats

Interface    Name    Status  Type     Speed    MTU InPackets Outpackets
ie0         ethernet   Up    6     10000000   1500    107385     85384
wan0                 Down    1           0   1500      0          0
wan1                 Down    1           0   1500      0          0
wan2                 Down    1           0   1500      0          0
wanidle0               Up    6     10000000   1500      0          0
lo0       loopback     Up   24     10000000   1500      0          0
```

The output contains the following fields:

Field	Description
Interface	Interface name.
Name	Name of the profile or a text name for the interface.
Status	Up (the interface is functional) or Down.
Type	Type of application being used on the interface, as specified in RFC 1213 (MIB-2). For example, 23 indicates PPP and 28 indicates SLIP.
Speed	Data rate in bits per second.
MTU	Maximum packet size allowed on the interface. MTU stands for Maximum Transmission Unit.
InPackets	Number of packets the interface has received.
OutPackets	Number of packets the interface has transmitted.

To display the packet count at each interface, broken down by type of packet, enter the Show IF Totals command. For example:

```
ascend% show if totals

Name  --Octets----Ucast-- -NonUcast- Discard -Error- Unknown -Same IF-
ie0  i:   7813606   85121     22383       0        0       0        0
     o: 101529978   85306       149       0        0       0        0
lo0  i:         0       0         0       0        0       0        0
     o:         0       0         0       0        0       0        0
```

The output contains these fields:

Field	Description
Name	Interface name.
Octets	Total number of bytes processed by the interface.
Ucast	Packets with a unicast destination address.
NonUcast	Packets with a multicast address or a broadcast address.
Discard	Number of packets that the interface could not process.
Error	Number of packets with CRC errors, header errors, or collisions.
Unknown	Number of packets the MultiVoice Gateway forwarded across all bridged interfaces because of unknown or unlearned destinations.
Same IF	Number of bridged packets whose destination is the same as the source.

Displaying IP statistics and addresses

To display the supported IP statistics and addresses commands:

```
ascend% show ip ?

show ip ?           Display help information
show ip stats       Display IP Statistics
```

```
show ip address     Display IP Address Assignments
show ip routes      Display IP Routes
```

Note: For information about the Show IP Routes command, see "Working with the IP routing table" on page 8-22.

To display statistics on IP activity, including the number of IP packets the MultiVoice Gateway has received and transmitted, enter the Show IP Stats command. For example:

```
ascend% show ip stats

107408 packets received.
     0 packets received with header errors.
     0 packets received with address errors.
     0 packets forwarded.
     0 packets received with unknown protocols.
     0 inbound packets discarded.
107408 packets delivered to upper layers.
 85421 transmit requests.
     0 discarded transmit packets.
     1 outbound packets with no route.
     0 reassembly timeouts.
     0 reassemblies required.
     0 reassemblies that went OK.
     0 reassemblies that Failed.
     0 packets fragmented OK.
     0 fragmentations that failed.
     0 fragment packets created.
     0 route discards due to lack of memory.
     64 default ttl.
```

To display IP interface address information, enter the Show IP address command. For example:

```
ascend% show ip address

Interface   IP Address    Dest Address   Netmask         MTU     Status
ie0         10.2.3.4      N/A            255.255.255.224   1500      Up
wan0        0.0.0.0       N/A            0.0.0.0           1500    Down
wan1        13.1.2.0      13.1.2.128     255.255.255.248   1500    Down
wan2        0.0.0.0       N/A            0.0.0.0           1500    Down
wan3        0.0.0.0       N/A            0.0.0.0           1500    Down
lo0         127.0.0.1     N/A            255.255.255.255   1500      Up
rj0         127.0.0.2     N/A            255.255.255.255   1500      Up
bh0         127.0.0.3     N/A            255.255.255.255   1500      Up
```

Displaying UDP statistics and listen table

To display the supported UDP-statistics commands:

```
ascend% show udp ?

show udp ?          Display help information
show udp stats      Display UDP Statistics
show udp listen     Display UDP Listen Table
```

To display the number of UDP packets received and transmitted, enter the Show UDP Stats command. For example:

```
ascend% show udp stats

22386 packets received.
    0 packets received with no ports.
    0 packets received with errors.
    0 packets dropped
    9 packets transmitted.
```

The Show UDP Listen command displays the socket number, UDP port number, and number of packets queued for each UDP port on which the MultiVoice Gateway is currently listening. The command's output also includes the following fields:

Field	Description
InQMax	Maximum number of queued UDP packets on the socket. (See Queue Depth and Rip Queue Depth parameters.)
InQLen	Current number of queued packets on the socket.
InQDrops	Number of packets discarded to prevent InQLen from exceeding InQMax.
Total Rx	Total number of packets received on the socket, including InQDrops.

For example:

```
ascend% show udp listen

udp:
Socket Local Port InQLen InQMax    InQDrops    Total Rx
0        1023       0       1           0           0
1         520       0      50           0         532
2           7       0      32           0           0
3         123       0      32           0           0
4        1022       0     128           0           0
5         161       0      64           0           0
```

Displaying TCP statistics and connections

To display the supported TCP-statistics commands:

```
ascend% show tcp ?

show tcp ?          Display help information
show tcp stats      Display TCP Statistics
show tcp connection Display TCP Connection Table
```

To display the number of TCP packets received and transmitted, enter the Show TCP Stats command. For example:

```
ascend% show tcp stats

     0 active opens.
    11 passive opens.
     1 connect attempts failed.
     1 connections were reset.
     3 connections currently established.
 85262 segments received.
```

```
 85598 segments transmitted.
   559 segments re-transmitted.
```

An `active open` is a TCP session that the MultiVoice Gateway initiated, and a `passive open` is a TCP session that the MultiVoice Gateway did not initiate.

To display current TCP sessions, enter the Show TCP Connection command. For example:

```
ascend% show tcp connection
Socket       Local              Remote                      State
0            *.23               *.*                       LISTEN
1            10.2.3.23          15.5.248.121.15003    ESTABLISHED
```

Configuring OSPF Routing

9

This chapter covers the following topics:

Introduction to OSPF

OSPF (Open Shortest Path First) is the next generation Internet routing protocol. The *Open* in its name refers to the fact that OSPF was developed in the public domain as an open specification. The *Shortest Path First* refers to an algorithm developed by Dijkstra in 1978 for building a self-rooted shortest-path tree from which routing tables can be derived. This algorithm is described in "The link-state routing algorithm" on page 9-8.

RIP limitations solved by OSPF

The rapid growth of the Internet has pushed Routing Information Protocol (RIP) beyond its capabilities, especially because of the following problems:

Problem	Description and solution
Distance-vector metrics	RIP is a distance-vector protocol, which uses a hop count to select the shortest route to a destination network. RIP always uses the lowest hop count, regardless of the speed or reliability of a link.
	OSPF is a link-state protocol, which means that OSPF can take into account a variety of link conditions, such as the reliability or speed of the link, when determining the best path to a destination network.
15-hop limitation	With RIP, a destination that requires more than 15 consecutive hops is considered unreachable, which inhibits the maximum size of a network.
	OSPF has no hop limitation. You can add as many routers to a network as you want.

Problem	Description and solution
Excessive routing traffic and slow convergence	RIP creates a routing table and then propagates it throughout the internet of routers, hop by hop. The time it takes for all routers to receive information about a topology change is called *convergence*. A slow convergence can result in routing loops and errors. A RIP router broadcasts its entire routing table every 30 seconds. On a 15-hop network, convergence can be as high as 7.5 minutes. In addition, a large table can require multiple broadcasts for each update, which consumes a lot of bandwidth. OSPF uses a topological database of the network and propagates only changes to the database (as described in "Exchange of routing information" on page 9-4).

Ascend implementation of OSPF

The primary goal of OSPF at this release is to enable the MultiVoice Gateway to communicate with other routers within a single autonomous system (AS).

The MultiVoice Gateway acts as an OSPF internal router with limited border router capability. At this release, Ascend does not recommend an area border router (ABR) configuration for the MultiVoice Gateway, so the Ethernet interface and all of the MultiVoice Gateway WAN links should be configured in the same area.

The MultiVoice Gateway does not function as a full AS border router (ASBR) at this release. However, it performs ASBR calculations for external routes such as WAN links that do not support OSPF. It imports external routes into its OSPF database and flags them as ASE (autonomous system external). It redistributes those routes by means of OSPF ASE advertisements, and propagates its OSPF routes to remote WAN routers that are running RIP.

The MultiVoice Gateway supports null and simple password authentication.

OSPF features

This section provides a brief overview of OSPF routing to help you properly configure the MultiVoice Gateway. For full details about how OSPF works, see RFC 1583, "OSPF Version 2," 03/23/1994, J. Moy.

An Autonomous System (AS) is a group of OSPF routers exchanging information, typically under the control of one company. An AS can include a large number of networks, all of which are assigned the same AS number. All information exchanged within the AS is *interior.*

Exterior protocols are used to exchange routing information between autonomous systems. They are referred to by the acronym EGP (exterior gateway protocol). The AS number can be used by border routers to filter out certain EGP routing information. OSPF can make use of EGP data generated by other border routers and added into the OSPF system as ASEs, as well as static routes configured in the MultiVoice Gateway or RADIUS.

Security

All OSPF protocol exchanges are authenticated. This means that only trusted routers can participate in the AS's routing. A variety of authentication schemes are available. In fact, different authentication types can be configured for each area. In addition, authentication provides added security for the routers that are on the network. Routers that do not have the password will not be able to gain access to the routing information, because authentication failure prevents a router from forming adjacencies.

Support for variable length subnet masks

OSPF enables the flexible configuration of IP subnets. Each route distributed by OSPF has a destination and mask. Two different subnets of the same IP network number may have different sizes (different masks). This is commonly referred to as variable length subnet masks (VLSM), or Classless Inter-Domain Routing (CIDR). A packet is routed to the best (longest or most specific) match. Host routes are considered to be subnets whose masks are all ones (0xFFFFFFFF).

Note: Although OSPF is very useful for networks that use VLSM, Ascend recommends that you attempt to assign subnets that are as contiguous as possible in order to prevent excessive link-state calculations by all OSPF routers on the network.

Interior gateway protocol (IGP)

OSPF keeps all AS-internal routing information within the AS. All information exchanged within the AS is *interior.*

For communication with other autonomous systems, an AS border router (ASBR) is required to use an external gateway protocol (EGP), as shown in Figure 9-1. An EGP acts as a shuttle service between autonomous systems.

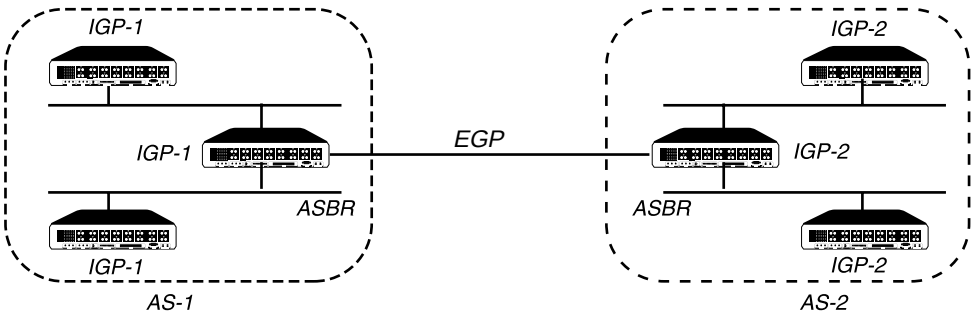


Figure 9-1. Autonomous system border routers

ASBRs perform calculations related to external routes. The MultiVoice Gateway imports external routes from RIP (for example, when it establishes a WAN link with a caller that does not support OSPF) and always performs the ASBR calculations.

If you must prevent the MultiVoice Gateway from performing ASBR calculations, you can disable them in Ethernet > Mod Config > OSPF Global Options.

Exchange of routing information

OSPF uses a topological database of the network and propagates only changes to the database. Part of the SPF algorithm involves acquiring neighbors, then forming an adjacency with one neighbor, as shown in Figure 9-2.

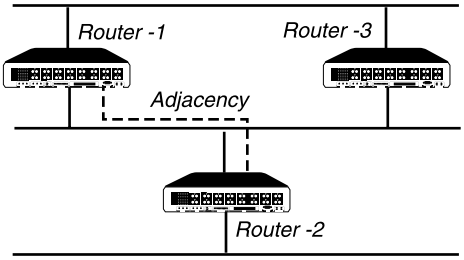


Figure 9-2. Adjacency between neighboring routers

An OSPF router dynamically detects its neighboring routers by sending its Hello packets to the multicast address `All SPFRouters`. It then attempts to form adjacencies with some of its newly acquired neighbors.

Adjacency is a relationship formed between selected neighboring routers for the purpose of exchanging routing information. Not every pair of neighboring routers becomes adjacent. Adjacencies are established during network initialization in pairs, between two neighbors. As the adjacency is established, the neighbors exchange databases and build a consistent, synchronized database between them.

When an OSPF router detects a change on one of its interfaces, it modifies its topological database and multicasts the change to its adjacent neighbor, which in turn propagates the change to its adjacent neighbor until all routers within an area have synchronized topological databases. This results in quick convergence among routers. OSPF routes can also be summarized in link-state advertisements (LSAs).

Designated and backup designated routers

In OSPF terminology, a broadcast network is any network that has more than two OSPF routers attached and that supports the capability to address a single physical message to all of the attached routers.

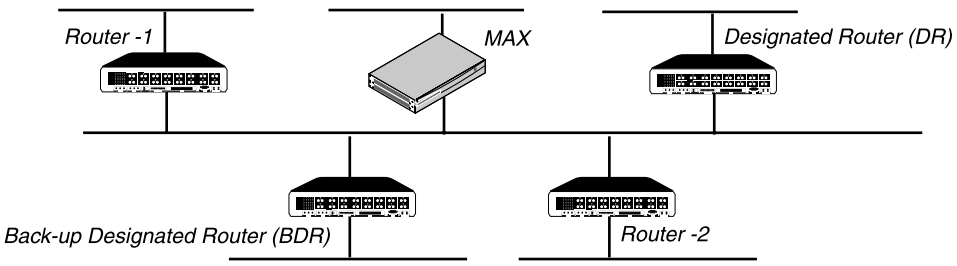


Figure 9-3. Designated and backup designated routers

The MultiVoice Gateway can function as a designated router (DR) or backup designated router (BDR). However, many sites choose to assign a LAN-based router for these roles in order to

dedicate the MultiVoice Gateway to WAN processing. The administrator chooses a DR and BDR on the basis of the device's processing power and reliability.

To reduce the number of adjacencies each router must form, OSPF calls one of the routers the designated router. A designated router is elected as routers are forming adjacencies, and then all other routers establish adjacencies only with the designated router. This simplifies the routing table update procedure and reduces the number of link-state records in the database. The designated router plays other important roles as well, to reduce the overhead of OSPF link-state procedures. For example, other routers send link-state advertisements to the designated router only by using the *all-designated-routers* multicast address of 224.0.0.6.

To prevent the designated router from becoming a serious liability to the network if it fails, OSPF also elects a backup designated router at the same time. Other routers maintain adjacencies with both the designated router and its backup router, but the backup router leaves as many of the processing tasks as possible to the designated router. If the designated router fails, the backup immediately becomes the designated router and a new backup is elected.

The administrator chooses which router is to be the designated router on the basis of the processing power, speed, and memory of the system, and then assigns priorities to other routers on the network in case the backup designated router is also down at the same time.

Configurable metrics

The administrator assigns a cost to the output side of each router interface. The lower the cost, the more likely the interface is to be used to forward data traffic. Costs can also be associated with the externally derived routing data.

The OSPF cost can also be used for preferred path selection. If two paths to a destination have equal costs, you can assign a higher cost to one of the paths, to configure it as a backup to be used only when the primary path is not available.

Figure 9-4 shows how costs are used to direct traffic over high-speed links. For example, if Router-2 in Figure 9-4 receives packets destined for Host B, it routes them through Router-1 across two T1 links (Cost=20) rather than across one 56Kbps B channel to Router-3 (Cost=240).

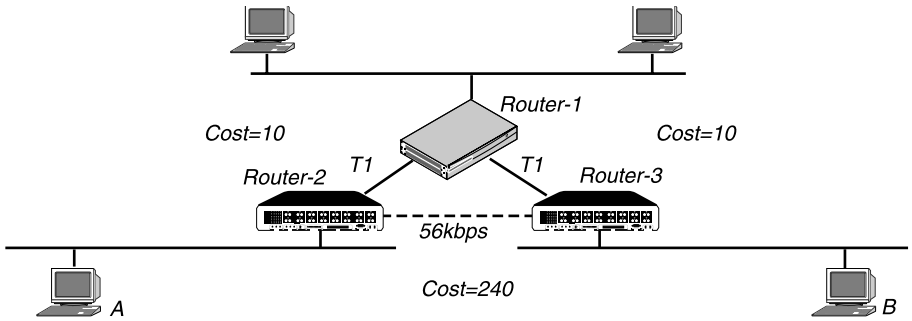


Figure 9-4. OSPF costs for different types of links

The MultiVoice Gateway has a default cost of 1 for a connected route (Ethernet) and 10 for a WAN link. If you have two paths to the same destination, the one with the lower cost will be used. You might want to account for the bandwidth of a connection when assigning costs. For

example, for a single B-channel connection, the cost would be 24 times greater than for a T1 link.

Note: Be careful when assigning costs. Incorrect cost metrics can cause delays and congestion on the network.

Hierarchical routing (areas)

If a network is large, the size of the database, time required for route computation, and related network traffic become excessive. An administrator can partition an AS into areas to provide hierarchical routing connected by a backbone.

The backbone area is special and always has the area number 0.0.0.0. Other areas are assigned area numbers that are unique within the autonomous system.

Each areas acts like its own network: All area-specific routing information stays within the area, and all routers within an area must have a synchronized topological database. To tie the areas together, some routers belong to the backbone area and to another area. These routers are area border routers (ABRs). In Figure 9-5, all of the routers are ABRs.If the ABRs and area boundaries are set up correctly, link-state databases are unique to an area.

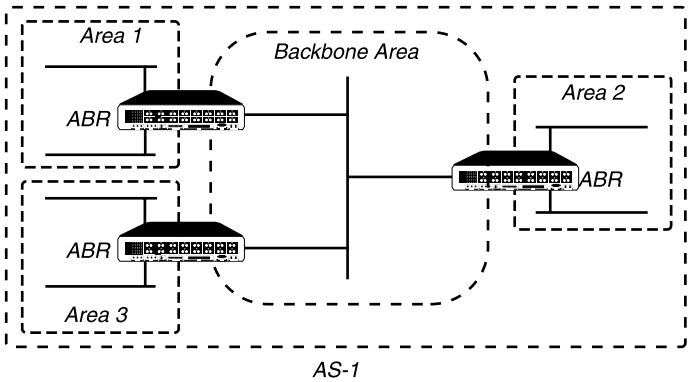


Figure 9-5. Dividing an AS into areas

Note: At this release, Ascend recommends that you do not configure the MultiVoice Gateway as an ABR. The current recommendation is that you use the same area number for the Ethernet interface of the MultiVoice Gateway and each of its WAN links. That number does not have to be the backbone area number. The MultiVoice Gateway can reside in any OSPF area.

Stub areas

To reduce the cost of routing, OSPF supports stub areas, in which a default route summarizes all external routes. For areas that are connected to the backbone by only one ABR (that is, the area has one exit point), there is no need to maintain information about external routes. Stub areas are similar to regular areas except that the routers do not enter external routes in the area's databases.

To prevent flooding of external routes throughout the AS, you can configure an area as a stub if the area has a single exit point, or if the choice of exit point need not be made on a per-external-destination basis. You might need to specify a stub area with no default cost (StubNoDefault) if the area has more than one exit point.

In a stub area, routing to AS-external destinations is based on a per-area default cost. The per-area default cost is advertised to all routers within the stub area by a border router, and is used for all external destinations.

If the MultiVoice Gateway supports external routes across its WAN links, you should not configure it in a stub area. Because an ABR configuration is not currently recommended for the MultiVoice Gateway, the area in which it resides should not be a stub area if any of its links are AS-external.

Not So Stubby Areas (NSSAs)

The MultiVoice Gateway supports OSPF Not So Stubby Areas (NSSAs) as described in RRC 1587. NSSAs allow you to treat complex networks similarly to stub areas. This can simplify your network's topology and reduce OSPF-related traffic.

NSSAs and Type-7 LSAs

NSSAs are similar to stub areas, except that they allow limited importing of Autonomous System (AS) external routes. NSSAs use Type-7 LSAs to import external route information into an NSSA. Type-7 LSAs are similar to Type-5 LSAs except that:

- NSSAs can originate and import Type-7 LSAs. Like stub areas, NSSAs cannot originate or import Type-5 LSAs.
- Type-7 LSAs can only be advertised within a single NSSA. They are not flooded throughout the AS as are Type-5 LSAs.

When you configure the MultiVoice Gateway as an NSSA internal router, you define the Type-7 LSAs you want to advertise throughout the NSSA as static routes.

You must also specify whether these Type-7 LSAs should be advertised outside the NSSA. If you choose to advertise a Type-7 LSA, the NSSA Area Border Router (ABR) converts it to a Type-5 LSA, which can then be flooded throughout the AS. If you choose not to advertise a Type-7 LSA, it is not advertised beyond the NSSA.

(For complete information on NSSAs, see RFC 1587.)

Configuring the MultiVoice Gateway as an NSSA internal router

Because the MultiVoice Gateway cannot be an area border router, when you configure OSPF on the MultiVoice Gateway keep in mind that:

- The Area-Type must be the same on all MultiVoice Gateway interfaces running OSPF.
- The Area ID (configured in the Area parameter) must be the same on all MultiVoice Gateway interfaces running OSPF.

To configure the MultiVoice Gateway as an NSSA:

1 Select Ethernet > Mod Config > OSPF options.

2 Set AreaType to NSSA.

3 Exit and save the Mod Config profile.

4 Select Ethernet > Static Rtes > *any Static Route profile*.

5 Configure a static route to the destination outside the NSSA.

6 Refer to the documentation that came with your MultiVoice Gateway.

7 In this static route profile, specify whether you want to advertise this route outside the NSSA:

- To advertise this route outside the NSSA, set NSSA-Type to Advertise.
- To not advertise this route outside the NSSA, set NSSA-Type to DoNotAdvertise.

8 Exit and save the Static Rtes profile.

9 Reset the MultiVoice Gateway.

The link-state routing algorithm

Link-state routing algorithms require that all routers within a domain maintain synchronized (identical) topological databases, and that the databases describe the complete topology of the domain. An OSPF router's domain can be an AS or an area within an AS.

OSPF routers exchange routing information and build Link-state databases. Link-state databases are synchronized between pairs of adjacent routers (as described in "Exchange of routing information" on page 9-4). In addition, each OSPF router uses its link-state database to calculate a self-rooted tree of shortest paths to all destinations, as shown in Figure 9-6.

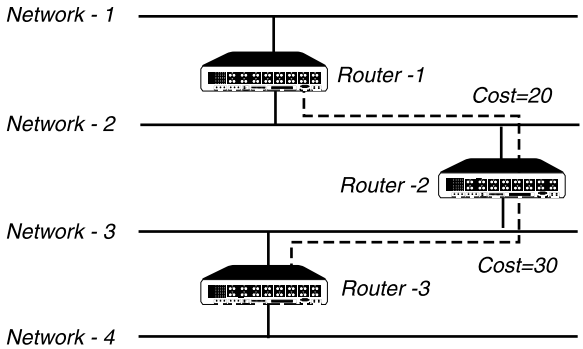


Figure 9-6. Sample network topology

The routers then use the trees to build their routing tables, as shown in Table 9-1.

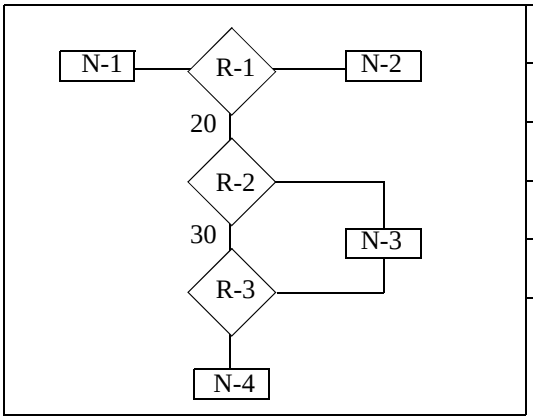
Table 9-1. Link state databases for network topology in Figure 9-6

Router-1	**Router-2**	**Router-3**
Network-1/Cost 0	Network-2/Cost0	Network-3/Cost 0
Network-2/Cost 0	Network-3/Cost0	Network-4/Cost 0
Router-2/Cost 20	Router-1/Cost 20	Router-2/Cost 30
	Router-3/Cost 30	

Table 9-2, Table 9-3, and Table 9-4 show another example of self-rooted shortest-path trees calculated from link-state databases, and the resulting routing tables. Actual routing tables also contain externally derived routing data, which is advertised throughout the AS but kept

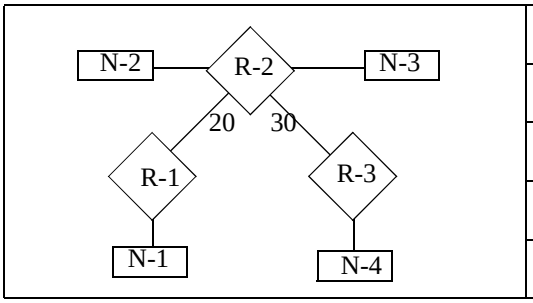
separate from the Link-state data. Also, each external route can be tagged by the advertising router, enabling the passing of additional information between routers on the boundary of the AS.

Table 9-2. Shortest-path tree and resulting routing table for Router-1



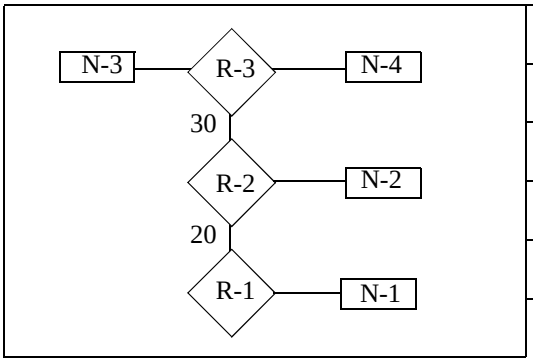
Destination	*Next Hop*	*Metric*
Network-1	Direct	0
Network-2	Direct	0
Network-3	Router-2	20
Network-4	Router-2	50

Table 9-3. Shortest-path tree and resulting routing table for Router-2



Destination	*Next Hop*	*Metric*
Network-1	Router-1	20
Network-2	Direct	0
Network-3	Direct	0
Network-4	Router-2	30

Table 9-4. Shortest-path tree and resulting routing table for Router-3



Destination	*Next Hop*	*Metric*
Network-1	Router-2	50
Network-2	Router-2	30
Network-3	Direct	0
Network-4	Direct	0

Configuring OSPF routing in the MultiVoice Gateway

The following examples shows the parameters related to OSPF routing in the MultiVoice Gateway:

```
Ethernet
   Mod Config
      OSPF options...
         RunOSPF=Yes
         Area=0.0.0.0
         AreaType=Normal
         HelloInterval=10
         DeadInterval=40
         Priority=5
         AuthType=Simple
         AuthKey=ascend0
         Cost=1
         ASE-type=N/A
         ASE-tag=N/A
         TransitDelay=1
         RetransmitInterval=5

      OSPF global options...
         Enable ASBR=Yes
```

Understanding the OSPF routing parameters

This section provides some background information about the OSPF parameters. For more information on each parameter, see the *MAX Reference Guide*. For OSPF routing, you set the following parameters:

Parameters	Description
RunOSPF	OSPF is turned off by default. To enable it on the interface, set RunOSPF to Yes.
Area	Sets the area ID for the interface. The format for this ID is dotted decimal, but it is not an IP address. (For a description of areas, see “Hierarchical routing (areas)” on page 9-6.)
AreaType	Specifies the type of area: Normal, Stub, or StubNoDefault. (For descriptions, see “Stub areas” on page 9-6.)
HelloInterval	Specifies how frequently, in seconds, the MultiVoice Gateway sends out Hello packets on the specified interface. OSPF routers use Hello packets to dynamically detect neighboring routers in order to form adjacencies.
DeadInterval	Specifies how many seconds the MultiVoice Gateway waits before declaring its neighboring routers down after it stops receiving their Hello packets. (For background information, see “Exchange of routing information” on page 9-4.)

Parameters	Description
Priority	Value used by the routers in the network to elect a Designated Router (DR) and Backup Designated Router (BDR). Assigning a priority of 1 would place the MultiVoice Gateway near the top of the list of possible designated routers. (Currently, you should assign a larger number.) Acting as a DR or BDR significantly increases the amount of OSPF overhead for the router. (For a discussion of the functions of DRs and BDRs, see “Designated and backup designated routers” on page 9-4.)
Auth Type	Type of authentication supported. The Normal setting specifies that the MultiVoice Gateway supports OSPF router authentication. (For more information, see “Security” on page 9-3.)
Auth Key	Specifies the key that the MultiVoice Gateway looks for in packets to support OSPF router authentication.
Cost	Specifies the link-state or output cost of a route. Assign realistic costs for each interface that supports OSPF. The lower the cost, the higher the likelihood of using that route to forward traffic. (For more information, see “Configurable metrics” on page 9-5.)
ASE-type and ASE-tag	Autonomous System External (ASE) routes are used only when OSPF is turned off on a particular interface. When OSPF is enabled, the ASE parameters are not applicable. ASE-type specifies the type of metric that the MultiVoice Gateway advertises for external routes. A Type-1 external metric is expressed in the same units as the link-state metric (the same units as interface cost). A Type-2 external metric is considered larger than any link state path. Use of Type-2 external metrics assumes that routing between autonomous systems is the major cost of routing a packet, and eliminates the need for conversion of external costs to internal link-state metrics.
TransitDelay	Specifies the estimated number of seconds it takes to transmit a Link State Update Packet over this interface, taking into account transmission and propagation delays. On a connected route, you can leave the default of 1.
RetransmitInterval	Specify the number of seconds between retransmissions of Link-State Advertisements, Database Description, and Link State Request Packets.
OSPF global options	Enable or disable Autonomous System Border Routers (ASBRs) calculations related to external routes. The MultiVoice Gateway imports external routes from RIP (for example, when it establishes a WAN link with a caller that does not support OSPF) and performs the ASBR calculations. If you must prevent the MultiVoice Gateway from performing ASBR calculations, you can disable them in Ethernet > Mod Config > OSPF Global Options.

Example of configuration adding the MultiVoice Gateway to an OSPF network

This section describes how to add a MultiVoice Gateway to your OSPF network. It assumes that you know how to configure the MultiVoice Gateway with an appropriate IP address as described in Chapter 8, "Configuring IP Routing." The procedures in this section are examples based on Figure 9-7. To apply one or more of the procedures to your network, enter the appropriate settings instead of the ones shown.

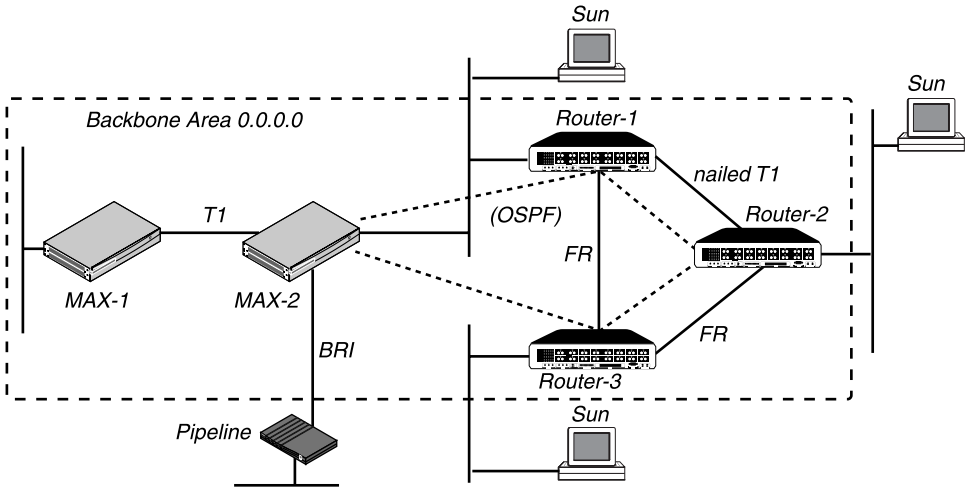


Figure 9-7. Example of an OSPF setup

In Figure 9-7, all OSPF routers are in the same area (the backbone area), so the units form adjacencies and synchronize their databases together.

Note: All OSPF routers in Figure 9-7 have RIP turned off. OSPF can learn routes from RIP without the added overhead of running RIP.

The MultiVoice Gateway's Ethernet interface in the sample network diagram is in the OSPF backbone area. Although there is no limitation stated in the RFC about the number of routers in the backbone area, you should keep the number of routers relatively small, because changes that occur in area zero are propagated throughout the AS.

Another way to configure the same units would be to create a second area (such as 0.0.0.1) in one of the existing OSPF routers, and add the MultiVoice Gateway to that area. You could then assign the same area number (0.0.0.1) to all OSPF routers reached through the MultiVoice Gateway across a WAN link.

After you configure the MultiVoice Gateway as an IP host on that interface, you could configure it as an OSPF router in the backbone area in the Ethernet profile. To configure the MultiVoice Gateway as an OSPF router on Ethernet:

1 Open Ethernet > Mod Config > Ether Options, and make sure the MultiVoice Gateway is configured as an IP host. For example:

```
Ethernet
   Mod Config
      Ether options...
         IP Adrs=10.168.8.17/24
         2nd Adrs=0.0.0.0
```

```
RIP=Off
Ignore Def Rt=Yes
Proxy Mode=Always
Filter=0
IPX Frame=N/A
```

Note that RIP is turned off. It is not necessary to run both RIP and OSPF, and turning RIP off reduces processor overhead. OSPF can learn routes from RIP, incorporate them in the routing table, assign them an external metric, and tag them as external routes. (For more information, see Chapter 8, “Configuring IP Routing.”)

2 Open Ethernet > Mod Config > OSPF Options and turn on RunOSPF:

```
OSPF options...
   RunOSPF=Yes
```

3 Specify the area number and area type for the Ethernet:

```
Area=0.0.0.0
AreaType=Normal
```

In this case, the Ethernet is in the backbone area. (The backbone area number is always 0.0.0.0.) The backbone area is not a stub area, so leave the setting at its default. (For background information, see “Stub areas” on page 9-6.)

4 Leave the Hello interval, Dead interval, and Priority values set to their defaults:

```
HelloInterval=10
DeadInterval=40
Priority=5
```

5 If authentication is required to get into the backbone area, specify the password.

For example:

```
AuthType=Simple
AuthKey=ascend0
```

If authentication is not required, set AuthType=None.

6 Configure the cost for the MultiVoice Gateway to route into the backbone area. For example:

```
Cost=1
```

Then type a number greater than zero and less than 16777215. By default the cost of a Ethernet connected route is 1.

7 Set the expected transit delay for Link State Update packets. For example:

```
TransitDelay=1
```

8 Specify the retransmit interval for OSPF packets.

```
RetransmitInterval=5
```

This parameter specifies the number of seconds between retransmissions of Link-State Advertisements, Database Description and Link State Request Packets.

9 Close the Ethernet profile.

When you close the Ethernet profile, the MultiVoice Gateway comes up as an OSPF router on that interface. It forms adjacencies and begins building its routing table.

Administering OSPF

This section describes how to work with OSPF information in the routing table and how to monitor OSPF activity in the terminal-server command-line interface.

To invoke the terminal-server interface, select System > Sys Diag > Term Serv and press Enter.

Working with the routing table

The OSPF routing table includes routes built from the router's link-state database as well as those added by external routing protocols such as RIP. You can also add routes statically (for example, to direct traffic destined for a remote site through one of several possible border routers.) For details about adding static routes (for example, if you want to force the use of one route over those learned from OSPF), see Chapter 8, "Configuring IP Routing.".

To display the IP routing table with added OSPF information, invoke the terminal-server (System > Sys Diag > Term Serv) and use the Iproute Show command with the –l option:

```
ascend% iproute show -l
```

In addition to the standard routing-table fields, which are described in Chapter 8, "Configuring IP Routing," the following three columns are specific to OSPF and are displayed only when you use the –l option. These OSPF-specific columns are displayed at the far right of the routing table:

```
...     Cost        T        Tag
...     1           0        0xc0000000
...     9           1        0xc8000000
...     10          0        0xc0000000
...     9           1        0xc8000000
...     1           1        0xc0000000
...     3           1        0xc8000000
...     9           1        0xc8000000
...     4           1        0xc8000000
...     5           1        0xc8000000
...     3           1        0xc8000000
...     3           1        0xc8000000
...     3           1        0xc8000000
```

Column	Description
Cost	The cost of an OSPF route. The interpretation of this cost depends on the type of external metric, which is displayed in the next column. If the MultiVoice Gateway is advertising Type-1 metrics, OSPF can use the specified number as the cost of the route. Type-2 external metrics are an order of magnitude larger.
T	The ASE-type of metric to be advertised for an external route. A 0 (zero) in this column means that the metric is an external-Type-1 or an OSPF internal route. A 1 means that the route is an external-Type-2 route.
Tag	Specifies a 32-bit hexadecimal number attached to each external route to tag it as external to the AS. This number may be used by border routers to filter this record.

Multipath routing

A MAX running OSPF can alternate between two equal cost gateways. When OSPF detects more than one equally good gateway, in terms of routing costs, each equal-cost gateway is put on an equal-cost list. The router will alternate between all the gateways on the list. This is called equal-cost multipath routing.

For example, if router A has two equal-cost routes to example.com, one via router B and the other via router C, the routing table could look like this:

```
Destination        Gateway         IF       Flg   Pref Met     Use
Age
10.174.88.0/25    10.174.88.12    wan2     OGM     10  10      52      19
10.174.88.0/25    10.174.88.13    wan3     OGM     10  10      52      19
10.174.88.12/32   10.174.88.12    wan2     OG      10  10       0      28
10.174.88.13/32   10.174.88.13    wan3     OG      10  10       0      28
192.168.253.0/24   -              ie0      C        0   0       1      49
192.168.253.6/32   -              lo0      CP       0   0      53      49
223.1.1.0/24       10.174.88.12   wan2     OG      10  10       0      19
223.5.1.0/24       10.174.88.12   wan2     OG      10  10       0      19
223.12.9.0/24      10.174.88.12   wan2     OG      10  10       0      19
255.255.255.255/32 -              ie0      CP       0   0       0      49
```

Note that the *M* in the Flags column indicates an equal-cost multipath. A Traceroute from router A to example.com would look like this:

```
ascend% traceroute -q 10 example.com

traceroute to example.com (10.174.88.1), 30 hops max, 0 byte pack-
ets

1  C.example.com (10.174.88.13)  20 ms B .example.com
(10.174.88.12)  20 ms C.example.com (10.174.88.13)  20 ms B .exam-
ple.com (10.174.88.12)  20 ms  20 ms C.example.com (10.174.88.13)
60 ms  20 ms B .example.com (10.174.88.12)  20 ms C.example.com
(10.174.88.13)  20 ms B .example.com (10.174.88.12)  20 ms

2  example.com (10.174.88.1)  20 ms  20 ms  20 ms  20 ms  30 ms  20
ms  20 ms  30 ms  20 ms  30 ms
```

Note: Notice the alternating replies. The replies are statistically dispatched to B and C, with roughly 50% of the packets sent through each gateway. (For background information about the routing table and about the Traceroute command, see Chapter 8, “Configuring IP Routing.”)

Third-party routing

A MultiVoice Gateway running OSPF can advertise routes to external destinations on behalf of another gateway (a *third-party*). This is commonly known as advertising a forwarding address. Depending on the exact topology of the network, other routers might be able to use this type of LSA and route directly to the forwarding address without involving the advertising MultiVoice Gateway, thereby increasing the total network throughput.

Third-party routing requires that all OSPF routers know how to route to the forwarding address. This usually means that the forwarding address must be on an Ethernet that has an OSPF router acting as the forwarding router, or that the designated router is sending LSAs for that Ethernet to any area that sees the static route's forwarding-address LSAs.

The following example shows how to configure a static route for OSPF to advertise a third-party gateway:

1. Open a static route in Ethernet > Static Rtes.
2. Set Third-Party to Yes.
3. Set the Gateway to the forwarding address.

```
Ethernet
   Static Rtes
      Name=third-party
      Silent=No
      Active=Yes
      Dest=10.212.65.0/24
      Gateway=101.2.3.4
      Metric=3
      Preference=100
      Private=No
      Ospf-Cost=1
      LSA-Type=Type1
      ASE-tag=c00000000
      Third-Party=Yes
```

4. Close the static route.

How OSPF adds RIP routes

When the MultiVoice Gateway establishes an IP routing connection with a caller that does not support OSPF, it imports the AS-external route from the Connection profile and adds it to the routing table. The MultiVoice Gateway does not have to run RIP to learn these routes. RIP should be turned off when the MultiVoice Gateway is running OSPF.

To enable OSPF to add the RIP-v2 routes to its routing table, configure RIP-v2 normally in the Connection profile. OSPF will import all RIP routes as Type-2 ASEs. The reason that RIP routes are imported with Type-2 metrics by default is that RIP metrics are not directly comparable to OSPF metrics. To prevent OSPF from interpreting RIP metrics, the imported ASE route is assigned a Type-2 metric, which means that it is so large compared to OSPF costs that the metric can be ignored.

Route preferences

Route preferences provide additional control over which types of routes take precedence over others. They are necessary in a router that supports multiple routing protocols, largely because RIP metrics are not comparable with OSPF metrics.

For each IP address and subnet-mask pair, the routing table holds one route per protocol, where the protocols are assigned preferences as follows:

- Connected routes, such as Ethernet, have Preference=0.
- Routes learned from ICMP Redirects have Preference=30.
- Routes placed in the table by SNMP MIB II have Preference=100.
- Routes learned from OSPF have a default of Preference=10. You can modify the default in Ethernet > Mod Config > Route Pref.
- Routes learned from RIP have a default of Preference=100. You can modify the default in Ethernet > Mod Config > Route Pref.

- A statically configured IP Route has a default of Preference=100. You can modify the default in the IP Route profile.

When choosing which routes should be put in the routing table, the router first compares the Preference values, preferring the lowest number. If the Preference values are equal, the router compares the Metric field, and uses the route with the lowest Metric.

If multiple routes exist for a given address and netmask pair, the route with the lowest Preference is best. If two routes have the same Preference, the lower Metric is better. The best route by these criteria is the one actually used by the router. The others remain latent or *hidden*, in case the best route is removed.

On Ethernet, the route preferences also include ASE-type and ASE-tag information for routes learned from RIP. These values affect all RIP information learned across the Ethernet. To change the route preferences on Ethernet:

1 Open Ethernet > Mod Config > Route Pref.

2 Modify the parameters to adjust Preference values. For example, to assign static routes the same Preference value as those learned from OSPF:

```
Ethernet
   Mod Config
      Route prefs...
         Static Preference=10
         Rip Preference=100
         RipAseType=Type2
         Rip Tag=c8000000
         OSPF Preference=10
```

Or, to change RIP metrics to Type-1:

```
Ethernet
   Mod Config
      Route prefs...
         Static Preference=100
         Rip Preference=100
         RipAseType=Type1
         Rip Tag=c8000000
         OSPF Preference=10
```

3 Close the Ethernet profile.

Monitoring OSPF

The terminal-server command-line interface provides commands for monitoring OSPF in the MultiVoice Gateway. To display the options, invoke the terminal-server interface (System > Sys Diag > Term Serv) and enter the Show OSPF command. For example:

```
ascend% show ospf ?

show ospf ?              Display help information
show ospf errors         Display OSPF errors
show ospf areas          Display OSPF areas
show ospf general        Display OSPF general info
show ospf interfaces     Display OSPF interfaces
show ospf lsdb           Display OSPF link-state DB
show ospf lsa            Display OSPF link-state advertisements
show ospf nbrs           Display OSPF neighbors
```

```
show ospf rtab          Display OSPF routing tab
show ospf io            Display OSPF io
```

Displaying OSPF errors

To display OSPF errors, enter the Show ISPF Errors command. For example:

```
ascend% show ospf errors

ERRORS from:                          boot
  0: IP: Bad OSPF pkt type              0: IP: Bad IP Dest
  0: IP: Bad IP proto id                1: IP: Pkt src = my IP addr
  0: OSPF: Bad OSPF version             0: OSPF: Bad OSPF checksum
  0: OSPF: Bad intf area id             0: OSPF: Area mismatch
  0: OSPF: Bad virt link info           0: OSPF: Auth type != area type
  0: OSPF: Auth key != area key         0: OSPF: Packet is too small
  0: OSPF: Packet size > IP length      0: OSPF: Transmit bad
  0: OSPF: Received on down IF          0: Hello: IF mask mismatch
  0: Hello: IF hello timer mismatch     0: Hello: IF dead timer mismatch
0: Hello: Extern option mismatch        0: Hello: Nbr Id/IPaddr confusion
0: Hello: Unknown Virt nbr              0: Hello: Unknown NBMA nbr
0: DD: Unknown nbr                      0: DD: Nbr state low
0: DD: Nbr's rtr = my rtrid             0: DD: Extern option mismatch
0: Ack: Unknown nbr                     0: Ack: Nbr state low
0: Ls Req: Nbr state low                0: Ls Req: Unknown nbr
0: Ls Req: Empty request                0: LS Req: Bad pkt
0: LS Update: Nbr state low             0: Ls Update: Unknown nbr
0: Ls Update: Newer self-gen LSA        0: Ls Update: Bad LS chksum
0: Ls Update: less recent rx            0: Ls Update: Unknown type
```

The output lists all error messages related to OSPF, with each message preceded by the number of times it has been generated since the MultiVoice Gateway powered up. Immediately following the number is a field indicating the packet type:

- `IP`—IP packets
- `OSPF`—OSPF packets
- `Hello`—Hello packets
- `DD`—Database Description packets, which are exchanged periodically between neighbors
- `Ack`—Every DD packet must be acknowledged
- `LS Req`—Link-state request (a request for an updated database)
- `LS Update`—An exchange to update databases

Displaying OSPF areas

To display information about OSPF areas, enter the Show OSPF Areas command. For example:

```
ascend% show ospf areas

Area ID: 0.0.0.0
Auth Type: Simple Passwd  Import ASE: On  Spf Runs: 23
Local ABRs: 0  Local ASBRs: 5  Inter LSAs: 7  Inter Cksum sum:
0x2ee0e
```

The output includes the following fields:

Field	Description
Area ID	Specifies the area number in dotted-decimal format.
Auth Type	Type of authentication, simple or null.
Import ASE	Relates to the way routes are calculated, in effect, it specifies whether the router is an ABR or not. This functionality is always ON in the MultiVoice Gateway.
Spf Runs	How many times the SPF calculation was run. The calculation is performed every time the router notes a topology change or receives an update from another router.
Local ABRs	Number of ABRs the router knows about and the number of areas. The number 0 means that the router knows about the backbone area only.
Local ASBRs	Number of ASBRs the router knows about.
Inter LSAs	Number of entries in the link-state database.
Inter Cksum sum	Checksum that is used to note that a database has changed.

Displaying OSPF general information

To display general information about OSPF, enter the Show OSPF General command. For example:

```
ascend% show ospf general

Rtr ID: 10.5.2.154
    Status: Enabled Version: 2 ABR: Off ASBR: On
    LS ASE Count: 8 ASE Cksum sum: Ox4c303 Tos Support: TOS 0 Only
    New LSA Originate Count: 13  Rx New LSA Count: 498
```

Field	Description
Rtr ID field	Contains the MultiVoice Gateway IP address (the IP address assigned to the MultiVoice Gateway Ethernet interface).
Status	Shows whether OSPF is enabled or disabled.
Version	Version of the OSPF protocols running.
ABR	Can be On or Off, depending on where the MultiVoice Gateway is situated on the network. If ABR is On, the MultiVoice Gateway performs additional calculations related to external routes.
ASBR	Always On in the MultiVoice Gateway. Although the MultiVoice Gateway cannot function as an IGP gateway, it does import external routes— for example, when it establishes a WAN link with a caller that does not support OSPF—and the ASBR calculations are always performed.
LS ASE	Count number of link-state database entries that are external.
ASE Cksum sum	Checksum that is used to note that ASE routes in the database have changed.
TOS Support	Level of TOS support in the router.

Field	Description
New LSA Originate Count	Number of LSAs this router created.
Rx New LSA Count	Number of LSAs this router received from other OSPF routers.

To display the OSPF interfaces, enter the Show OSPF Interfaces command. For example:

```
ascend% show ospf interfaces
Area      IP Address  Type  State    Cost Pri DR           BDR
-------------------------------------------------------------------
0.0.0.0   10.5.32.154 Bcast BackupDR 1    5   10.5.2.155   10.5.2.154
0.0.0.0   10.5.32.154 PtoP  2-Way    10   5   None         None
0.0.0.0   10.5.32.154 PtoP  2-Way    10   5   None         None
```

Field	Description
Area	Area ID (0.0.0.0 is the backbone).
IP Address	Address assigned to the interface. In the MultiVoice Gateway, the IP address is always the address assigned to the Ethernet interface. To identify WAN links, use the Type and Cost fields.
Type	Can be broadcast or point-to-point. WAN links are point-to-point.
State	How far along the router is in the process of electing a DR or BDR. The state can be `1-way` (indicating that the election process has begun), `2-way` (indicating that the router has received notification), `BackupDR`, or `DR`.
Cost	Metric assigned to the link. The default cost for Ethernet is 1.
Pri	Designated router election priority assigned to the MultiVoice Gateway.
DR	The designated router.
BDR	The backup designated router.

Displaying the OSPF link-state database

To display the router's link-state database, enter the Show OSPF LSDB command. For example:

```
ascend% show ospf lsdb
```

Note: You can expand each entry in the link-state database to display additional information about a particular LSA. (For further information, see "Displaying OSPF link-state advertisements" on page 9-21.)

```
LS Data Base:
Area        LS Type Link ID      Adv Rtr      Age  Len Seq #    Metric
-------------------------------------------------------------------------
0.0.0.0      STUB    10.5.2.146    10.5.2.146    3600 24  0        0
0.0.0.0      STUB    10.5.2.154    10.5.2.154    3600 24  0        0
0.0.0.0      STUB    10.5.2.155    10.5.2.155    3600 24  0        0
0.0.0.0      STUB    10.5.2.162    10.5.2.162    3600 24  0        0
0.0.0.0      STUB    10.5.2.163    10.5.2.163    3600 24  0        0
0.0.0.0      RTR     10.5.2.146    10.5.2.146    659  72  8000003e 0
```

```
0.0.0.0      RTR     10.5.2.154    10.5.2.154    950  84  8000000a 0
0.0.0.0      RTR     10.5.2.155    10.5.2.155    940  60  80000005 0
0.0.0.0      RTR     10.5.2.162    10.5.2.162    980  84  8000003b 0
0.0.0.0      RTR     10.5.2.163    10.5.2.163    961  60  80000005 0
0.0.0.0      NET     10.5.2.155    10.5.2.155    940  32  80000003 0
0.0.0.0      NET     10.5.2.163    10.5.2.163    961  32  80000003 0
0.0.0.0      ASE     10.5.2.16     10.5.2.163    18   36  80000098 3
0.0.0.0      ASE     10.5.2.18     10.5.2.163    546  36  80000004 10
0.0.0.0      ASE     10.5.2.144    10.5.2.146    245  36  80000037 1
0.0.0.0      ASE     10.5.2.152    10.5.2.154    536  36  80000006 1
0.0.0.0      ASE     10.5.2.152    10.5.2.155    526  36  80000004 1
0.0.0.0      ASE     10.5.2.152    10.5.2.163    18   36  80000097 9
0.0.0.0      ASE     10.5.2.155    10.5.2.163    17   36  80000097 9
0.0.0.0      ASE     10.5.2.160    10.5.2.162    568  36  80000037 1
```

The output includes the following fields:

Field	Description
Area field	Area ID.
LS Type	Type of link as defined in RFC 1583: Type 1 (RTR) are router-LSAs that describe the collected states of the router's interfaces. Type 2 (NET) are network-LSAs that describe the set of routers attached to the network. Types 3 and 4 (STUB) are summary-LSAs that describe point-to-point routes to networks or AS boundary routers. Type 5 (ASE) are AS-external-LSAs that describe routes to destinations external to the Autonomous System. A default route for the Autonomous System can also be described by an AS-external-LSA.
Link ID	Target address of the route.
Adv Rtr	Address of the advertising router.
Age	Age of the route in seconds.
Len	Length of the LSA.
Seq #	Number that begins with 80000000 and increments by one for each LSA received.
Metric	Cost of the link, not of a route. The cost of a route is the sum of all intervening links, including the cost of the connected route.

Displaying OSPF link-state advertisements

To display additional information about an LSA in the link-state database, first display the database as described in the preceding section. Then specify an LSA to expand. Use the following format:

```
show ospf lsa area ls-type ls-id adv-rtr
```

This command requires that you include the first four fields of the LSA as listed in the database. You can select the first four fields and paste them in after typing the command. For

example, to display an expanded view of the last entry in the link-state database shown in the previous section:

```
ascend% show ospf lsa 0.0.0.0 ase 10.5.2.160 10.5.2.162

LSA  type: ASE ls id: 10.5.2.160 adv rtr: 110.5.2.162 age: 568
           len: 36 seq #: 80000037 cksum: 0xfffa
           Net mask: 255.255.255.255 Tos 0 metric: 10 E type: 1
           Forwarding Address: 0.0.0.0 Tag: c0000000
```

Displaying OSPF neighbors

To display adjacencies, enter the Show OSPF Nbrs command. For example:

```
ascend% show ospf nbrs

Area       Interface     Router Id     Nbr IP Addr   State      Mode
Pri
-------------------------------------------------------------------------
0.0.0.0    10.5.2.154    10.5.2.155    10.5.2.155    Full       Slave  5
0.0.0.0    10.5.2.154    10.5.2.146    10.5.2.146    Full       Master 5
0.0.0.0    10.5.2.154    10.5.2.162    10.5.2.162    Full       Slave  5
```

The output contains the following fields:

Field	Description
Area	Area ID.
Interface	Address assigned to the interface. In the MultiVoice Gateway, the IP address is always the address assigned to the Ethernet interface.
Router Id	IP address of the router used to reach a neighbor. This is often the same address as the neighbor itself.
Nbr IP Addr	IP address of the neighbor.
State	State of the link-state database exchange. `Full` means that the databases are fully aligned between the MultiVoice Gateway and its neighbor.
Mode	Whether the neighbor is functioning in master or slave mode. The master sends Database Description packets (polls) which are acknowledged by Database Description packets (responses) sent by the slave.
Pri	Designated router election priority assigned to the MultiVoice Gateway.

Displaying the OSPF routing table

To view the OSPF routing table, type:

```
ascend% show ospf rtab

SPF algorithm run 24 times since boot
Dest          D_mask          Area    Cost E Path Nexthop AdvRtr
-------------------------------------------------------------------------
Nets:
10.5.2.163   255.255.255.248  0.0.0.0  10  3 EXT  10.5.2.163 10.5.2.163
10.5.2.163   255.255.255.255  0.0.0.0  20  0 EXT  10.5.2.163 10.5.2.163
10.5.2.146   255.255.255.248  0.0.0.0  20  1 EXT  10.5.2.154 10.5.2.146
```

```
10.5.2.146   255.255.255.255  0.0.0.0  20  0 STUB 10.5.2.154 10.5.2.146
10.5.2.155   255.255.255.248  0.0.0.0  10  0 INT  10.5.2.154 10.5.2.155
10.5.2.154   255.255.255.255  0.0.0.0  21  0 STUB 10.5.2.163 10.5.2.154
10.5.2.155   255.255.255.255  0.0.0.0  20  9 STUB 10.5.2.155 10.5.2.155
10.5.2.163   255.255.255.248  0.0.0.0  11  1 INT  10.5.2.163 10.5.2.163
10.5.2.162   255.255.255.255  0.0.0.0  20  0 STUB 10.5.2.163 10.5.2.162
10.5.2.163   255.255.255.255  0.0.0.0  10  0 STUB 10.5.2.163 10.5.2.163
```

The output contains the following fields:

Field	Description
Dest	Destination address.
D_mask	Destination netmask.
Area	Area ID.
Cost	Cost of the route.
E	Cost of the link. (The cost of a route is the sum of the cost of each intervening link, including the cost to the connected route.)
Path	Type of link: EXT (exterior), INT (interior), or STUB (a default).
Next hop	Target address from this router.
Adv Rtr	Advertising router. Sometimes a router will advertise routes for which it is not the gateway.

Displaying OSPF protocol i/o

To display information about packets sent and received by the OSPF protocol, enter the Show OSPF IO command. For example:

```
ascend% show ospf io

IO stats from:                        boot
>> RECEIVED:
       0: Monitor request
     785: Hello
      13: DB Description
       6: Link-State Req
    1387: Link-State Update
      64: Link-State Ack
>> SENT:
     794: Hello
      15: DB Description
       6: Link-State Req
    1017: Link-State Update
     212: Link-State Ack
```

MultiVoice Gateway System Administration

10

Introduction to MultiVoice Gateway administration

This chapter describes administrative configurations and commands, and SNMP administration.

Administrative configurations are system- or network-wide configurations related to the unit itself. They are described in “System and Ethernet profile configurations” on page 10-3.

Administrative commands are terminal-server commands related to managing the system, its networks, and its calls. This chapter focuses on those related to the system itself, and tells you where to find information about the network and connection-oriented commands.

For SNMP administration, MultiVoice Gateway configurations control which classes of events will generate traps to be sent to an SNMP manager and which SNMP managers may access the unit. The configurations also control how community strings protect that access. This chapter shows you how to set up the unit to work with SNMP.

Note: You can manage the MultiVoice Gateway from your workstation by establishing a Telnet session and logging in with sufficient administrative privileges.

Where to find additional administrative information

The following administrative topics are documented in a separate guide or supplement:

Topic	Description
Machine Interface Format (MIF) interface	MIF is an Ascend-specific language that provides an alternative configuration interface for Ascend units. You can use a command line or write a MIF program that sets Ascend parameters, rather than use the configuration menus to change one parameter after another. MIF programs provide a batch-processing method of changing a configuration or performing a series of actions. For MIF instructions, see the *MAX MIF Supplement*.
Sys Diag and Line Diag commands	The Sys Diag commands enable you to reset the device, save or restore configuration information, and perform other administrative functions. The Line Diag commands enable loopbacks and other diagnostics on WAN lines. For details, see the *MAX Reference Guide*. You can also reset the MultiVoice Gateway, set the configuration state of a T1 line, and obtain configuration information from RADIUS by using SNMP. For details, see the Ascend Enterprise MIB. You can download the most up-to-date version of the Ascend Enterprise MIB by logging in as *anonymous* to ftp.ascend.com. (No password is required.)
DO commands	Pressing Ctrl-D in the VT100 interface displays the DO menu, which contains commands for changing security levels in the MultiVoice Gateway, or for manually dialing or clearing a call. For details, see the *MAX Reference Guide*.
Status windows	The status windows in the VT100 interface provide information about what is currently happening in the MultiVoice Gateway. For details, see the *MAX Reference Guide*.
Troubleshooting	For troubleshooting tips, see Appendix A, “Troubleshooting.”

Activating administrative permissions

Before you can use the administrative commands and profiles, you must log in as the superuser by activating a Security profile that has sufficient permissions, such as the Full Access profile. To do so:

1 Press Ctrl-D to open the DO menu, then press P (or select P=Password).

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

2 In the list of Security profiles that opens, select Full Access. The MultiVoice Gateway prompts you for the Full Access password:

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

 Press > to accept
```

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

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

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

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

Note: The default password for the Full Access login is `Ascend`. The first task you should perform after logging in as the superuser is to assign a new password to the profile.

System and Ethernet profile configurations

This section describes the system-administration configurations shown in the following example:

```
System
   Sys Config
      Name=gateway-1
      Location=east-bay
      Contact=thf
      Date=2/20/97
      Time=10:00:29
      Term Rate=9600
      Console=Standard
      Remote Mgmt=Yes
      Max Dialout Time=20
      Parallel Dial=5
      Single Answer=Yes
      Sub-adr=None
      Serial=0
      Lan=0
      DM=0
      Use Trunk Grps=No
      Excl Routing=No
      Auto Logout=No
      Idle Logout=0
      DS0 Min Rst=Off
      Max DS0 Mins=N/A
      High BER=10 ** -3
      High BER Alarm=No
      No Trunk Alarm=No
      Edit=00-000
      Status 1=10-100
```

```
            Status 2=10-200
            Status 3=90-100
            Status 4=00-200
            Status 5=90-300
            Status 6=90-400
            Status 7=20-100
            Status 8=20-200


      Ethernet
         Mod Config
            Log...
               Syslog=Yes
               Log Host=10.65.212.12
               Log Port=514
               Log Facility=Local0
               Log CallInfo=None
               Log Call Progress=Yes
```

For complete information about these parameters, see the *MAX Reference Guide.* For background information about additional parameters that appear in the System profile, see Chapter 5, “Configuring the WAN Interfaces.”

The system name

The system name can contain up to 16 characters. Keeping the name simple is a good idea (do not include special characters), because it is used in negotiating bridged PPP, AIM, and BONDING connections.

Specifying the unit’s location and the contact for problems

The Location and Contact fields are SNMP readable and adjustable, and should indicate the MultiVoice Gateway unit’s location and the person to contact about any problems, respectively. You can enter up to 80 characters.

Setting the system date and time

The Date and Time parameters set the system date and time. If you are using Simple Network Time Protocol (SNTP), the MultiVoice Gateway can maintain its date and time by accessing the SNTP server. (For more information, see Chapter 8, “Configuring IP Routing.”)

Console and term rate

The Console parameter enables you to change the configuration interface. For example, you can change it from Standard to MIF. If you set it to MIF, the Machine Interface Format interface comes up when you power up the MultiVoice Gateway. `Limited` brings up simplified menus for operation with the serial host ports (but not for bridging and routing). (For details, see the *MAX MIF Supplement*.)

You should also verify that the data rate of your terminal emulation program is set to 9600 baud or lower and that the Term-Rate parameter in the System profile is also set to 9600. Higher speeds might cause transmission errors.

Logging out the console port

The Auto Logout parameter specifies whether to log out and go back to default privileges upon loss of DTR from the serial port. Idle Logout specifies the number of minutes an administrative login can remain inactive before the MultiVoice Gateway logs out and hangs up.

Setting the call attempt time out

The Max Dailout Time parameter specifies the amount of time, in seconds, that a MultiVoice Gateway waits for a destination Gateway to answer an outgoing call. If no connection is established when time expires, the Gateway will drop the call attempt. This allows you to reduce the number of failed call attempts, resulting from changing network conditions, by adjusting the time interval a MultiVoice Gateway waits for an answer.

You may specify a time interval between `1` and `255` seconds. A `0` entry causes the MultiVoice Gateway to use the default setting of 20 seconds. Changing the value for Max Dialout Time requires a reboot of the MultiVoice Gateway.

Setting a high-bit-error alarm

High BER specifies the maximum bit-error rate for any PRI line. The bit-error rate consists of the number of bit errors that occur per second. The number that comes after the double asterisks specifies the power of 10 for the current ratio of error bits to total bits.

High BER Alarm specifies whether the back-panel alarm relay closes when the bit-error rate exceeds the value specified by the High BER parameter.

Setting an alarm when no trunks are available

No Trunk Alarm specifies whether the back-panel alarm relay closes when all T1 PRI lines (or trunks) go out of service.

Customizing the VT100 interface

The Edit and Status parameters customize the status windows in the vt100 interface so that particular screens appear at start-up. (For details, see the *MAX Reference Guide*.)

Interacting with the syslog daemon to save ASCII log files

The Syslog Log Host and Facility parameters relate to the sending of log messages to `syslogd` running on a UNIX host. To maintain a permanent log of MultiVoice Gateway system events and send Call Detail Reporting (CDR) reports to a host that can record and process them, configure the MultiVoice Gateway to report events to a Syslog host on the local IP network. The host running a `syslog` daemon is typically a UNIX host, but it can also be a Windows system. If the log host is not on the same subnet as the MultiVoice Gateway, the MultiVoice Gateway must have a route to that host, by means of either RIP or a static route.

The Log Facility parameter is used to flag messages from the MultiVoice Gateway. After you set a Log Facility number, you need to configure the `syslog` daemon to write all messages containing that facility number to a particular log file. (That file will be the MultiVoice

Gateway log file.) You may include/exclude call-related messages by changing the values for the Log CallInfo and Log Call Progress parameters.

Examples of administrative configurations

This section uses examples to show how to set basic system parameters and configure the MultiVoice Gateway to interact with `syslog`.

Setting basic system parameters

To configure the system name and other basic parameters in the System profile:

1. Open the System profile.
2. Specify a system name up to 16 characters long, enter the physical location of the MultiVoice Gateway unit, and indicate a person to contact in case of problems:

```
System
   Sys Config
      Name=gateway-1
      Location=east-bay
      Contact=thf
```

3. If necessary, set the system date and time:

```
      Date=3/20/98
      Time=10:00:29
```

4. Specify the data transfer rate of the MultiVoice Gateway Control port:

```
      Term Rate=9600
```

5. Close the System profile.

Configuring the MultiVoice Gateway to interact with `syslog`

To maintain a permanent log of MultiVoice Gateway system events and send Call Detail Reporting (CDR) reports to a host that can record and process them, configure the MultiVoice Gateway to report events to a Syslog host on the local IP network. Note that the Ethernet interface sends out the Syslog reports. To configure the MultiVoice Gateway to send messages to a `syslog` daemon:

1. Open Ethernet > Mod Config > Log.
2. Turn on Syslog.
3. Specify the IP address of the host running the `syslog` daemon.
4. Specify the port at which the `syslog` daemon listens for Syslog messages from this MultiVoice Gateway.
5. Set the log facility level.

```
Ethernet
   Mod Config
      Log...
         Syslog=Yes
         Log Host=10.65.212.12
         Log Port=514
         Log Facility=Local0
         Log CallInfo=None
         Log Call Progress=Yes
```

6 Close the Ethernet profile.

To configure the `syslog` daemon, you need to modify `/etc/syslog.conf` on the log host. This file specifies which action the daemon will perform when it receives messages from a particular log facility number (which represents the MultiVoice Gateway). For example, if you set Log Facility to Local5 in the MultiVoice Gateway, and you want to log its messages in `/var/log/`MultiVoice Gateway, add this line to `/etc/syslog.conf`:

```
local5.info<tab>/var/log/MultiVoice Gateway
```

Note: The `syslog` daemon must reread `/etc/syslog.conf` after it has been changed.

Terminal-server commands

This section describes the commands available in the terminal-server command-line interface. To invoke the terminal-server command-line interface, you must have administrative privileges. (For details, see "Activating administrative permissions" on page 10-2.)

You can open the terminal-server command-line interface by using any of the following methods:

- Select System > Sys Diag > Term Serv, and press Enter.
- Press Ctrl-D to open the DO menu in the Main Edit menu, and select E=Termsrv.
- Enter the following keystroke sequence (Escape key, left square bracket, Escape key, zero) in rapid succession:

  ```
  <Esc> [ <Esc> 0
  ```

If you have sufficient privileges to invoke the command line, you will see the command-line prompt; for example:

```
** Ascend Terminal Server **

ascend%
```

Note: If you have a MAX running Multiband Simulation, you cannot use the following terminal server commands: Close, Ipxping, Open, Resume, Rlogin, Telnet.

Displaying terminal-server commands

To display the list of terminal-server commands, enter a question mark:

```
ascend% ?
```

Or:

```
ascend% help
```

?	Displays help information
help	Displays help information
quit	Closes terminal server session
hangup	Closes terminal server session
test	test <number> frame-count.] [<optional fields>]

local	Go to local mode
remote	remote <station> - This command is not supported on the MultiVoice Gateway
set	Set various items. Type ‘set ?’ for help
show	Show various tables. Type ‘show ?’ for help
iproute	Manage IP routes. Type ‘iproute ?’ for help
dnstab	Displays help information about the DNS table. Type 'dnstab ?' for help
slip	SLIP command - This command is not supported on the MultiVoice Gateway
cslip	Compressed SLIP command - This command is not supported on the MultiVoice Gateway
ppp	PPP command - - This command is not supported on the MultiVoice Gateway
menu	Host menu interface
telnet	telnet [-a|-b|-t] <host-name> [<port-number>]
tcp	tcp <host-name> <port-number>
ping	ping <host-name>
ipxping	ipxping <host-name> - This command is not supported on the MultiVoice Gateway
traceroute	Trace route to host. Type 'traceroute -?' for help
rlogin	rlogin [-l user -ec] <host-name> [-l user]
open	open < modem-number | slot:modem-on-slot > - This command is not supported on the MultiVoice Gateway
resume	resume virtual connect session - This command is not supported on the MultiVoice Gateway
close	close virtual connect session - This command is not supported on the MultiVoice Gateway
kill	terminate session - This command is not supported on the MultiVoice Gateway

Returning to the VT100 menus

The following commands close the terminal-server command-line interface and return the cursor to the VT100 menus.

```
quit                Closes terminal server session
hangup                 "      "       "       "
local               Go to local mode
For example:
```

```
ascend% quit
```

Commands for monitoring networks

The following commands are specific to IP routing connections:

```
iproute             Manage IP routes.  Type 'iproute ?' for help
ping                ping <host-name>
traceroute          Trace route to host.  Type 'traceroute -?' for help
```

(For details of using IProute, Ping, and Traceroute, see Chapter 8, "Configuring IP Routing.")

Commands for use by terminal-server users

The following commands must be enabled for use in Ethernet > Mod Config > TServ Options. If they are enabled, login users can initiate sessions by invoking the commands in the terminal-server interface.

```
menu                Host menu interface
telnet              telnet [ -a|-b|-t ] <host-name> [ <port-number> ]
rlogin              rlogin [ -l user -ec ] <host-name> [ -l user ]
tcp                 tcp <hostname> <port-number>
```

These commands initiate a session with a host or modem, or toggle to a different interface that displays a menu selection of Telnet hosts.

SLIP, CSLIP, and PPP commands

The Serial Line IP (SLIP), Compressed SLIP (CSLIP), and PPP sessions, respectively, from the terminal-server command line.

Menu command

You can enter the Menu command to invoke the terminal-server menu mode, which lists up to four hosts. They can be either Telnet hosts or raw TCP hosts. You can mix Telnet and raw TCP hosts in a menu.

Specifying Telnet hosts

The Menu command invokes the terminal-server menu mode, which lists up to four Telnet hosts as configured in Ethernet > Mod Config > TServ Options. For example:

```
Up to 16 lines of up to 80 characters each
will be accepted. Long lines will be truncated.
Additional lines will be ignored


        1. host1.abc.com
        2. host2.abc.com
        3. host3.abc.com
        4. host4.abc.com
          Enter Selection (1-4, q)
```

To return to the command line, press 0 (zero). Terminal-server security must be set up to allow the operator to *toggle* between the command line and menu mode, or the Menu command has no effect.

Specifying raw TCP hosts

To specify IP addresses or DNS names of hosts to which you establish a raw TCP connection, proceed as follows:

1. Open the Ethernet > Mod Config > TServ options menu.
2. Select one of the Host # Addr fields and enter the following:

   `rawTcp` *`hostaddress portnumber`*

   rawTcp is the required string that causes the MAX to establish a raw TCP connection when the user chooses this host number. This entry is case-sensitive and must be entered exactly as shown.

   `hostname` can be the DNS name of the host or the IP address of the host. The total number of characters, including the `rawTcp` string, must not exceed 31.

   `portnumber` is the number of the port on which the connection for this host is to be established.
3. Enter a description of the host on the Host # Text field.

Note: You cannot configure raw TCP hosts if you are using a RADIUS server to provide the list of hosts.

Example of configuration combining Telnet hosts and raw TCP hosts

Suppose you configure the following values in the TServ Options menu:

```
Remote Conf=No
Host #1 Addr=10.10.10.1
Host #1 Text=Cleveland
Host #2 Addr=
Host #2 Text=
Host #3 Addr=
Host #3 Text=
Host #4 Addr=rawTcp corp-host 7
Host #4 Text=The Office - port 7
Immed Service=None
Immed Host=N/A
Immed Port=N/A
Telnet Host Auth=No
```

The Terminal-Server menu displays the following text:

```
** Ascend Pipeline Terminal Server **

     1. Cleveland
     2. The Office - port 7

     Enter Selection (1-2,q)
```

If you select 2, the a raw TCP connection is established to the host Corp-Host on port 7.

If a you select 1, the MultiVoice Gateway establishes a Telnet connection to the host 10.10.10.1 on port 23, the default Telnet port.

Telnet command

The Telnet command initiates a login session to a remote host. It uses the following format:

```
telnet [-a|-b|–t] hostname [port-number]
```

If DNS is configured in the Ethernet profile, you can specify a hostname:

```
ascend% telnet myhost
```

If you do not configure DNS, you must specify the host's IP address instead. There are also several options in Ethernet > Mod Config > TServ Options that affect Telnet. For example, if you set Def Telnet to Yes, you can just type a hostname to open a Telnet session to that host:

```
ascend% myhost
```

Another way to open a session is to invoke Telnet first, then enter the Open command at the Telnet prompt. For example:

```
ascend% telnet
telnet> open myhost
```

The Telnet prompt is `telnet>`. When you see that prompt, you can enter any of the Telnet commands described in "Telnet session commands" on page 10-12. You can quit the Telnet session at any time by typing `quit` at the Telnet prompt:

```
telnet> quit
```

Note: During an open Telnet connection, press Ctrl-] to display the `telnet>` prompt and the Telnet command-line interface. Any valid Telnet command returns you to the open session. Note that Ctrl-] does not function in binary-mode Telnet. If you log into the MultiVoice Gateway through Telnet, you might want to change its escape sequence from Ctrl-] to a different setting.

Telnet command arguments

The Telnet command accepts the following arguments:

Argument	Description
hostname	If you configure DNS, you can specify the remote system's *hostname*. Otherwise, hostname must be the IP address of the remote station.
`-a | -b | -t`	Specify ASCII, Binary, or Transparent mode, respectively. A specification on the command line overrides the setting of the Telnet Mode parameter. In ASCII mode, the MultiVoice Gateway uses standard seven-bit mode. In Binary mode, the MAX tries to negotiate eight-bit Binary mode with the server at the remote end of the connection. In Transparent mode, the user can send and receive binary files, and use eight-bit file transfer protocols, without having to be in Binary mode.
port-number	Port to use for the session. The default is 23, the well-known port for Telnet.

Telnet session commands

The commands in this section can be typed at the Telnet prompt during an open session. To display the Telnet prompt during an active login to the specified host, press Ctrl-] (hold down the Control key and type a right-bracket). To display information about Telnet session commands, use the Help or ? command. For example:

```
telnet> ?
```

To open a Telnet connection after invoking Telnet, use the Open command. For example:

```
telnet> open myhost
```

To send standard Telnet commands such as *Are You There* or *Suspend Process*, use the Send command. For example:

```
telnet> send susp
```

For a list of Send commands and their syntax, enter the Send command with a question mark:

```
telnet> send ?
```

To set special characters for use during the Telnet session, use the Set command. For example:

```
telnet> set eof ^D
```

To display current settings:

```
telnet> set all
```

To see a list of Set commands:

```
telnet> set ?
```

To quit the Telnet session and close the connection, enter the Close or Quit command:

```
telnet> close
```

Telnet error messages

The MultiVoice Gateway generates an error message for any condition that causes the Telnet session to fail or terminate abnormally. The following error messages can appear:

- `no connection: host reset` (Destination host reset the connection.)
- `no connection: host unreachable` (Destination host is unreachable.)
- `no connection: net unreachable` (Destination network is unreachable.)
- `Unit busy. Try again later.` (Host already has open the maximum number of concurrent Telnet sessions.)

Rlogin command

The Rlogin command initiates a login session to a remote host. It uses the following format:

`rlogin` `rlogin [-ec] hostname [-l username]`

If you configure DNS, you can specify a hostname such as:

```
ascend% rlogin myhost
```

If DNS has not been configured, you must specify the host's IP address instead. Rlogin must also be enabled in Ethernet > Mod Config > TServ Options. The arguments to the Rlogin command are:

Argument	Description
hostname	If you configure DNS, you can specify the remote system's hostname. Otherwise, `hostname` must be the IP address of the remote station.
`-e char`	Sets the escape character to `char`. For example: `rlogin -e$ 10.2.3.4` The default for `char` is a tilde (~).

-l username	Specifies that you log into the remote host as `username`, rather than as the name you used to log into the terminal server. You can specify the `-l` option before or after `hostname`. For example, the following two lines perform identical functions:
	`rlogin -l jim 10.2.3.4`
	`rlogin 10.2.3.4 -l jim`
	If you did not log into the terminal-server through RADIUS or TACACS, you can use this option on the command line instead of being prompted for it by the remote host.

To terminate the remote login, use the Exit command at the remote system's prompt. Or you can press the Enter key and then type the escape character and a period.:

For example, to terminate a remote login that was initiated with the default escape character (a tilde), press Enter and then type a tilde followed by a period.

TCP command

The TCP command initiates a login session to a remote host. It uses the following format:

```
tcp hostname port-number
```

where:

- `hostname` is the IP address of the remote station or, if you have configured DNS, the remote system's hostname.
- `port-number` is port to use for the session. The port number typically indicates a custom application that runs on top of the TCP session. For example, port number 23 starts a Telnet session. However, terminating the Telnet session does not terminate the raw TCP session.

For example:

```
ascend% tcp myhost
```

When the raw TCP session starts running, the MultiVoice Gateway displays the word `connected`. You can now use the TCP session to transport data by running an application on top of TCP. You can hang up the device at either end to terminate the raw TCP session. If you are using a remote terminal-server session, ending the connection also terminates raw TCP.

If a raw TCP connection fails, the MultiVoice Gateway returns one of the following error messages:

`Cannot open session:` *hostname port-number*

If you entered an invalid or unknown value for *hostname*, you entered an invalid value for *port-number*, or if you failed to enter a port number, one of the following error messages appears:

- `no connection: host reset` (Destination host reset the connection.)
- `no connection: host unreachable` (Destination host is unreachable.)
- `no connection: net unreachable` (Destination network is unreachable.)

Administrative commands

The following commands are related to system administration:

```
test                test <number> frame-count> ] [ <optional fields> ]
set                 Set various items. Type 'set ?' for help
show                Show various tables. Type 'show ?' for help
```

Test command

To run a self-test in which the MultiVoice Gateway calls itself, the MultiVoice Gateway must have two open channels: one for placing the call, and the other for receiving it. The Test command has the following format:

`test` *phonenumber* `[`*frame-count*`] [`*optional fields*`]`

where:

- *phonenumber* is the phone number of the channel receiving the test call. It can include the numbers 0 through 9 and the characters ()[]-, but cannot include spaces.
- *frame-count* is the number of frames to send during the test (a number from 1 to 65535.) The default is 100.

The optional fields are:

Field	Usage
`data-svc=`*data-svc*	Enter a data service identical to any of the values available for the Data Svc parameter of the Connection profile. For a list of valid values, see the *MAX Reference Guide*. If you do not specify a value, the default value is the one specified for the Data Svc parameter.

Field	Usage
`call-by-call=`*T1-PRI-service*	Enter any value available to the Call-by-Call parameter of the Connection profile. The Call-by-Call parameter specifies the PRI service that the MultiVoice Gateway uses when placing a PPP call. For a list of valid values, see the *MAX Reference Guide*. If you do not specify a value, the default is as specified for the Call-by-Call parameter.
`primary-number-type=`*AT&T-switch*	Specify any value available to the PRI # Type parameter of the Connection profile. The PRI # Type parameter specifies an AT&T switch. For a list of valid values, see the *MAX Reference Guide*. If you do not specify a value, the default value is the one specified for the PRI # Type parameter.
`transit-number=IEC`	Specify any value available to the Transit # parameter of the Connection profile. The Transit # parameter specifies the U.S. Interexchange Carrier (IEC) you use for long distance calls over a PRI line. For a list of valid values, see the *MAX Reference Guide*. If you do not specify a value, the default is as specified for the Transit # parameter.

For example:

```
ascend% test 555-1212
```

You can press Ctrl-C at any time to terminate the test. While the test is running, the MultiVoice Gateway displays the status. For example:

```
calling...answering...testing...end
200 packets sent, 200 packets received
```

If you enable trunk groups on the MultiVoice Gateway, you can specify the outgoing lines used in the self test. If you do not, the MultiVoice Gateway uses the first available T1 (or E1) line. For example, if you assign the trunk group 7 to line 1 on a Net/BRI module and a preceding *9* is required by your PBX to make an outgoing call, the following command places the outgoing call on line 1 of the Net/BRI module:

```
ascend% test 7-9-555-1212
```

The MultiVoice Gateway generates an error message for any condition that causes the test to terminate before sending the full number of packets. Possible error messages are as follows:

Message	Explanation
`bad digits in phone number`	The phone number you specified contained a character other than the numbers 0 through 9 and the characters `()[]-`.

Message	Explanation
`call failed`	The MultiVoice Gateway did not answer the outgoing call. This error can indicate a wrong phone number or a busy phone number. Use the Show ISDN command to determine the nature of the failure.
`call terminated` *N1* `packets sent` *N2* `packets received`	This message indicates the number of packets sent (*N1*) and received (*N2*).
`cannot handshake`	The MultiVoice Gateway answered the outgoing call, but the two sides did not properly identify themselves. This error can indicate that the call was routed to the wrong MultiVoice Gateway module, or that the phone number was incorrect.
`frame-count must be in the range 1-65535`	The number of frames requested exceeded 65535.
`no phone number`	You did not specify a phone number on the command line.
`test aborted`	The test was terminated (Ctrl-C).
`unit busy`	You attempted to start another self-test when one was already in progress. You can run only a single self-test at a time.
`unknown items on command line`	The command-line contained unknown items. Inserting one or more spaces in the telephone number can generate this error.
`unknown option` *option*	The command-line contained the option indicated by *option*, which is invalid.
`unknown value` *value*	The command-line contained the value indicated by *value*, which is invalid.
`wrong phone number`	A device other than the MultiVoice Gateway answered the call. Therefore, the phone number you specified was incorrect.

Set command

The Set command takes several arguments. The ? argument lists them:

```
ascend% set ?

set ?               Display help information
set all             Display current settings
set term            Sets the telnet/rlogin terminal type
set password        Enable dynamic password serving
set fr              Frame Relay datalink control
set circuit         Frame Relay Circuit control
```

The Set All command displays current settings. For example:

```
ascend% set all

term = vt100
dynamic password serving = disabled
```

To specify a terminal type other than the default VT100, use the Set Term command.

The Set Password command puts the terminal server in password mode, where a third-party ACE or SAFEWORD server at a secure site can display password challenges dynamically in the terminal-server interface. When the terminal server is in password mode, it passively waits for password challenges from a remote ACE or SAFEWORD server. This command applies only when using security card authentication. To enter password mode:

```
ascend% set password
Entering Password Mode...

[^C to exit] Password Mode>
```

To return to normal terminal-server operations and thereby disable password mode, press Ctrl-C.

Note: Note that each channel of a connection to a secure site requires a separate password challenge, so for multichannel connections to a secure site, you must leave the terminal server in password mode until all channels have been established. The APP Server utility is an alternative way to allow users to respond to dynamic password challenges obtained from hand-held security cards. (For discussion of dynamic password serving, see the *MAX Security Supplement*.)

The Set FR commands enable you to bring down the nailed connection specified in the named Frame Relay profile. The connection will be reestablished within a few seconds. With the Set Circuit commands, you can activate or deactivate a Frame Relay circuit. (For details, see Chapter 7, “Configuring Frame Relay.”)

Show command

The Show command takes several arguments. The `?` argument lists them:

```
ascend% show ?
```

show ?	Display help information
show arp	Display the arp cache
show icmp	Display ICMP information
show if	Display Interface info. Type ‘show if ?’ for help
show ip	Display IP information. Type 'show ip ?' for help.
show udp	Display UDP information. Type 'show udp ?' for help
show igmp	Display IGMP information. Type 'show igmp ?' for help.
show mrouting	Display MROUTING information. Type 'show mrouting ?' f ?’
show ospf	Display OSPF information. Type 'show ospf ?' for help.
show tcp	Display TCP information. Type 'show tcp ?' for help
show dnstab	Display local DNS table. Type ‘show dnstab ?’ for help
show netware	Display IPX information. Type 'show netware ? ' for help
show isdn	Display ISDN events. Type 'show isdn <line number’ for help
show fr	Display Frame relay info. Type 'show fr ?' for help
show pools	Display the assign address pools
show modems	Display status of all modems
show calls	Display status of calls
show pad	Display X25/PAD information
show uptime	Display system uptime
show revision	Display system revision
show v.110s	Display status of all v.110 cards
show users	Display concise list of active users
show x25	Display status of X.25 stack

Note: Many of the Show commands are specific to a particular type of usage, such as IP routing or OSPF, and are described in the relevant chapter.

Show commands related to network information

The following Show commands are related to monitoring protocols and other network-specific information:

Table 10-1.Network-specific Show commands

Show command	Where described
`show arp`	See Chapter 8, “Configuring IP Routing.”
`show icmp`	See Chapter 8, “Configuring IP Routing.”
`show if`	See Chapter 8, “Configuring IP Routing.”
`show ip`	See Chapter 8, “Configuring IP Routing.”
`show udp`	See Chapter 8, “Configuring IP Routing.”
`show ospf`	See Chapter 9, “Configuring OSPF Routing.”
`show tcp`	See Chapter 8, “Configuring IP Routing.”
`show dnstab`	See Chapter 8, “Configuring IP Routing.”
`show fr`	See Chapter 7, “Configuring Frame Relay.”

Show ISDN

The Show ISDN command enables the MultiVoice Gateway to display the last 20 events that have occurred on the specified ISDN line. Enter the command in this format:

`show isdn` ***`line-number`***

where ***`line-number`*** is the number of the ISDN line. (For discussion of how lines are numbered, see Chapter 5, “Configuring the WAN Interfaces.”) For example, to display information about the left-most built-in WAN port, specify line 0 (zero):

```
ascend% show isdn 0
```

The MultiVoice Gateway responds with one or more of the following messages:

```
PH: ACTIVATED
PH: DEACTIVATED
DL: TEI ASSIGNED (BRI interfaces only)
DL: TEI REMOVED (BRI interfaces only)
NL: CALL REQUEST
NL: CLEAR REQUEST
NL: ANSWER REQUEST
NL: CALL CONNECTED
NL: CALL FAILED/T303 EXPIRY
NL: CALL CLEARED/L1 CHANGE
NL: CALL REJECTED/OTHER DEST
NL: CALL REJECTED/BAD CALL REF
NL: CALL REJECTED/NO VOICE CALLS
```

```
NL: CALL REJECTED/INVALID CONTENTS
NL: CALL REJECTED/BAD CHANNEL ID
NL: CALL FAILED/BAD PROGRESS IE
NL: CALL CLEARED WITH CAUSE
```

In some cases, the message can include a phone number (prefixed by #), a data service (suffixed by K for Kbps), a channel number, TEI assignment, and cause code. For example, the following information might appear:

```
PH: ACTIVATED
NL: CALL REQUEST: 64K, #442
NL: CALL CONNECTED: B2, #442
NL: CLEAR REQUEST: B1
NL: CALL CLEARED WITH CAUSE 16 B1 #442
```

For information about each of the messages that can appear, see the CCITTT Blue Book Q.931 or other ISDN specifications.

Show Calls

The Show Calls command displays information about active calls on a German 1TR6 or Japan NTT switch type. For example:

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

The output includes the following fields:

Field	Description
CallID	An identifier for the call.
CalledPartyID	The telephone number of the answering device (that is, this unit). This ID is obtained from layer 3 protocol messages during call setup.
CallingPartyID	The telephone number of the caller. This ID is obtained from layer 3 protocol messages during call setup.
InOctets	The total number of octets received by the user from the moment the call begins until it is cleared.
OutOctets	The total number of octets sent by the user from the moment the call begins until it is cleared.

Show Uptime

To see how long the MultiVoice Gateway has been running, enter the Show Uptime command. For example:

```
ascend% show uptime
system uptime: up 2 days, 4 hours, 38 minutes, 43 seconds
```

If the MultiVoice Gateway stays up for 1000 consecutive days with no power cycles, the number of days displayed turns over to 0 and begins to increment again.

Show Revision

The Show Revision command displays the software load and version number currently running in the MultiVoice Gateway. For example:

```
ascend% show revision
techpubs-lab-17 system revision: ebiom.m40 5.0A
```

Show Users

To display the number of active sessions, enter the Show Users command. For example:

```
ascend% show users
I Session    Line: Slot: Tx    Rx    Service    Host         User
O ID         Chan  Port  Data  Rate  Type[mpID] Address      Name
O 231849873  1:1   9:1   56K   56K   MPP[1]     10.10.68.2   jdoe
I 231849874  1:3   3:1   28800 33600 Termsrv    N/A          Modem 3:1
O 214933581  1:2   9:2   56K   56K   MPP[1]     10.10.4.9    arwp50
O 214933582  1:6   9:3   56K   56K   MPP[1]     MPP Bundle   arwp50
```

The output contains the following fields:

Field	Description
I/O	Incoming call (I) or Outgoing call (O).
Session ID	Unique session-ID. This is the same as Acct-Session-ID in RADIUS.
Line:Chan	Line and channel on which the session is established.
Slot:Port	Slot and port of the service being used by the session. Can indicate the number of a slot containing a modem card and the modem on that card, or the virtual slot of the MultiVoice Gateway unit's bridge/router. If the slot is virtual, the port number represents a virtual interface to the bridge/router, starting with 1 for the first session of a multichannel session.
Tx Data Rate	Transmit rate in bits per second.
Rx Data Rate	Receive rate in bits per second.
Service Type	Type of session, which can be Termsrv or a protocol name. For MP and MPP, this field shows the bundle ID shared by the calls in a multichannel session. The special values `Initial` and `Login` document the progress of a session. `Initial` identifies sessions that do not yet have a protocol assigned. `Login` identifies Termsrv sessions during the login process.
Host Address	Network address of the host originating the session. For some sessions this field is N/A. For outgoing MPP sessions, only the first connection has a valid network address associated with it. All other connections in the bundle have the network address listed as MPP Bundle.

Field	Description
User Name	Station name associated with the session. Initially, this value is Answer. It is usually replaced with the name of the remote host. For terminal-server sessions it is the login name. Before login completion, this field will show the string `modem x:y` where `x` and `y` are the slot and port of the modem servicing the session.

SNMP administration support

The MultiVoice Gateway supports SNMP on a TCP/IP network. An SNMP management station that uses the Ascend Enterprise MIB can query the MultiVoice Gateway, set some parameters, sound alarms when certain conditions appear in the MultiVoice Gateway, and so forth. An SNMP manager must be running on a host on the local IP network, and the MultiVoice Gateway must be able to find that host through either a static route or RIP.

SNMP has its own password security, which you should set up to prevent reconfiguration of the MultiVoice Gateway from an SNMP station.

Configuring SNMP access security

There are two levels of SNMP security: community strings, which must be known by a community of SNMP managers to access the box, and address security, which denies SNMP access unless it is initiated from a specified IP address. The following example shows the relevant parameters:

```
Ethernet
   Mod Config
      SNMP options...
         Read Comm=Ascend
         R/W Comm Enable=No
         R/W Comm=Secret
         Security=Yes
         RD Mgr1=10.0.0.1
         RD Mgr2=10.0.0.2
         RD Mgr3=10.0.0.3
         RD Mgr4=10.0.0.4
         RD Mgr5=10.0.0.5
         WR Mgr1=10.0.0.11
         WR Mgr2=10.0.0.12
         WR Mgr3=10.0.0.13
         WR Mgr4=10.0.0.14
         WR Mgr5=10.0.0.15
```

(For complete information about each parameter, see the *MAX Reference Guide*.)

Enabling SNMP set commands

R/W Comm Enable disables SNMP Set commands by default. Before you can use an SNMP Set command, you must set R/W Comm Enable to Yes.

Note: Even if you enable R/W Comm, you must still know the read-write community string to use a Set command.

Setting community strings

The Read Comm parameter specifies the SNMP community name for read access (up to 32 characters), and the R/W Comm parameter specifies SNMP community name for read/write access.

Setting up and enforcing address security

If the Security parameter is set to No (its default value), any SNMP manager that presents the right community name will be allowed access. If you set this parameter to Yes, the MultiVoice Gateway checks the source IP address of the SNMP manager and allows access only to those IP addresses listed in the RD MgrN and WR MgrN parameters, each of which specifies up to five host addresses.

Resetting the MultiVoice Gateway and determining whether it has reset

You can use SNMP (`sysReset` object) to reset a MultiVoice Gateway from an SNMP manager. After the Reset command is issued, a one-minute timeout (not modifiable) permits the MultiVoice Gateway to confirm the `set request` before the unit is reset.

Information held in the Ascend Events Group is erased and its values are initialized when the MultiVoice Gateway is reset by software or by toggling the power off and on. The SNMP object `sysAbsoluteStartupTime` is the time in seconds since January 1, 1990, and is not modified. To determine whether the MultiVoice Gateway has actually reset, you can retrieve `sysAbsoluteStartupTime` and compare this value against the previous poll's value for Ascend Events Group variables.

Example of a SNMP security configuration

This example sets the community strings, enforces address security, and prevents write access:

1. Open Ethernet > Mod Config > SNMP Options.
2. Set R/W Comm Enable to Yes.
3. Specify the Read Comm and R/W Comm parameter strings.
4. Set Security to Yes.
5. Specify up to five host addresses in the RD MgrN parameters. Leave the WR MgrN parameters set to zero to prevent write access.

```
Ethernet
   Mod Config
      SNMP options...
         Read Comm=Secret-1
         R/W Comm Enable=Yes
         R/W Comm=Secret-2
         Security=Yes
         RD Mgr1=10.0.0.1
         RD Mgr2=10.0.0.2
         RD Mgr3=10.0.0.3
         RD Mgr4=10.0.0.4
         RD Mgr5=10.0.0.5
         WR Mgr1=0.0.0.0
         WR Mgr2=0.0.0.0
         WR Mgr3=0.0.0.0
```

```
WR Mgr4=0.0.0.0
WR Mgr5=0.0.0.0
```

6 Close the Ethernet profile.

Setting SNMP traps

A trap is a mechanism for reporting system change in real time (for example, reporting an incoming call to a serial host port). When a trap is generated by some condition, a traps-PDU (protocol data unit) is sent across the Ethernet to the SNMP manager.

The following example shows the parameters related to setting SNMP traps:

```
Ethernet
   SNMP Traps
      Name=
      Alarm=Yes
      Port=Yes
      Security=Yes
      Comm=
      Dest=10.2.3.4
```

(For complete information about each parameter and the events that generate traps in the various classes, see the *MAX Reference Guide*.)

Understanding the SNMP trap parameters

To specify the community string for communicating with the SNMP manager, set the Comm field to the community name associated with the SNMP PDU.

The next three fields specify whether the MultiVoice Gateway traps alarm events, port events, and/or security events, respectively, and sends a trap-PDU to the SNMP manager.

The Port field specifies the destination address for the trap-status report. If DNS or YP/NIS is supported, the Dest field can contain the hostname of a system running an SNMP manager. If the DNS or YP/NIS is not supported, the Dest field must contain the host's address.

Note: To turn off SNMP traps, set Dest=0.0.0.0 and delete the value for Comm.

Example of an SNMP trap configuration

The procedure in this example creates a profile that specifies a community name, all three trap types, and the host's IP address:

1 Open an SNMP Traps profile and assign it a name.

2 Specify the community name (for example, Ascend).

3 Set the trap types to Yes.

4 Specify the IP address of the host to which the trap-PDUs will be sent.

You have now created the following subprofile:

```
Ethernet
   SNMP Traps
      Name=security-traps
      Alarm=Yes
      Port=Yes
```

```
Security=Yes
Comm=Ascend
Dest=10.2.3.4
```

5 Close the SNMP Traps profile.

Ascend enterprise traps

This section provides a brief summary of the traps generated by alarm, port, and security events. For more details, see the Ascend Enterprise MIB. To obtain the Ascend MIB, see "Supported MIBs" on page 10-26.

Alarm events

Alarm events (also called *error events*) use trap types defined in RFC 1215 and 1315, as well as an Ascend enterprise trap type. The MultiVoice Gateway supports the following trap types:

Alarm event	**Signifies that the MultiVoice Gateway**
`coldStart` (RFC-1215 trap-type 0)	Is reinitializing itself so that the configuration of the SNMP manager or the unit might be altered.
`warmStart` (RFC-1215 trap-type 1)	Is reinitializing itself so that neither the configuration of the SNMP manager nor the unit is altered.
`linkDown` (RFC-1215 trap-type 2)	Recognizes a failure in one of the communication links represented in the SNMP manager's configuration.
`linkUp` (RFC-1215 trap-type 3)	Recognizes that one of the communication links represented in the SNMP manager's configuration has come up.
`frDLCIStatusChange` (RFC-1315 trap-type 1)	Recognizes that one of the virtual circuits (to which a DLCI number has been assigned) has changed state. That is, the link has either been created, invalidated, or it has toggled between the active and inactive states.
`eventTableOverwrite` (ascend trap-type 16)	Detected that a new event has overwritten an unread event. This trap is sent only for systems that support Ascend's accounting MIB. Once sent, additional overwrites will not cause another trap to be sent until at least one table's worth of new events has occurred.

Security events

Security events are used to notify users of security problems and to track access to the unit from the console. The MIB-II event *authenticationFailure* is a security event. The other security events are Ascend-specific. They include:

Security event	Signifies
`authenticationFailure` (RFC-1215 trap-type 4)	The MultiVoice Gateway sending the trap is the addressee of a protocol message that is not properly authenticated.
`consoleStateChange` (ascend trap-type 12)	The console associated with the passed console index has changed state. To read the console's state get ConsoleEntry from the Ascend enterprise MIB.
`portUseExceeded` (ascend trap-type 13)	The serial host port's use exceeds the maximum set by the Max DS0 Mins Port parameter associated with the passed index (namely, the interface number).
`systemUseExceeded` (ascend trap-type 14)	The serial host port's use exceeds the maximum set by the Max DS0 Mins System parameter associated with the passed index (namely, the interface number).
`maxTelnetAttempts` (ascend trap-type 15)	A user has made three consecutive failed attempts to log into this MultiVoice Gateway via Telnet.

Supported MIBs

You can download the most up-to-date version of the Ascend Enterprise MIB by logging in as `anonymous` to ftp.ascend.com. (No password is required.) In addition to the Ascend MIB, the MultiVoice Gateway also supports objects related to Ascend functionality in the following Internet standard MIBs:

- MIB-II implementation (RFC 1213)
- DS1 MIB implementation (RFC 1406)
- RS232 MIB implementation (RFC-1317)
- Frame Relay MIB implementation (RFC-1315)

You can download the most recent version of these RFCs by logging in as `anonymous` to ftp.ds.internic.net. (No password is required.)

Troubleshooting

A

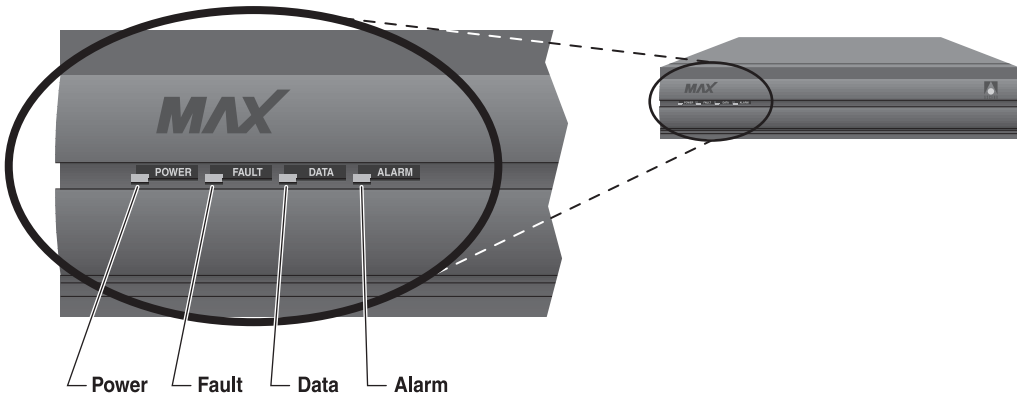
LEDs

This section describes the types of LEDs available on different MultiVoice Gateway models, and explains the information they display.

MultiVoice Gateway front panel

Figure A-1 shows the LEDs on the front panel of the MAX 6000/400 MultiVoice Gateway:

Figure A-1. MultiVoice Gateway front-panel LEDs



The front-panel LEDs indicate the status of the system, the PRI interface, and the data transfer in active sessions.

Table A-1 lists and describes each LED.

Table A-1. MultiVoice Gateway front-panel LEDs

LED	Description
Power	On when the MultiVoice Gateway power is on.
Fault	On in one of two cases: either a hardware self-test is in progress or there is a hardware failure. When a hardware self-test is in progress, the LED stays on. If any type of hardware failure occurs, the LED flashes. If the failure is isolated to a expansion card, the MultiVoice Gateway might continue to function without the expansion card.
Data	On when calls are active.
Alarm	On when there is a WAN alarm or when a trunk is out of service, such as during line loopback diagnostics. WAN alarms include Loss of Sync, Red Alarm, Yellow Alarm, and All Ones (or AIS).

Figure A-2 shows the location of the LEDs on the front panel of the Redundant MultiVoice Gateway.

Figure A-2. Location of LEDs on the Redundant MultiVoice Gateway

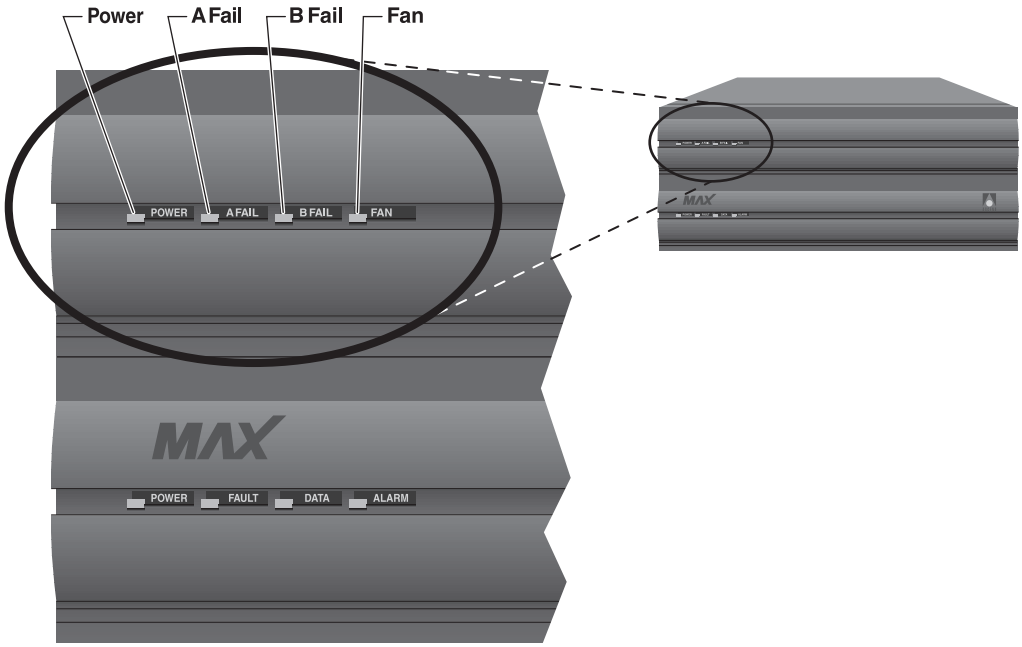


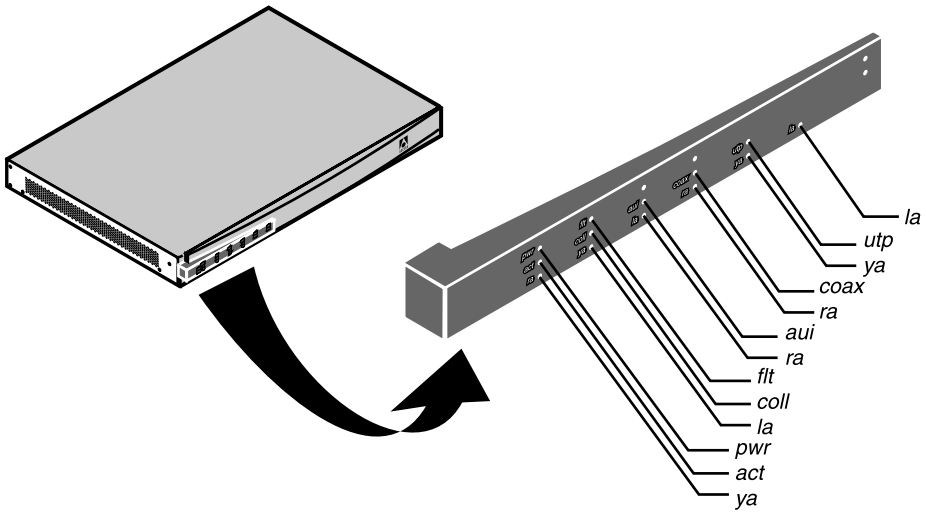
Table A-2 lists and describes each LED on the Redundant MultiVoice Gateway.

Table A-2. Redundant MultiVoice Gateway LEDs

LED	Description
Power	On when the Redundant MultiVoice Gateway power supply is on.
A Fail	On only if one or more of the voltages from side A of the power supply has failed (+12, +5, +3.3, -5, -12).
B Fail	On if one or more of the voltages from side B side of the power supply has failed (+12, +5, +3.3, -5, -12).
Fan	On when the fans are functioning properly (if +12 VDC from either A or B is good). This LED goes off in the event of a fan failure.

Figure A-3 shows the location shows the location of LEDs on the MAX 2000 front panel.

Figure A-3. Location of the MAX 2000 LEDs



Refer to the following table to understand each LED.

Table A-3. MAX 2000 LEDs

LED	Description
pwr	This LED is on when the MAX power is on.
act	This LED is ON if there is activity on the Ethernet interface.
ya (left-most—for Line 1)	This LED is ON when the MAX is receiving a Yellow Alarm pattern, indicating that the other of the of the line cannot recognize signals transmitted from the MAX.

Table A-3. MAX 2000 LEDs

LED	Description
flt	This LED is ON in one of two cases—either a hardware self-test is in progress or there is a hardware failure. When a hardware self-test is in progress, the LED is ON. If any type of hardware failure occurs, the LED flashes. If the failure is isolated to an expansion card, the MAX may continue functioning without the expansion card.
coll	This LED is ON if there are collisions on the Ethernet.
la (left-most—for Line 1)	This LED is ON when the link is active and there are no pending alarms or tests. If a PRI is active and using D-channel signaling, this LED blinks when the unit is unable to establish layer 2 and 3 protocol communications with the central office switch. This may indicate a configuration error.
aui	This LED is ON to reflect the AUI interface.
ra (left-most—for Line 1)	This LED is ON when the MAX is receiving a Red Alarm pattern, indicating an improper receive signal or no receive signal. This condition can occur as a result of a high error rate or improper line configuration. When such a condition arises, this red LED is ON and a Yellow Alarm is transmitted toward the WAN.
coax	This LED is ON if the 10Base-2 interface is chosen.
utp	This LED is ON if the 10BaseT interface is chosen.
ra, ya, and la (righ-most—for Line 2)	These LEDs have the same meanings as their left-most counterparts, except they apply only to Line 2.

MultiVoice Gateway back panel

Figure A-4 shows the MAX 6000 MultiVoice Gateway back-panel LEDs, which display the status of the Ethernet interface.

Figure A-4. Ethernet interface.LEDs on MultiVoice Gateway back panel

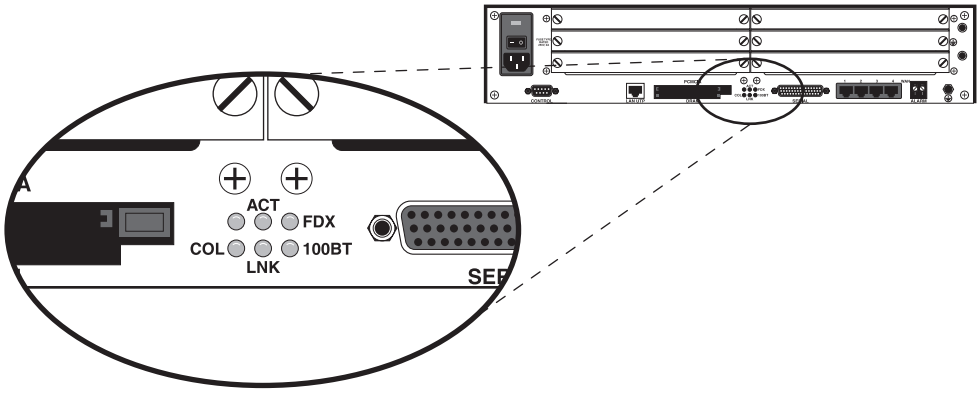


Table A-4 describes the Ethernet interface LEDs

Table A-4. MAX 6000 Ethernet interface LEDs on back panel

LED	Description
ACT (Activity)	On when the MultiVoice Gateway is detecting activity (network traffic) on its Ethernet interface.
COL (Collisions)	On when the MultiVoice Gateway detects packet collisions on the Ethernet.
FDX	On indicates full duplex on the Ethernet interface.
100ST	On indicates 100BT. Off indicates 10BT.
LINK (Link integrity)	On when the Ethernet interface is functional.

Figure A-5 shows the MultiVoice Gateway back-panel LEDs for the MAX 4000, which display the status of the Ethernet interface.

Figure A-5. Ethernet interface LEDs on the MAX 4000 back panel

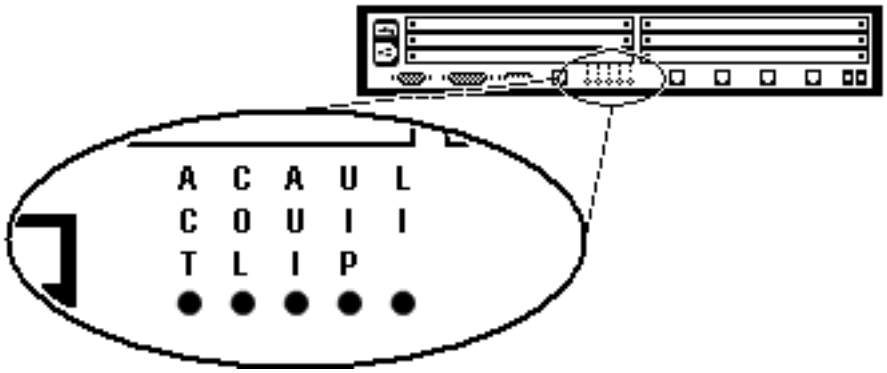


Table A-5 describes the Ethernet interface LEDs for the MAX 4000.

Table A-5. MAX 4000 Ethernet interface LEDs on back panel

LED	Description
ACT (Activity)	On when the MultiVoice Gateway is detecting activity (network traffic) on its Ethernet interface.
COL (Collisions)	On when the MultiVoice Gateway detects packet collisions on the Ethernet.
AUI	On, indicates Ethernet interface is through AUI port.
UIP	On, indicates Ethernet interface is through LAN UTP port.
LI (Link integrity)	On when the Ethernet interface is functional.

ISDN cause codes

ISDN cause codes are numerical diagnostic codes sent from an ISDN switch to a DTE. These codes provide an indication of why a call failed to be established or why a call was terminated. The cause codes are part of the ISDN D-channel signaling communications supported by the Signaling System 7 supervisory network (WAN). When you dial a call from the MultiVoice Gateway over a line with ISDN signaling, the MultiVoice Gateway reports the cause codes in the Message Log status menu. When the MultiVoice Gateway clears the call, a cause code is reported even when inband signaling is in use. If the PRI or BRI switch type is 1TR6 (Germany), see Table A-7.

Table A-6 lists the numeric cause codes and provides a description of each.

Table A-6. ISDN cause codes

Code	Cause
0	Valid cause code not yet received
1	Unallocated (unassigned) number
2	No route to specified transit network (WAN)
3	No route to destination
4	Send special information tone
5	Misdialed trunk prefix
6	Channel unacceptable
7	Call awarded and being delivered in an established channel
8	Prefix 0 dialed but not allowed
9	Prefix 1 dialed but not allowed
10	Prefix 1 dialed but not required
11	More digits received than allowed, but the call is proceeding
16	Normal clearing
17	User busy
18	No user responding
19	No answer from user (user alerted)
21	Call rejected
22	Number changed
23	Reverse charging rejected

Table A-6. ISDN cause codes (continued)

Code	Cause
24	Call suspended
25	Call resumed
26	Nonselected user clearing
27	Destination out of order
28	Invalid number format (incomplete number)
29	Facility rejected
30	Response to STATUS ENQUIRY
31	Normal, unspecified
33	Circuit out of order
34	No circuit/channel available
35	Destination unattainable
37	Degraded service
38	Network (WAN) out of order
39	Transit delay range cannot be achieved
40	Throughput range cannot be achieved
41	Temporary failure
42	Switching equipment congestion
43	Access information discarded
44	Requested circuit channel not available
45	Pre-empted
46	Precedence call blocked
47	Resource unavailable, unspecified
49	Quality of service unavailable
50	Requested facility not subscribed
51	Reverse charging not allowed
52	Outgoing calls barred

Table A-6. ISDN cause codes (continued)

Code	Cause
53	Outgoing calls barred within CUG
54	Incoming calls barred
55	Incoming calls barred within CUG
56	Call waiting not subscribed
57	Bearer capability not authorized
58	Bearer capability not presently available
63	Service or option not available, unspecified
65	Bearer service not implemented
66	Channel type not implemented
67	Transit network selection not implemented
68	Message not implemented
69	Requested facility not implemented
70	Only restricted digital information bearer capability is available
79	Service or option not implemented, unspecified
81	Invalid call reference value
82	Identified channel does not exist
83	A suspended call exists, but this call identity does not
84	Call identity in use
85	No call suspended
86	Call having the requested call identity has been cleared
87	Called user not member of CUG
88	Incompatible destination
89	Nonexistent abbreviated address entry
90	Destination address missing, and direct call not subscribed
91	Invalid transit network selection (national use)
92	Invalid facility parameter

Table A-6. ISDN cause codes (continued)

Code	Cause
93	Mandatory information element is missing
95	Invalid message, unspecified
96	Mandatory information element is missing
97	Message type nonexistent or not implemented
98	Message not compatible with call state, or message type nonexistent or not implemented
99	Information element nonexistent or not implemented
100	Invalid information element contents
101	Message not compatible with call state
102	Recovery on timer expiry
103	Parameter nonexistent or not implemented
111	Protocol error, unspecified
127	Internetworking, unspecified

Table A-7 lists the cause codes for the 1TR6 switch type.

Table A-7. ISDN cause codes for 1TR6 switch type

1TR6 Code	Cause
1	Invalid call reference value
3	Bearer service not implemented. (Service not available in the A-exchange or at another position in the network, or no application has been made for the specified service.)
7	Call identity does not exist. (Unknown call identity)
8	Call identity in use. (Call identity has already been assigned to a suspended link.)
10	No channel available. (No useful channel available on the subscriber access line—only local significance.)
16	Requested facility not implemented. (The specified FAC code is unknown in the A-exchange or at another point in the network.)
17	Request facility not subscribed. (Request facility rejected because the initiating or remote user does not have appropriate authorization.)

Table A-7. ISDN cause codes for 1TR6 switch type (continued)

1TR6 Code	Cause
32	Outgoing calls barred. (Outgoing call not possible due to access restriction that has been installed.)
33	User access busy. (If the total made up of the number of free B-channels and the number of calling procedures without any defined B-channel is equal to four, any new incoming calls will be cleared down from within the network. The calling party receives a DISC with a cause of *user access busy*, which indicates the first busy instance, and a busy signal.
34	Negative CUG comparison. (Link not possible because of negative CUG comparison.)
37	Communication as semipermanent link not permitted.
48 - 50	Not used. (Link not possible because, for example, RFNR check is negative.)
53	Destination not obtainable. (Link cannot be established in the network because of incorrect destination address, services, or facilities.)
56	Number changed. (Number of B-subscriber has changed.)
57	Out of order. (Remote TE not ready)
58	No user responding. (No TE has responded to the incoming SETUP or call has been interrupted, absence assumed—expiry of call timeout T3AA.)
59	User busy. (B-subscriber busy)
61	Incoming calls barred. (B-subscriber has installed restricted access against incoming link, or the service, which has been requested, is not supported by the B-subscriber.)
62	Call rejected. (To A-subscriber: Link request actively rejected by B-subscriber, by sending a DISC in response to an incoming SETUP. To a TE during the phase in which an incoming call is being established: The call has already been accepted by another TE on the bus.)
89	Network congestion. (Bottleneck situation in the network; for example, all-trunks-busy, no conference set free)
90	Remote user initiated. (Rejected or cleared down by remote user or exchange.)

Table A-7. ISDN cause codes for 1TR6 switch type (continued)

1TR6 Code	Cause
112	Local procedure error. (In REL: Call cleared down as a result of local errors; for example, invalid messages or parameters, expiry of timeout. In SUS REJ: The link must not be suspended because another facility is already active. In RES REJ: No suspended call available. In FAC REJ: No further facility can be requested because one facility is already being processed, or the specified facility can not be requested in the present call status.)
113	Remote procedure error. (Call cleared down because of error at remote end.)
114	Remote user suspended. (The call has been placed on hold or suspended at the remote end.)
115	Remote user resumed. (Call at remote end is no longer on hold, suspended, or in the conference status.)
127	User Info discarded locally. (The USER INFO message is rejected locally. This cause is specified in the CON message.)
35	Nonexistent CUG. (This CUG does not exist.)

Common problems and their solutions

This section lists problems you might encounter and describes ways to resolve them. It categorize common problems as configuration problems, hardware configuration problems, ISDN-interface problems, and problems indicated by the LEDs.

Configuration problems

The most common problems result from improperly configured profiles.

DO menus do not allow most operations

When the list of DO commands appears, many operations might not be not available if the right profile has not been selected. Because the MultiVoice Gateway can manage a number of calls simultaneously, you might need to select a specific Connection profile, Port profile, or Call profile in order to see certain DO commands. For example, to dial from a Call profile or a Connection profile, you must move to the Call profile (Host/6 > Port N Menu > Directory) or the Connection profile and then press Ctrl-D, then 1.

Note that you cannot dial if `Operations=No` for the control port. If a call is already active, DO 2 (Hang Up) appears instead of DO 1 (Dial). If the T1 or E1 line is not available, Trunk Down appears in the message log and you cannot dial.

The MultiVoice Gateway cannot dial out on a T1 or E1 line

To verify that a profile is correctly configured:

1. Make certain that you have entered the correct phone number to dial.
2. Verify that the Data Svc parameter specifies a WAN service available on your line.
   If you request a WAN service that is not available on your line, the WAN rejects your request to place a call.
3. Check whether the channels using the requested WAN service are busy.
   If these channels are busy, an outgoing call might be routed to channels for which you did not request the specified WAN service. Check the Data Svc, Call-by-Call, and PRI # Type parameter values in the profile.

No Channel Avail error message

If the error message No Channel Avail appears in the Message Log display when the MultiVoice Gateway tries to place a call, check the Line profile configuration. This message can also indicate that the lines' cables have been disconnected or were installed incorrectly.

Hardware configuration problems

If you cannot communicate with the MultiVoice Gateway through the VT100 control terminal, you might have a problem with terminal configuration, the control port cable, or the MultiVoice Gateway hardware.

Cannot access the VT100

If no data is displayed on the VT100, verify that the unit successfully completes all of the power-on self tests. Proceed as follows:

1. Verify that the MultiVoice Gateway and your terminal are set at the same speed.
2. Locate the LED labeled Fault.
3. Switch on the MultiVoice Gateway.

The Fault LED should remain off except during the power-on self tests. If you are using the VT100 interface, press Ctrl-L to refresh the screen.

If the Fault LED remains on longer than a minute, there is a MultiVoice Gateway hardware failure. A blinking Fault LED also indicates a hardware failure. Should these situations arise, contact Ascend Customer Support.

Fault LED is off but no menus are displayed

If the unit passed its power-on self tests and you still cannot communicate with the vt100 interface, press Ctrl-L to refresh the screen. If you still do not see any data, check the cabling between the MultiVoice Gateway and your terminal as follows:

1. Check the pin-out carefully on the 9-pin cable.
   The control terminal plugs into the HHT-VT100 cable or the 9-pin connector labeled Control on the back of the MultiVoice Gateway. If you are connecting to an IBM PC-like 9-pin serial connector, a straight-through cable is appropriate. Otherwise, you might need a 9-to-25 pin conversion cable.

2 Check the flow control settings on your VT100 terminal.

If you are not communicating at all with the MultiVoice Gateway, see whether you can establish communication after you have turned off all transmit and receive flow control at your terminal or terminal emulator.

3 Determine whether you need a null-modem cable converter.

In general, it is not required for communications to the MultiVoice Gateway. However, so many different cable and terminal configurations are available that in some cases a null-modem cable converter might be required.

Random characters appear in the VT100 interface

If random or illegible characters appear on your display, you probably have a communications settings problem, specify the following settings:

- 9600 bps data rate
- 8 data bits
- 1 stop bit
- No flow control
- No parity

If you have changed the data rate through the Port profile, make certain that your VT100 terminal matches that rate.

A Power-On Self Test fails

If the start-up display indicates a failure in any of its tests, an internal hardware failure has occurred with the unit. In this case, contact Ascend Customer Support.

ISDN PRI and BRI interface problems

Problems sometimes encountered with ISDN PRI and BRI interfaces include calls not dialed or answered reliably, Net/BRI lines not dialing or answering calls, apparent logical-link failures, and WAN calling errors in outbound Net/BRI calls.

Calls are not dialed or answered reliably

If calls are not dialed or answered reliably:

1 Check your cabling.

The first and most critical aspect of the interface is the physical cable connecting the MultiVoice Gateway to the line or terminating equipment. Typically, WAN interface cabling problems appear immediately after installation. If you are unsure about the cabling required, contact Ascend Customer Support. *MAX Getting Started* describes the general PRI and BRI interface requirements and lists cabling pin-outs.

2 If the cabling is not the problem and the MultiVoice Gateway is a T1 unit, ensure that the value of the Buildout parameter or the Length parameter in the Line profile matches the actual distance in your configuration.

The MultiVoice Gateway displays the Buildout parameter if its interface to the T1 line is equipped with an internal CSU. Its enumerated values can be 0 dB, 7.5 dB, 15 dB, and 22.5 dB. Contact your carrier representative to determine which value to choose.

If the line interface is not equipped with an internal CSU, the Length parameter is displayed. It can specify a cable length, of 1-133, 134-266, 267-399, 400-533, or 534-655, in feet, which should correspond to the distance between the MultiVoice Gateway and the WAN interface equipment, typically a CSU or multiplexer.

Note: T1 PRI ports not equipped with internal CSUs require an external CSU or other equipment approved for the metallic interface between the MultiVoice Gateway and the WAN facility.

The Net/BRI lines do not dial or answer calls

Do not connect the MultiVoice Gateway unit's Net/BRI ports directly to U-interface BRI lines. The MultiVoice Gateway unit's Net/BRI ports require carrier-approved Network Terminating-type 1 (NT1) equipment between the MultiVoice Gateway and BRI lines. Note that Net/BRI outbound calls require the use of trunk groups.

No Logical Link status

If you notice that the status of a Net/BRI line in the Line Status display is No Logical Link, you might or might not have a problem.

In some countries outside the U.S., it is common for no logical link to exist before the MultiVoice Gateway places a call. In the U.S., when you first plug a line into the MultiVoice Gateway or switch power on, the central office switch can take as long as 15 minutes to recognize that the line is now available. You might have to wait that long for the line state to change to Active (A). The physical link can exist without a logical link up.

If you wait longer than 15 minutes and the line is still not available:

1. Determine whether all the ISDN telephone cables are wired straight through.
   If you are running multipoint (passive bus) on your switch, all of the ISDN telephone cables must be wired straight through. If any of the cables are wired to cross over, you will not be able to place calls.
2. Verify that 100% termination is provided on each ISDN line.
3. Determine whether you have correctly specified the Service profile Identifiers (SPIDs) in the Line profile for each line. If the SPIDs are not correctly specified, the line status might indicate No Logical Link. Check with your system manager or carrier representative to obtain the SPID or SPIDs for your line. To specify your SPIDs, use the Pri SPID and Sec SPID parameters in the Line profile.

WAN calling errors occur in outbound Net/BRI calls

Should you encounter a problem in which the Call Status window immediately indicates a WAN calling error when the MultiVoice Gateway places a call on a Net/BRI module, proceed as follows to resolve the problem:

1. Check the value of the `Data Svc` parameter in the Call or Connection profile.
   Try both the 64K and 56K options for `Data Svc`, to see whether using a different value solves the problem.
2. Verify that you are using the correct dialing plan.
   Depending on how the BRI lines are configured, you might need to type four, seven, or ten digits to communicate with the remote end.

Four-digit dialing involves the last four digits of your phone number. For example, if your phone number is (415) 555-9015, four-digit dialing requires that you type only the last four digits—9015. Seven-digit dialing specifies that you dial the digits 5559015, and ten-digit dialing requires 4155559015.

If you are sending the incorrect number of digits, the MultiVoice Gateway cannot route the call. Ask your carrier representative for the correct dialing plan, or simply try all of the possibilities.

3 Ask your carrier representative to verify that the line is capable of supporting the call types you are requesting.

Callers dial destination correctly, but nothing happens

If callers dial a MultiVoice Gateway, hear a dial-tone, and dial the destination phone number, but nothing more happens:

- Make sure that the destination MultiVoice Gateway is registered and that the MultiVoice Access Manager (MVAM) is on and operating correctly. Attempt to `ping` both the MultiVoice Gateway and the Gatekeeper running MVAM from a remote system.
- Also check for IP-network congestion, which might cause packet loss between MultiVoice Gateways. Because IP-network congestion can occur in bursts, you might advise the caller to wait a few seconds, then try the call again.
- Check the MultiVoice Gateway to verify whether an IP address is entered for the `2nd GK IP` parameter. Make sure the settings for the `Pri GK Retries`, `Reg Retry Timer`, and `Keepalive Timer` parameters are appropriate for the operating conditions on you network.
- If ANI authentication is used, verify that the `Collect CLID/ANI` parameters is enabled, and make sure the proper settings for the Net/T1 or Net/E1 parameters are enabled for ANI collection.

Callers dial destination, hear tick-tock sound, but nothing happens

In a PRI environment, callers should hear the ringing tone after dialing the destination phone number. In the absence of a ringing tone, the MultiVoice Gateway generates a tick-tock sound.

If callers dial into the local MultiVoice Gateway, hear a dial-tone, dial the destination phone number, and hear a tick-tock sound in phone, but nothing more happens, make sure the destination MultiVoice Gateway is available and operating correctly. Also check for IP-network congestion, which might cause packet loss between MultiVoice Gateways. Because IP-network congestion can occur in bursts, you might advise the caller to wait a few seconds, then try the call again. If necessary, reboot the destination MultiVoice Gateway.

Callers hear a fast busy tone after dialing, using single-stage dialing

If callers dial into the local MultiVoice Gateway, using single-stage dialing, and hears silence, then a fast busy signal, the Destination Number Identification String (DNIS) was not passed to the Gateway. In this case:

- Make sure the user entered both the access number for the Gateway and destination number when they dialed.

- Check the switch, or PBX. If it cannot pass the DNIS to the Gateway, change the setting on the MultiVoice Gateway for the Single Dial Enable parameter to No. Callers will dial the Gateway and destination telephone numbers separately.
- If the switch, or PBX, passes the DNIS to the Gateway, check the switch configuration, and the Gateway configuration. Make sure the Gateway is using the proper settings for the Net/T1 or Net/E1 parameters.

Testing a switch

You can test your switch (or PBX) to determine whether it supports passing DNIS to the MultiVoice Gateway by running the `h323calldisplay` command from the Terminal Server screen of the MAX.

To perform this test, use the following procedure:

1 Make sure the MAX is configured for single-stage dialing.

2 Press Ctrl-D to display the Diagnostics profile. Select `D-Diagnostics`.

3 At the prompt, enable `h323calldisplay`:

```
> h323calldisplay
H323 call display is ON

 >
```

4 Place a call through the MAX, using single stage dialing.

After approximately 16 seconds, the MAX will display a message similar to the following:

```
_lanMakeCall: Tel. # = XXXXX
```

If `XXXXX` is the called telephone number, then the switch supports DNIS pass-through.

If `XXXXX` is anything other than the called telephone number, and you heard a dial tone from the MAX, the switch doesn't support DNIS pass-through. In this case, the MAX should be configured for two-stage dialing

Note: The 16-second delay results from not terminating the dial string with a #. The MAX waited for the inter-digit timer to expire.

Problems indicated by the LEDs

LEDs do not illuminate for the secondary E1 or T1 line

If no LEDs related to the secondary line are illuminated, the line is disabled in the Line profile. You can enable the secondary line by modifying the Line profile.

The E1 or T1 line is in a Red Alarm state

If the Alarm LED and the Line Status menu indicate that the line is in a Red Alarm state, the MultiVoice Gateway cannot establish proper synchronization and frame alignment with the WAN. This behavior is normal for as long as 30 seconds after a PRI line is first plugged into the MultiVoice Gateway.

If the Red Alarm condition persists for longer than 30 seconds:

1 Check the value of the Framing Mode parameter in the Line profile.

Change the value to the other available option and check to see whether the Red Alarm condition goes away within 30 seconds.

2 If the Red Alarm state persists, check the cabling.

You might have a crossover cable installed when a straight-through cable is required, or vice versa. If the MultiVoice Gateway is connected through bantam plugs, reverse the transmit and receive plugs. Then allow the MultiVoice Gateway to attempt to establish synchronization for an additional 30 seconds.

3 You can eliminate the cabling as a possible cause by replacing the connection with a loopback plug. The LS LED should go off immediately, followed by the RA LED in about 30 seconds.

A PRI line is in use and the Alarm LED blinks

A blinking ALARM LED means that the physical configuration of the E1 or T1 line is correct but the D channel is not communicating with the WAN. To resolve this problem:

1 Verify with your carrier representative that the D channel is channel 16 (E1) or 24 (T1).

2 If the D channel number is correct, check the value of the Line Encoding parameter in the Line profile. When B8ZS encoding is in use, a noninverted D channel is established. If AMI encoding is selected, an inverted D channel is established. Check the line translations provided by your carrier representative and set the line encoding to match the inversion requirements.

3 Determine whether your WAN interface or the MultiVoice Gateway T1 unit is equipped with a CSU.

If the WAN interface or the MultiVoice Gateway is not equipped with a CSU, the ALARM LED blinks. Verify that you have specified the proper Length or Buildout value in the Line profile.

4 Verify that the D channel is in service.

If no equipment has been plugged into the line for a short period of time (five to ten minutes), the D channel is taken out of service. You might need to ask your carrier to put the D channel back into service.

Provisioning the Switch

B

Provisioning the switch for T1 access

If you use an inband signaling line, the T1 circuit at the Point-of-Presence (POP) must support the translations listed in Table B-1 for compatibility with the MultiVoice Gateway.

Table B-1. T1 access provisioning information

Translation	**Optional or required**
Two-state DTMF (Dual-Tone Multifrequency) dialing	Required.
Outgoing wink start	Required.
Incoming immediate seizure	Optional for a switch. Does not apply on T1 lines to a PBX.
Incoming wink start	Optional for a switch Required on T1 lines to a PBX
Incoming digits suppressed	Required, except when a PBX is connected to a T1 line supplied by the MultiVoice Gateway through PRI-to-T1 conversion.
Answer supervision	Required.
Switched data	Required. No voice/digital loss plan is allowed, but the drop-and-insert channels to a PBX and the channels to digital modems can be voice channels.

Four-state A-bit signaling, four-state B-bit signaling, and pulse dialing are not supported. However, lines using these types of signaling are passed through transparently when the MultiVoice Gateway performs drop-and-insert between lines #1 and #2.

(For further information about wink-start and inband signaling, see the description of the Rob Ctl parameter in the *MAX Reference Guide*.)

Provisioning the switch for T1 PRI access

Request the following information from your WAN provider about your WAN interface:

- Whether the line uses inband or ISDN D-channel signaling.
- Whether the line uses B8ZS or AMI line encoding.
- Whether the line uses ESF or D4 framing.
- Each phone number assigned to the line on a channel-by-channel or service-by-service basis.
- The number of nailed-up channels, if any.
- The number of unused channels, if any.
- The types of call-by-call services (also called NSF identifiers) on the switched channels.
- Whether the line uses B channel, H0 channel, or H11 channel provisioning.
- The D-channel assignment.
- The NFAS ID number (if the T1 PRI line is provisioned for NFAS).

Keep the following additional information in mind:

- In general, ESF framing and B8ZS line encoding are both recommended for T1 PRI-based applications. In addition, channel 24 must be the D channel, except for applications using Non-Facility Associated signaling (NFAS).
- Applications that require NFAS must be connected to an AT&T or Northern Telecom switch provisioned with NFAS.

  The service provider supplies guidelines for NFAS ID assignments and D-channel assignments. Note that the MultiVoice Gateway must have D-channel signaling functionality and at least two WAN ports to use NFAS.
- The MultiVoice Gateway can receive multichannel calls using Combinet or MP encapsulation only if all channels of the call share a common phone number (namely, a hunt group).

  You can request that your service provider supply you with a hunt group.

What you need from your E1/PRI service provider

You need the following information from your E1/PRI service provider:

- The phone numbers assigned to your E1/PRI interface, channel-by-channel
- Nailed-up channels (also called private WAN), if any
- Unused channels, if any
- Switch type (or emulation)—DPNSS only
- Switch layers 2 and 3 configuration—DASS 2 and DPNSS only (A/B end, X/Y end)

- Rate adaptation protocol—DASS 2 and DPNSS only (X.30 and V.110)

Note: The MultiVoice Gateway can receive multichannel calls using Combinet or MP encapsulation only if all channels of the call share a common phone number (namely, a hunt group). You can request that your service provider supply you with a hunt group.

Supported WAN switched services

The MultiVoice Gateway E1 PRI supports the following WAN switched services:

- 56 Kbps and 64 Kbps data services
- GloBanD (and GVPN in CCITT countries) PRI network services—multiples of 64 Kbps

When ordering a data service, make sure it is available end-to-end. Otherwise, the data carried by the call will be corrupted or the carrier will reject the call. For example, a GloBanD 512 Kbps call made at a PRI interface is rejected when the called end is BRI, because GloBanD does not support BRI.

Provisioning the switch for ISDN BRI access

When ordering ISDN BRI service, make sure you understand the settings for BRI-specific provisioning parameters and the information the carrier gives you about the BRI line.

Parameters on the MultiVoice Gateway

The tables that follow supply provisioning information for the ISDN BRI interface when a Net/BRI module (MX-SL-8BRIN) is installed. These requirements vary by switch type. Table B-2 provides information for AT&T 5ESS switches operating in Point-to-Point (PTP), Multi-Point (MP), or National ISDN-1 (NI-1) mode.

Table B-2. AT&T 5ESS provisioning information

Element	Value	Comments
Terminal Type	A	
Number of Circuit Switched Data (CSD)	2	Except when it handles calls to digital modems, the MultiVoice Gateway is a data device, and you can substitute voice service for data service only if end-to-end data integrity is guaranteed. Voice service is required if digital modems are installed.
Number of Circuit Switched Voice (CSV)	1	Except when it handles calls to digital modems, the MultiVoice Gateway is a data device, and you can substitute voice service for data service only if end-to-end data integrity is guaranteed. Voice service is required if digital modems are installed.
Number of Call Appearances	1	Not relevant for proper operation of the MultiVoice Gateway.

Table B-2. AT&T 5ESS provisioning information (continued)

Element	Value	Comments
Ringing/Idle Call Appearances	Idle	The default for Terminal Type A.
Autohold is Y/N	No	The default for Terminal Type A.
Onetouch is Y/N	No	The default for Terminal Type A.

Table B-3 provides provisioning information for Northern Telecom switches.

Table B-3. Northern Telecom provisioning information

Element	Value	Comments
Signaling	Functional	
Protocol Version Control (PVC)	1 or 2	1 is NTI custom. 2 is NI-1 (National ISDN-1), which requires a TID to be assigned as a suffix to the SPID.
TEI assignment	Dynamic	
Release Key	No	Not relevant for proper operation of the MultiVoice Gateway.
Ringing Indicator	No	Not relevant for proper operation of the MultiVoice Gateway.
EKTS (Electronic Key Telephone System)	Off	

Note: The MultiVoice Gateway can receive multichannel calls using Combinet or MP encapsulation only if all channels of the call share a common phone number (namely, a hunt group). You can request that your service provider supply you with a hunt group.

Information required from the ISDN BRI provider

If a Net/BRI module (MX-SL-8BRIN) is installed, your ISDN BRI provider must provide you with the following information:

- The phone number assigned to your ISDN BRI line.
- The SPIDs assigned to your ISDN BRI line (for lines running in any mode other than AT&T Point-to-Point). In countries outside the United States, SPIDs might or might not be required. Check with your carrier.
- Which channels are nailed up or unused, if any.

SPIDs for AT&T 5ESS switches

If your ISDN BRI line comes from an AT&T 5ESS switch operating in Multi-Point (MP) or National ISDN-1 (NI-1) mode, each SPID has the following format:

```
01 NNNNNNN 0 TT
```

where:

- *NNNNNNN* is the 7-digit phone number of the ISDN BRI line.
- *TT* is the 2-digit TID (required only for NI-1).

  The TID can be a value from 00 to 62. It is assigned by your carrier. Ascend recommends that you use 00 as the TID for all SPIDs.

For example, suppose that 555-1212 is the 7-digit phone number of an ISDN BRI line using Multi-Point mode. The telephone company gives you the following SPID:

```
0155512120
```

Note: Because Multi-Point mode is not an NI-1-compliant, no 2-digit TID is required.

Now, suppose that 555-6001 and 555-6002 are the 7-digit phone numbers of an ISDN BRI line using NI-1 mode. You choose TID=00 for both numbers and the telephone company gives you the following SPIDs:

```
015556001000
015556002000
```

If your ISDN BRI line operates in Point-to-Point (PTP) mode, SPIDs are not required.

SPIDs for Northern Telecom DMS-100 switches

If your ISDN BRI line comes from a Northern Telecom (NTI DMS-100) switch, each SPID has the following format:

```
AAANNNNNNN SS TT
```

where:

- *AAA* is the 3-digit area code of your ISDN BRI line.
- *NNNNNNN* is the 7-digit phone number of your ISDN BRI line.
- *SS* is the SPID suffix, which can contain zero, one, or two digits as follows:
  - Empty
  - 1 and 2 for each ISDN BRI line
  - 01 and 02 for each ISDN BRI line
- *TT* is the 2-digit TID (required only for NI-1 [PVC=2]).

  The TID can be a value from 00 to 62. It is assigned by your carrier. Ascend recommends that you use 00 as the TID for all SPIDs.

For example, suppose you are using Northern Telecom in NTI Custom mode [PVC=1]). The phone number of your ISDN BRI line, including the area code, is 415-555-1212. The telephone company gives you the following SPID:

```
415555121201
```

Now suppose you are using Northern Telecom in NI-1 mode [PVC=2]). 510-555-6001 and 510-555-6002 are the phone numbers of your ISDN BRI line. You choose TID=00 for both numbers and the telephone company gives you the following SPIDs:

```
5105550010100
5105550020200
```

MultiVoice Gateway Technical Specifications

C

This appendix covers the following topics:

Battery

The MultiVoice Gateway contains an internal 3V lithium battery. The normal operating life of the battery exceeds five years.

Only trained engineers authorized by Ascend should open the MultiVoice Gateway unit's case for testing, maintenance, installation, or any other purpose. Furthermore, only trained engineers should replace MultiVoice Gateway components.

Warning: The battery can explode if incorrectly replaced. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

ATTENTION: IL Y A DANGER D'EXPLOSION S'IL Y A REMPLACEMENT INCORRECT DE LA BATTERIE. REMPLACER UNIQUEMENT AVEC UNE BATTERIE DU MÉME TYPE OU D'UN TYPE RECOMMANDEÉ PAR LE CONSTRUCTEUR. METTRE AU RÉBUT LES BATTERIES USAGÉES CONFORMÉMENT AUX INSTRUCTIONS DU FABRICANT.

Power requirements

Table C-1 list the MultiVoice Gateway unit's source power requirements.

Table C-1. MultiVoice Gateway source power requirements

Element	Value
Voltage	90-240 Vac
Phase	Single
Frequency	47-63 Hz

Table C-2 lists the redundant-power requirements for the MultiVoice Gateway.

Table C-2. Redundant-power MultiVoice Gateway requirements

Element	Value
Voltage	-43 to -60 Vdc
Input Power	MultiVoice Gateway 6000: 80W (nominal)-200W (maximum) Standard MultiVoice Gateway: 80W (nominal)-120W (maximum)
Fuses	7.5 Amp GMT (two fuses)

The MultiVoice Gateway unit's configuration profiles are stored in battery-protected memory. When the MultiVoice Gateway is turned off, the profiles are not lost.

Note: Use a protected AC power source, or add surge protection between the power source and the MultiVoice Gateway.

Environmental requirements

For best results, you should house the MultiVoice Gateway in a room with constant temperature and humidity. In general, cooler environments are better. An operating temperature of 32° to 104° Fahrenheit (0° to 40° Celsius) is recommended. Storage temperatures of -40° to 176° Fahrenheit (-71.4° to 80° Celsius) are acceptable.

Humidity should be high enough to prevent accumulation of static electricity, but low enough to prevent condensation. An operating relative humidity of up to 90% is acceptable.

You can operate the MultiVoice Gateway at altitudes of 0 to 14800 ft. (0-4500 m).

The MultiVoice Gateway base system weighs 15 lbs (6.81 kg). A fully loaded system weighs 30 lbs (13.6 kg). The MultiVoice Gateway has these dimensions: 3.0" x 17" x 12" (8.9 cm x 43.2 cm x 30.5 cm).

The base system of a redundant power MultiVoice Gateway or MultiVoice Gateway 6000 weighs 41 lbs (18.6 kg). A fully loaded system weighs 56 lbs (25.5 kg). The redundant power MultiVoice Gateway has the dimensions 7.0" x 17.5" x 12" (17.8 cm x 44.5 cm x 30.5 cm).

Alarm relay operating specifications

On the back panel of the Ascend unit is a pair of alarm-relay terminal-block contacts that remains open during normal operation. The contacts close during loss of power, hardware failure, or reset.

The maximum rated load for the alarm relay is:

- 1 amp at 30 Vdc.
- 0.6 amp at 60 Vdc.
- 0.6 amp at 60 Vac.

Caution: To reduce the risk of electric shock, do not connect the alarm circuit to a device with an output exceeding 30 Vrms, 42.4 Vpeak, or 60 Vdc.

Additional details on the technical specifications for the MAX 6000, MAX 4000 and MAX 2000 MultiVoice Gateways may be found in the *Getting Started Guide* for that particular switch.

Cables and Connectors

D

Additional details on the cables and connectors for the MAX 6000, MAX 4000 and MAX 2000 MultiVoice Gateways may be found in the *Getting Started Guide* for that particular switch.

User interface specifications

This section provides cabling pinouts for the Control Monitor, Palmtop Controller, and MIF interfaces.

Control port and cabling pinouts for the Control Monitor and MIF

The Control port uses a standard DE-9 female connector that conforms to the EIA RS-232 standard for serial interfaces. Table D-1 lists all MultiVoice Gateway models that use the RS-232 pinouts.

Table D-1. Control Monitor and MIF Control port and cabling pinouts

DE-9 pin number	RS-232 signal name	Function	I/O
1	DCD	Data Carrier Detect	O
2	RD	Serial Receive Data	O
3	SD	Serial Transmit Data	I
4	DTR	Data Terminal Ready	I
5	GND	Signal Ground	
6	DSR	Data Set Ready	O
7	RTS	Request to Send	I
8	CTS	Clear to Send	O
*9	*RI	*Ring Indicator	*O

Note: *Pin 9 is not active (Ring Indication signal not supplied).

Pinouts for the Palmtop Controller

Table D-2 specifies the pins and corresponding functions of the Palmtop Controller jacks. In the I/O columns, Out (O) is from the MultiVoice Gateway toward the Palmtop.

Table D-2. Palmtop Controller pinouts

MultiVoice Gateway RJ12 pin	Function	I/O
1	Power to Palmtop, +5V	O
2	Control Out	O
3	Control In	I
4	Serial Transmit Data	O
5	Serial Receive Data	I
6	Ground	

Palmtop port and cabling pinouts for a Control Monitor

Table D-1 illustrates the MIF Palmtop port and cabling pinouts for a Control Monitor.

Figure D-1. Control Monitor and MIF Palmtop port and cable

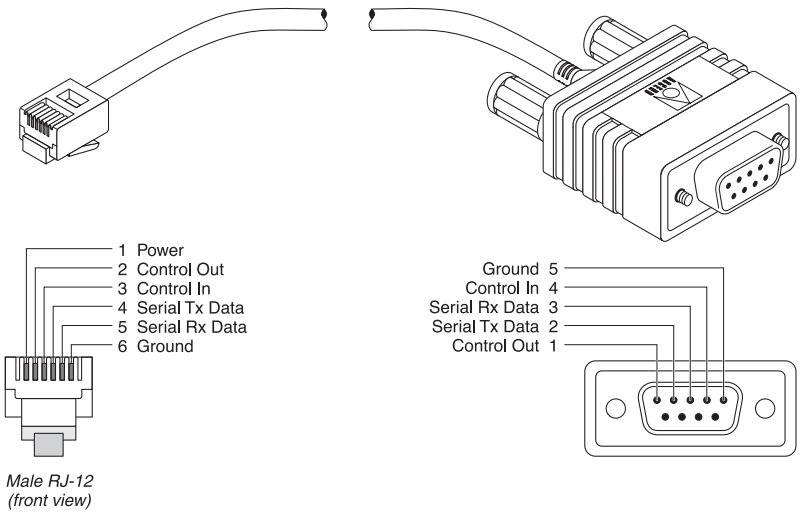


Table D-3 lists the specifications you need to adapt the Palmtop port for use as a Control Monitor or MIF interface through a VT100 terminal.

Table D-3. Control Monitor and MIF Palmtop port and cabling pinouts

Model number HHT-VT-100 Part number 2510-0088-001		
Signal (MultiVoice Gateway)	**MultiVoice Gateway RJ12 pin number**	**VT-100 female DE-9 pin number**
Power (+5V)	1	Not connected
Control Out	2	1
Control In	3	4
Serial Transmit Data	4	2
Serial Receive Data	5	3
Ground	6	5

Ethernet interface specifications

The base unit of a MultiVoice Gateway has an Ethernet interface that supports the physical specifications of IEEE 802.3 and IEEE 802.14 with Ethernet 2 (Ethernet/DIX) framing. The unit provides a single Ethernet interface that auto-senses the Ethernet type to which it is connected. It supports the following types:

- 10Base-T (Unshielded Twisted Pair): Twisted pair Ethernet and IEEE 802.3 (10Base-T) with an RJ-45 connector, labeled LAN UTP.
- 100 Base-T: 100 Mbps Baseband Modulation on Twisted Pair.
- AUI (Attachment Unit Interface): Standard Ethernet and IEEE (10Base-5) with a 15-pin AUI connector (MAX 4000/MAX 2000).

The Ethernet address used to identify the Ethernet interface resides in the MultiVoice Gateway unit's motherboard.

To install the Ethernet interface, you must have the equipment described in either of the following sections.

10Base-T

For 10Base-T, you need a twisted-pair Ethernet cable and a dual twisted-pair cable terminated with RJ-45 modular jacks.

Use an EIA/TIA 568 or IEEE 802.3 10Base-T cable.

100Base-T

For 100Base-T, you need a twisted-pair Ethernet cable and a dual twisted-pair cable terminated with RJ-45 modular jacks.

Use one of the following cables: 100BASE-T2, 100BASE-T4 (not very popular), 100BASE-TX, or 100BASE-FX.

AUI

For Standard Ethernet, you need a transceiver and transceiver cable.

T1/PRI interface specifications

This section provides the specifications for the MultiVoice Gateway unit's T1/PRI interface and covers cabling requirements.

T1/PRI CSU requirements

T1/PRI requirements differ depending on whether a T1/PRI port on the MultiVoice Gateway is equipped with an internal Channel Service Unit (CSU).

Port with internal CSU

If a T1/PRI port on the MultiVoice Gateway has an internal CSU, you can connect the port directly to the metallic interface of the WAN.

To avoid harming the WAN, you must contact your carrier for approval before installation. Once you install the MultiVoice Gateway, you must notify the carrier before disconnecting the MultiVoice Gateway from the WAN. If you disconnect or turn off the MultiVoice Gateway without prior notification, the carrier might temporarily discontinue your T1/PRI service.

The MultiVoice Gateway unit's internal CSUs are compatible with dry-loop T1/PRI lines, and with span-powered or wet-loop powered T1/PRI lines.

Port without internal CSU

A T1/PRI port of the MultiVoice Gateway that does not have an internal CSU cannot connect directly to the WAN.

You must connect the port to other equipment that provides the interface to the WAN (for example, an external CSU). Your carrier determines the correct value for the line buildout

setting of the CSU. You configure this parameter during installation. (For more information, see the *MAX Reference Guide*.)Refer to Table D-4 lists CSU specifications.

Table D-4.CSU specifications

Information	**Value**
CSU Registration	2CZUSA-74421-DE-N
Critical Circuitry Power Source	Dry Loop from local AC power source
Line Capture Frequency	1.544 Mb/s +/- 200 b/s
Line Code	AMI or B8ZS
Line Framing	D4 or ESF
Line Input/Output Impedance	100 Ohms +/- 5%
Received Signal Level Range	DSX-1 level to -27.5 dB
Transmitted Signal Level	DSX-1 level into 100 Ohms
Line Buildout	0.0, 7.5, 15.0, or 22.5 dB
Pulse Density and Consecutive Zeros Enforcement	In accordance with requirements of AT&T Pub 62411
Line Loopback (LLB) Set Inband Code	(10000) repeating binary pattern
Line Loopback (LLB) Reset Inband Code	(100) repeating binary pattern

Note: During loss of power or whenever the MultiVoice Gateway restarts, a relay closure returns the T1 PRI signal to the WAN. That is, the T1 PRI line is looped back. However, if the MultiVoice Gateway is configured for framing-compatible drop-and-insert functionality, all channels of line #1 are passed to line #2. Note that line #1 and line #2 of a MultiVoice Gateway expansion module always loop back upon loss of power, regardless of how they are configured.

T1/PRI cable specifications

The maximum cable distance between the T1/PRI WAN interface equipment and the MultiVoice Gateway should not exceed 655 feet (200 m) for a MultiVoice Gateway without CSUs. Measure the line length and record it when you install the MultiVoice Gateway. You must specify this length when you configure the Line Profile parameters. (For more information, see the *MAX Reference Guide*.)

Use only cables specifically constructed for transmission of T1/PRI signals. The cables should meet standard T1 attenuation and transmission requirements. The following specifications are recommended:

- 100 Ω
- Two twisted pairs, Category 3 or better

The WAN interface cables and plugs described in the following sections are available for the MultiVoice Gateway unit's WAN interfaces.

T1/PRI crossover cable: RJ48C/RJ48C

Install the RJ48C/RJ48C crossover cable when the WAN transmits on pins 5 and 4 and receives on pins 2 and 1. Refer to Figure D-2 and Table D-5.

Figure D-2. RJ48C/RJ48C crossover cable

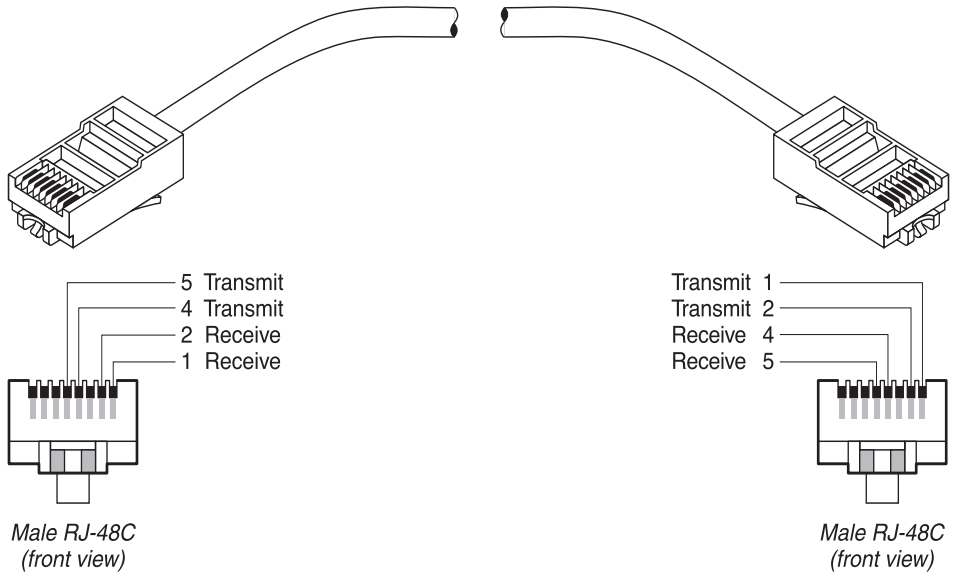


Table D-5. RJ48C/RJ48C crossover cable specifications

Model number RJ48C-X **Part number 2510-0059/0323-001**			
Pair #	**Signal (MultiVoice Gateway)**	**Male RJ48C (MultiVoice Gateway)**	**Male RJ48C (remote)**
1	Receive	2 1	5 4
2	Transmit	5 4	2 1

T1/PRI straight-through cable: RJ48C/RJ48C

Before installing the RJ48C/RJ48C straight-through cable, verify that the WAN transmits on pins 2 and 1 and receives on pins 5 and 4. Refer to Figure D-3 and Table D-6.

Figure D-3. RJ48C/RJ48C straight-through cable specifications

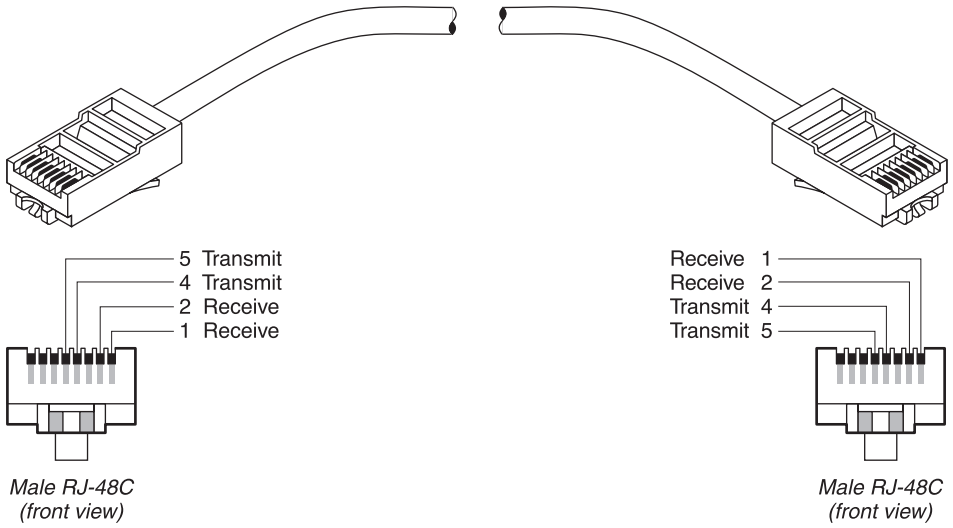


Table D-6. RJ48C/RJ48C straight-through cable specifications

Model number RJ48C-S Part number 2510-0064-001			
Pair #	**Signal (MultiVoice Gateway)**	**Male RJ48C (MultiVoice Gateway)**	**Male RJ48C (remote)**
1	Receive	1 2	1 2
2	Transmit	5 4	5 4

T1/PRI straight-through cable: RJ48C/DA-15

Before installing the RJ48C/DA-15 straight-through cable, verify that the WAN transmits on pins 3 and 11 and receives on pins 1 and 9. Refer to Figure D-4 and Table D-7.

Figure D-4. RJ48C/DA-15 straight-through cable

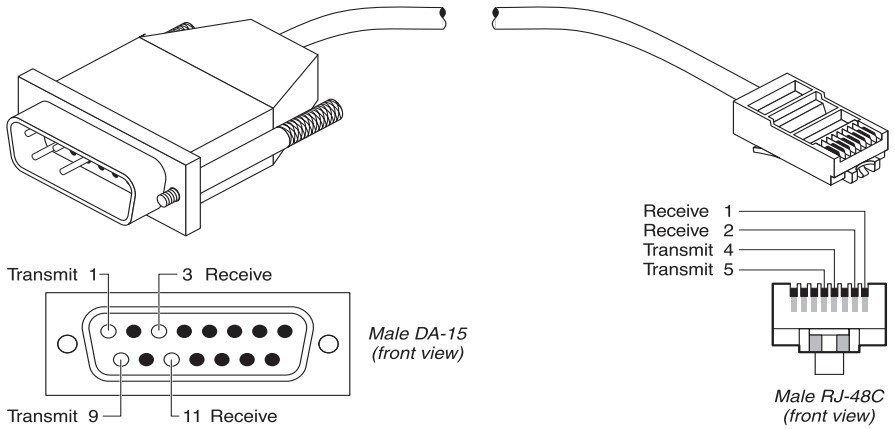


Table D-7. RJ48C/DA-15 straight-through cable specifications

Model number DA15-X Part number 2510-0082-001			
Pair #	**Signal (MultiVoice Gateway)**	**Male RJ48C (MultiVoice Gateway)**	**Male DA-15P (remote)**
1	Receive	1 2	3 11
2	Transmit	5 4	1 9

T1/PRI crossover cable: RJ48C/DA

Before installing the RJ48C/DA crossover cable, verify that the WAN transmits on pins 1 and 9 and receives on pins 3 and 11. Refer to Figure D-5 and Table D-8.

Figure D-5. RJ48C/DA crossover cable

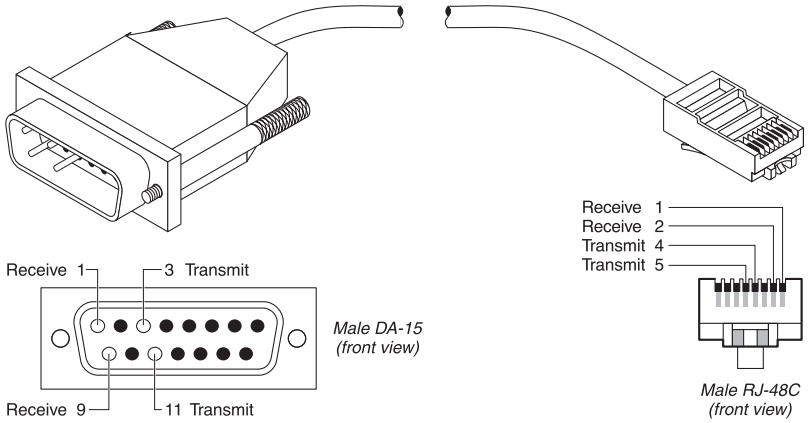


Table D-8.RJ48C/DA crossover cable specifications

Model number DA15-S Part number 2510-0065-001			
Pair #	**Signal (MultiVoice Gateway)**	**Male RJ48C (MultiVoice Gateway)**	**Male DA-15P (remote)**
1	Receive	1 2	1 9
2	Transmit	5 4	3 11

T1/PRI straight-through cable: RJ48C/Bantam

The WAN side of the RJ48C/Bantam straight-through cable connects to dual bantam jacks. Refer to Figure D-6 and Table D-9.

Figure D-6. RJ48C/Bantam straight-through cable

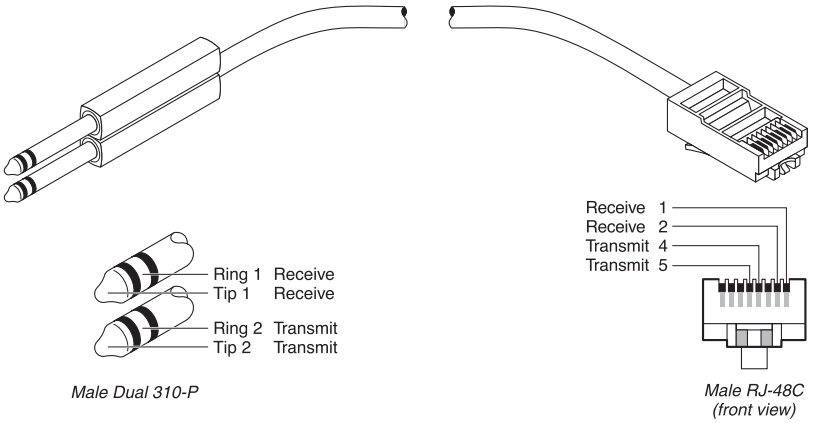


Table D-9.RJ48C/Bantam straight-through cable specifications

Model number DBNT-RJ45 Part number 2510-0066-001			
Pair #	**Signal (MultiVoice Gateway)**	**Male RJ48 (MultiVoic e Gateway)**	**Male Dual - 310P (remote)**
1	Receive	1 2	Tip 1 Ring 1
2	Transmit	5 4	Tip 2 Ring 2

T1 RJ48C-Loopback plug

The Rj48C-Loopback plug loops the transmit signal back to the MultiVoice Gateway.

Table D-10.RJ48C-Loopback plug specifications

Pair #	**Signal**	**Male RJ48C**
1	Receive	1 (connects to 5) 2 (connects to 4)
2	Transmit	5 (connects to 1) 4 (connects to 2)

T1/PRI WAN ports

Table D-11 lists the pins on RJ48C sockets used for T1/PRI WAN interface on the MultiVoice Gateway. Only pins 1, 2, 4, and 5 are used. The remaining pins are not connected.

Table D-11.Transmit and Receive pins

MultiVoice Gateway T1/PRI interface	RJ48C DTE
Receive (input) pair, Tip (T1)	Position 2
Receive (input) pair, Ring (R1)	Position 1
Transmit (output) pair, Tip (T)	Position 5
Transmit (output) pair, Ring (R)	Position 4

WAN switched services available to the MultiVoice Gateway

The MultiVoice Gateway is compatible with both AT&T and Northern Telecom central office switches, and can access all T1/PRI switched digital services offered by AT&T's ACCUNET Switched Digital Services:

- MCI 56 Kbps and 64 Kbps services
- Sprint Switched 56 Kbps and 64 Kbps services
- MultiRate and GloBanD (and GVPN in CCITT countries) PRI network services

Note: The MultiVoice Gateway can access only Switched-56 Kbps services on a T1 access line or a Switched-56 line.

For a listing of the compatible switch types, see the Switch Type parameter in the *MAX Reference Guide*. In addition to switched circuits, the MultiVoice Gateway can connect to nailed-up circuits and to aggregate nailed-up and switched circuits.

E1/PRI interface specifications

This section provides the specifications for the MultiVoice Gateway unit's E1/PRI interface and covers cabling requirements.

During loss of power or whenever the MultiVoice Gateway restarts, a relay closure returns the E1 PRI signal to the WAN. That is, the E1 PRI line is looped back. However, if the MultiVoice Gateway is configured for framing-compatible drop-and-insert functionality, all channels of line #1 are passed to line #2. Note that line #1 and line #2 of a MultiVoice Gateway Net/E1 expansion module always loop back upon loss of power, regardless of how they are configured.

E1/PRI cable specifications

The WAN interface cables and plugs described in this section are available for the MultiVoice Gateway unit's WAN interfaces. Use only the cable specifically constructed for transmission.

E1/PRI crossover cable: RJ48C/RJ48C

Install the RJ48C/Rj48C crossover cable when the WAN transmits on pins 5 and 4 and receives on pins 2 and 1. Refer to Figure D-7 and Table D-12.

Figure D-7. RJ48C/RJ48C crossover cable

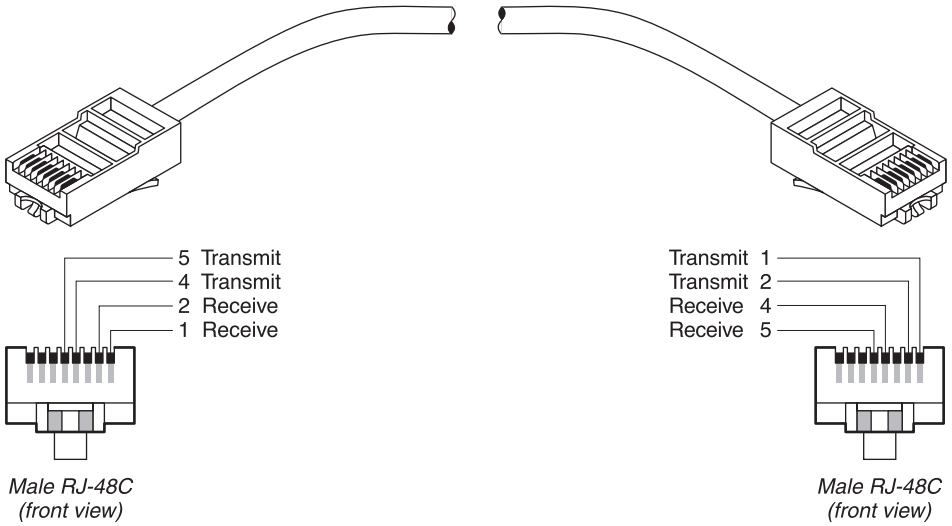


Table D-12.RJ48C/RJ48C crossover cable specifications

Model number RJ48C-X Part number 2510-0059/0323-001			
Pair #	**Signal (MultiVoice Gateway)**	**Male RJ48C (MultiVoice Gateway)**	**Male RJ48C (remote)**
1	Receive	2 1	5 4
2	Transmit	5 4	2 1

E1/PRI straight-through cable: RJ48C/RJ48C

Before installing the RJ48C/RJ48C straight-through cable, verify that the WAN transmits on pins 2 and 1 and receives on pins 5 and 4. Refer to Figure D-8 and Table D-13.

Figure D-8. RJ48C/RJ48C straight-through cable specifications

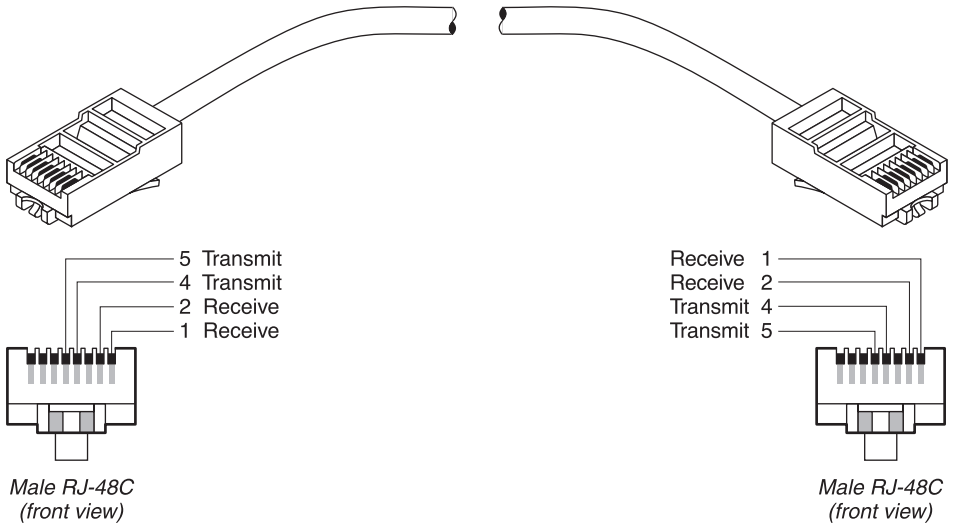


Table D-13.RJ48C/RJ48C straight-through cable specifications

Model number RJ48C-S Part number 2510-0064-001			
Pair #	**Signal (MultiVoice Gateway)**	**Male RJ48C (MultiVoice Gateway)**	**Male RJ48C (remote)**
1	Receive	1 2	1 2
2	Transmit	5 4	5 4

E1/PRI straight-through cable: RJ48C/DA-15

Before installing the RJ48C/DA-15 straight-through cable, verify that the WAN transmits on pins 3 and 11 and receives on pins 1 and 9. Refer to Figure D-9 and Table D-14.

Figure D-9. RJ48C/DA-15 straight-through cable

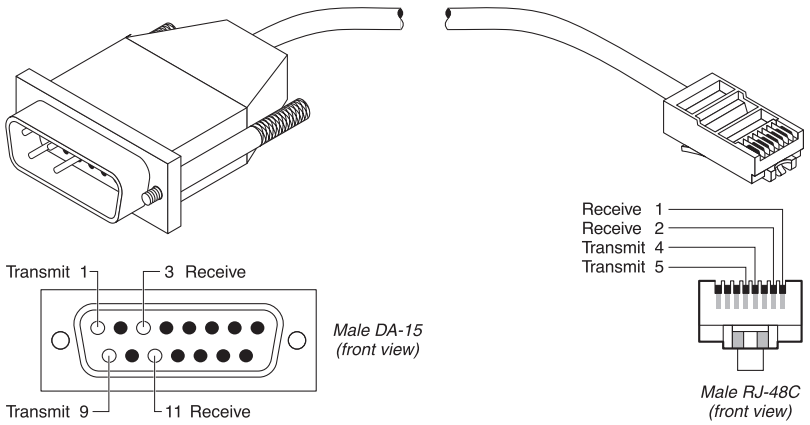


Table D-14.RJ48C/DA-15 straight-through cable specifications

Model number DA15-X Part number 2510-0082-001			
Pair #	**Signal (MultiVoice Gateway)**	**Male RJ48C (MultiVoice Gateway)**	**Male DA-15P (remote)**
1	Receive	1 2	3 11
2	Transmit	5 4	1 9

E1/PRI crossover cable: RJ48C/DA

Before installing the RJ48C/DA crossover cable, verify that the WAN transmits on pins 1 and 9 and receives on pins 3 and 11. Refer to Figure D-10 and Table D-15.

Figure D-10.RJ48C/DA crossover cable

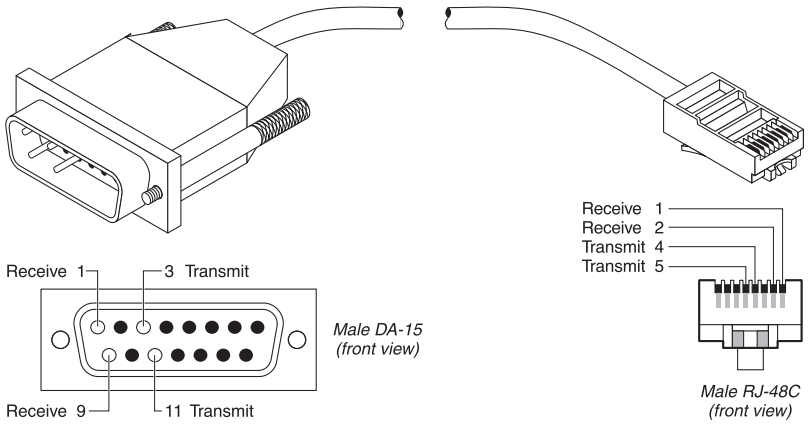


Table D-15.RJ48C/DA crossover cable specifications

Model number DA15-S Part number 2510-0065-001			
Pair #	**Signal (MultiVoice Gateway)**	**Male RJ48C (MultiVoice Gateway)**	**Male DA-15P (remote)**
1	Receive	1 2	1 9
2	Transmit	5 4	3 11

E1/PRI straight-through cable: RJ48C/Bantam

The WAN side of the RJ48C/Bantam straight-through cable connects to dual bantam jacks. Refer to Figure D-11 and Table D-16.

Figure D-11.RJ48C/Bantam straight-through cable

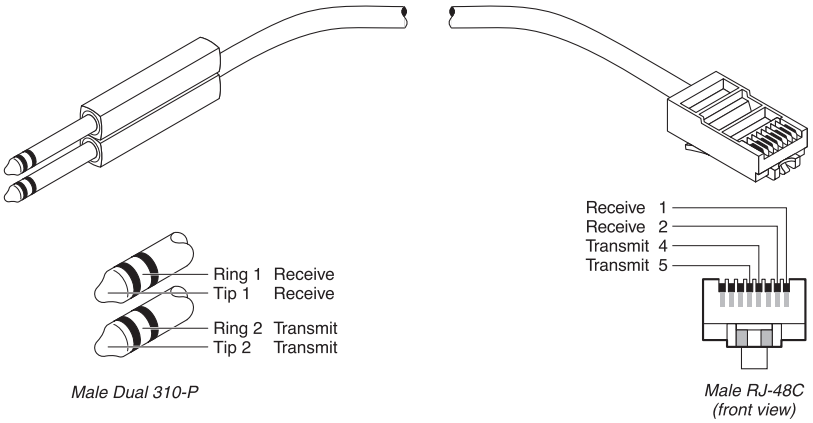


Table D-16.RJ48C/Bantam straight-through cable specifications

Model number DBNT-RJ45 Part number 2510-0066-001			
Pair #	**Signal (MultiVoice Gateway)**	**Male RJ48 (MultiVoice Gateway)**	**Male Dual - 310P (remote)**
1	Receive	1 2	Tip 1 Ring 1
2	Transmit	5 4	Tip 2 Ring 2

E1/PRI straight-through cable: MultiVoice Gateway BNC to RJ48C

The MultiVoice Gateway BNC to RJ48C straight-through cable adapts a modular E1 port on the MultiVoice Gateway to coaxial cable E1 lines. You must also set the jumpers within the MultiVoice Gateway for 50 Ohm service. Refer to Figure D-12 and Table D-17.

Figure D-12.MultiVoice Gateway BNC to RJ-48C straight-through cable

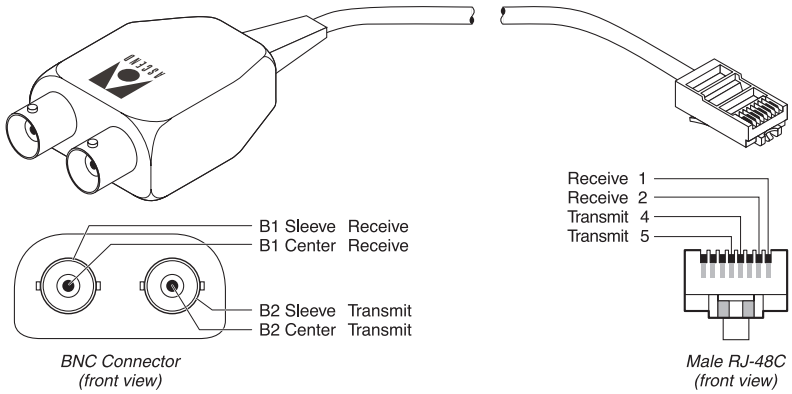


Table D-17.MultiVoice Gateway BNC to RJ-48C straight-through cable specifications

Part number 2510-0272-001			
Pair #	**Signal (MultiVoice Gateway)**	**Male RJ48-C (MultiVoice Gateway)**	**Male Dual - BNC (remote)**
1	Transmit	4 5	B1 Sleeve B1 Center
2	Receive	1 2	B2 Sleeve B2 Center

E1/PRI WAN ports

Table D-18 lists the pins on RJ48C sockets on the MultiVoice Gateway used for E1/PRI WAN interface. Only pins 1, 2, 4, and 5 are used. The remaining pins are not connected.

Table D-18.Transmit and Receive pins

MultiVoice Gateway E1/PRI interface	RJ48C DTE
Receive (input) pair, Tip (T1) Receive (input) pair, Ring (R1)	Position 2 Position 1
Transmit (output) pair, Tip (T) Transmit (output) pair, Ring (R)	Position 5 Position 4

Note: E1/PRI models are also equipped with BNC connectors.

ISDN BRI interface specifications

This section provides the specifications for the MultiVoice Gateway unit's ISDN BRI interface.

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

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

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

For the Net/BRI module

The Net/BRI module (MX-SL-8BRIN) connects to the WAN through a network termination (NT1) device. You must install a cable from the NT1 that ends in a 100Ω termination. The maximum distance between the NT1 and its termination is 3280 feet (1000 m). You can install the Net/BRI module anywhere along the length of the cable. Use only cable specifically constructed for ISDN BRI interfaces.

Note: In Belgium, install 10 m of cable between the Net/BRI module and the NT1. Significant data errors can result from use of shorter cables.

For the Host/BRI module

Each ISDN BRI line provided by the Host/BRI module (MX-SL-8BRIT) must end in a 100Ω termination. The maximum cable distance between the Host/BRI and its termination is 3280 feet (1000 m). You can install the local ISDN BRI device anywhere along the length of the cable. Use only cable specifically constructed for ISDN BRI S interfaces.

Cable length requirements

Table D-19 specifies the recommended maximum length of the cable between the MultiVoice Gateway and the serial host equipment. Longer distances at the specified data rates are possible when you use terminal timing, and still longer distances are supported by the installation of the Ascend RPM, a hardware device that provides an extended distance high-speed link between the MultiVoice Gateway and the serial host equipment.

Table D-19.Cable length requirements

Max cable length	Serial data rate
25 feet	3 Mbps
75 feet	2 Mbps
150 feet	512 Kbps

Serial WAN cabling specifications

The MultiVoice Gateway unit's serial WAN interface supports nailed-up connections to the WAN. Data packets from the MultiVoice Gateway unit's bridge/router module can use this interface, but bit streams from devices connected to the MultiVoice Gateway unit's serial host ports cannot.

The MultiVoice Gateway unit's serial WAN port is compatible with the following two electrical standards:

- V.35
- RS-449/422

In the cable wiring tables that follow, the MultiVoice Gateway is the Data Terminal Equipment (DTE) that connects to a Data Circuit-Terminating Equipment (DCE) device through its serial WAN port. The MultiVoice Gateway receives the Send timing and Receive timing clocks from the DCE device.

V.35 cable to WAN

You connect a V.35 cable to the V.35 port of a DCE device. Table D-20 describes the V.35 cable pinouts.

Table D-20.V.35 cable pinouts

Pair #	Signal (MultiVoice Gateway)	MultiVoice Gateway male DB-44 (MultiVoice Gateway)	Host male V.35
1	FGND RI	1 8	A J
2	SD+ SD-	39 40	P S
3	RD+ RD-	30 29	R T
4	ST+ ST-	41 42	Y AA
5	RT+ RT-	32 31	V X
6	TT+ TT-	38 37	U W
7	DTR DSR	6 11	H E
8	DCD SGND	9 25	F B
9	CTS RTS	7 36	D C

RS-449 cable to WAN

You can connect an RS-449 cable to the RS-449 port of a DCE device. The RS-449 cable has the pinouts described in Table D-21.

Table D-21.RS-449 cable pinouts

Pair #	Signal (MultiVoice Gateway)	MultiVoice Gateway male DB-44 (MultiVoice Gateway)	Host female DB-37
1	FGND RI	1 8	1 15
2	SD+ SD-	39 40	4 22
3	RD+ RD-	30 29	6 24
4	ST+ ST-	41 42	5 23
5	RT+ RT-	32 31	8 26
9	TT+ TT-	38 37	17 35
8	DTR DSR	6 11	12 11
6	DCD SGND	9 25	13 19, 20, 37*
7	CTS RTS	7 36	9 7

Note: *Pin positions separated by commas are jumped to each other.

Warranties and FCC Regulations

E

Product warranty

1 Ascend Communications, Inc. 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 Communications, Inc. shall incur no liability under this warranty if

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

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

4 Ascend Communications, Inc. MAKES NO EXPRESS OR IMPLIED WARRANTIES REGARDING THE QUALITY, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE BEYOND THOSE THAT APPEAR IN THE APPLICABLE Ascend Communications, Inc. USER'S DOCUMENTATION. Ascend Communications, Inc. 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 Communications, Inc. 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 Communications, Inc. 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 Communications, Inc. will ship surface freight. Expedited freight is at customer's expense.

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

Out-of warranty repair

Ascend Communications, Inc. 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.

FCC Part 15 Notice

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 or her 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 Communications, Inc.

FCC Part 68 Notice

This Ascend equipment complies with Part 68 of the FCC rules. Located on the equipment is a label that contains, among other information, the FCC registration number. If requested, this information must be provided to the telephone company.

This equipment cannot be used on the telephone company-provided coin service. Connection to Party Line Service is subject to State Tariffs.

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. If advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment. operations, or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make the necessary modifications in order to maintain uninterrupted service.

If trouble is experienced with this equipment, please contact:

Ascend Communications, Inc.
1701 Harbor Bay Parkway
Alameda, CA 94502

If the trouble is causing harm to the telephone network, the telephone company may request you to remove the equipment from the network until the problem is resolved.

It is recommended that the customer install an AC surge arrestor in the AC outlet to which this device is connected. This is to avoid damage to the equipment caused by local lightening strikes and other electrical surges.

This equipment uses the following USOC jacks and codes:

Model Name	Facility Interface Code	Service Order Code	Jack Type
MAX 6000 T1	04DU9-BN	6.0N	RJ48C
MAX 6000 T1	04DU9-DN	6.0N	RJ48C
MAX 6000 T1	04DU9-1KN	6.0N	RJ48C
MAX 6000 T1	04DU9-1SN	6.0N	RJ48C
MAX 6000 T1	04DU9-1ZN	6.0N	RJ48C
MAX 4000 T1	04DU9-BN	6.0N	RJ48C
MAX 4000 T1	04DU9-DN	6.0N	RJ48C
MAX 4000 T1	04DU9-1KN	6.0N	RJ48C
MAX 4000 T1	04DU9-1SN	6.0N	RJ48C
MAX 2000 T1	04DU9-BN	6.0N	RJ48C
MAX 2000 T1	04DU9-DN	6.0N	RJ48C
MAX 2000 T1	04DU9-1KN	6.0N	RJ48C
MAX 2000 T1	04DU9-1SN	6.0N	RJ48C
MAX 2000 T1	04DU9-1ZN	6.0N	RJ48C

IC CS-03 Notice

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). 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. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative 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 to rural areas.

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

Index

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z