MultiVoice Access Manager User's Guide

Ascend Communications, Inc.
Part Number: 7820-0584-002
For software version 2.0.0
November 12, 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.

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.

Obtaining Technical Assistance

You can obtain technical assistance by telephone, email, fax, or modem, as well as 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 line.
- 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.

Contacting 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

Contents

Figures

Tables

About This Guide

This guide explains how to install, configure, administer, and troubleshoot the MultiVoice Access Manager (MVAM).

Note: Certain new features added to MultiVoice Access Manager Release 2.0.0 are only supported on networks which use MultiVoice Gateways running TAOS Release 7.0.0 of the *MultiVoice for the MAX* software. These features are not available on networks which use MultiVoice Gateways running TAOS Release 6.x.x of the MultiVoice for the MAX.

How to use this guide

Following is a chapter-by-chapter description of how to use this guide:

- Chapter 1, “Introducing MultiVoice concepts,” provides a brief overview of traditional voice communications and describes several applications of MultiVoice in a voice communications network.
- Chapter 2, “Setting Up MultiVoice Access Manager,” explains how to install and launch the MultiVoice Access Manager, and how to install and configure a World Wide Web (WWW) server to work with MVAM.
- Chapter 3, “Configuring the MultiVoice Access Manager,” describes how to connect to the MVAM from supported Web browsers. The chapter also explains how to configure users, MultiVoice Gateways, dialing prefixes, telephone aliases, and security on the MVAM.
- Chapter 4, “MultiVoice Gateway Administration,” discusses monitoring and log information. The chapter also explains how to locate MultiVoice Gateways for callers, and how to display the MVAM version and license information.

- Chapter 5, “Troubleshooting,” presents common problems, error messages, and troubleshooting tips.
- Appendix A, “MVAM initialization file,” lists the possible values for each parameter in the MultiVoice Access Manager Initialization file.
- Appendix B, “Upgrading the MVAM License,” describes how to upgrade the license of the MVAM.
- Appendix C, “Warranty,” discusses warranty information.

The guide also includes an index.

What you should know

This guide is for the person who configures and maintains the MultiVoice Access Manager. To configure the MVAM, you need to know:

- Basic voice telecommunications concepts
- Wide area network (WAN) concepts
- Local area network (LAN) concepts

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.

Convention	Meaning
Italics	Represent variable information. Do not enter the words themselves in the command. Enter the information they represent. In ordinary text, italics are used for titles of publications, for some terms that would otherwise be in quotation marks, and to show emphasis.
[ ]	Square brackets indicate an optional argument you might add to a command. To include such an argument, type only the information inside the brackets. Do not type the brackets unless they appear in bold type.
|	Separates command choices that are mutually exclusive.
>	Points to the next level in the path to a parameter or menu item. The item that follows the angle bracket is one of the options that appears when you select the item that precedes the angle bracket.
Key1-Key2	Represents a combination keystroke. To enter a combination keystroke, press the first key and hold it down while you press one or more other keys. Release all the keys at the same time. (For example, Ctrl-H means hold down the Control key and press the H key.)
Press Enter	Means press the Enter, or Return, key or its equivalent on your computer.
Note:	Introduces important additional information.
 **Caution:**	Warns that a failure to follow the recommended procedure could result in loss of data or damage to equipment.
 **Warning:**	Warns that a failure to take appropriate safety precautions could result in physical injury.

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, which provide such information:

- *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
- *MultiVoice Gateway for the MAX -- User Guide*, Ascend Communications

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 publication. Ascend does not maintain the sites, and cannot guarantee their availability in the future.

Introducing MultiVoice concepts

1

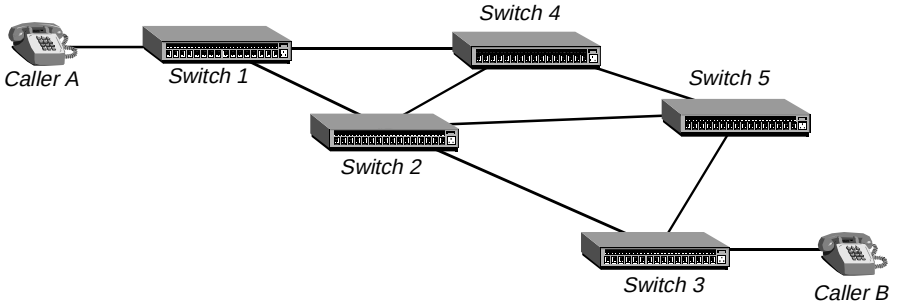
A brief overview

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?

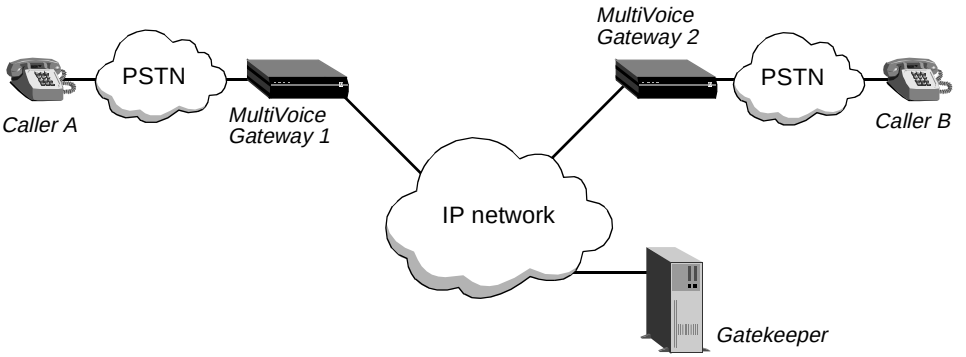
In response to customers wanting to utilize their existing IP networks to support voice communications, the International Telecommunications Union (ITU) has created the ITU-T H.323 standards. H.323 standards define a framework for the transmission of real-time voice communications by means of IP-based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

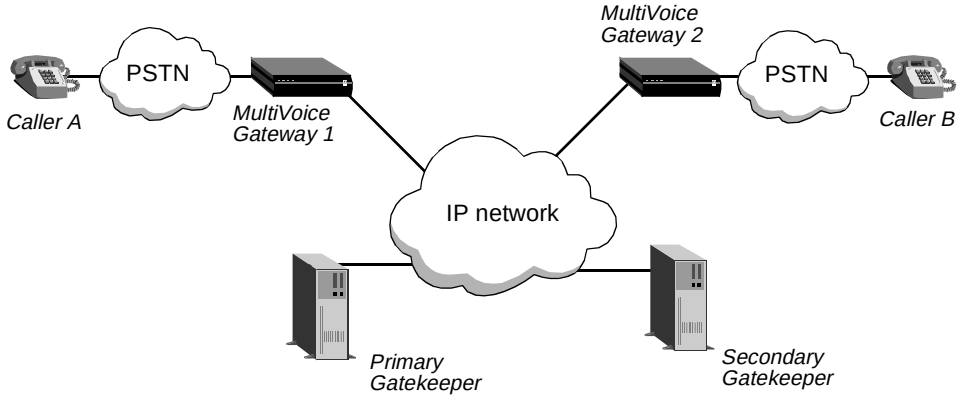
Multivoice network with a secondary Gatekeeper

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 the authentication passcode (if required) and Caller B's phone number.

2 MultiVoice Gateway 1 attempts to register with its 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 authentication passcode 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).

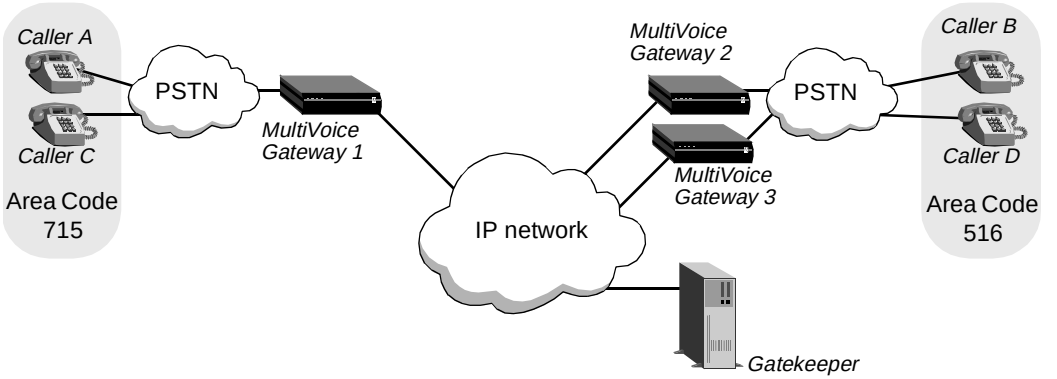
MultiVoice network with overlapping coverage areas

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 authentication passcode 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 authentication passcode 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

Basic public long-distance service

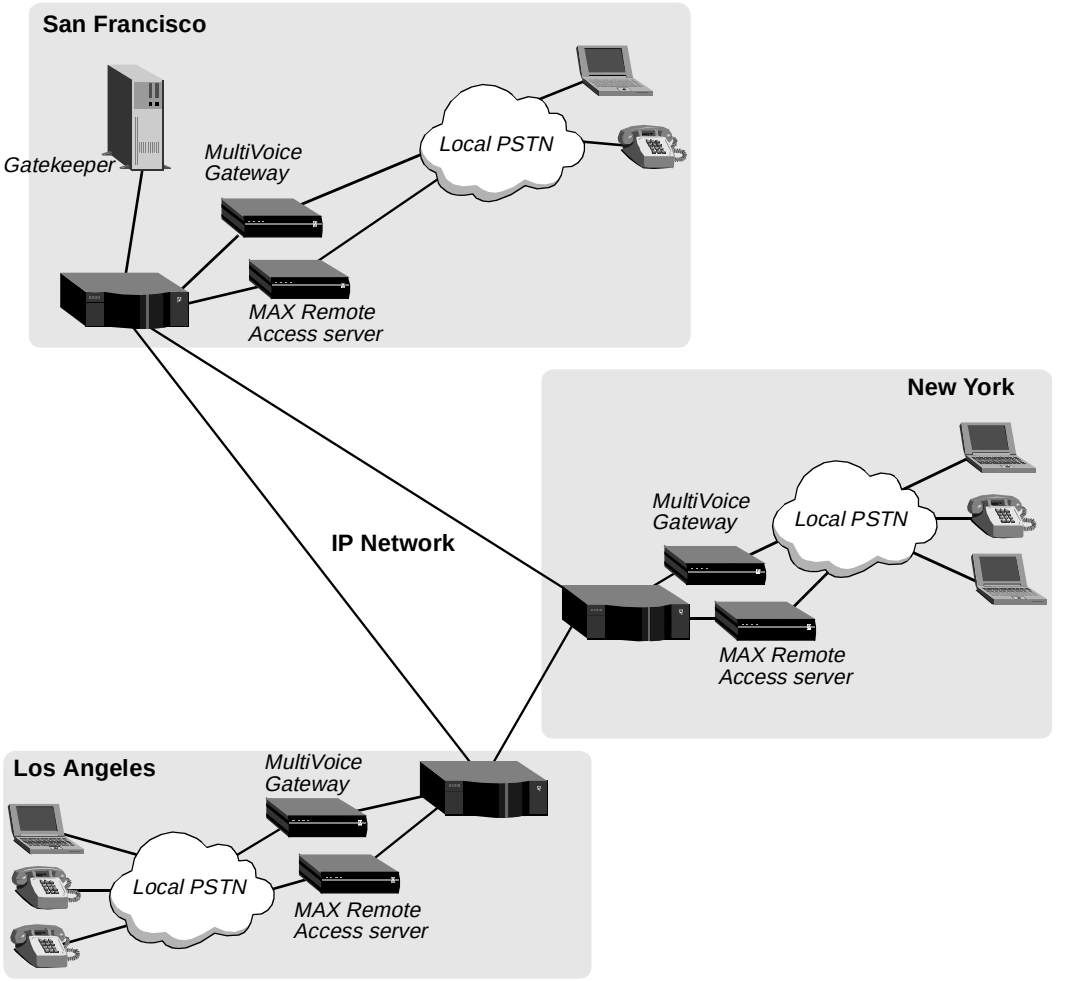
Basic public long-distance service is the most beneficial to Competitive Local Exchange Carriers (CLECs) and Internet Service Providers (ISPs) that:

- 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.

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.

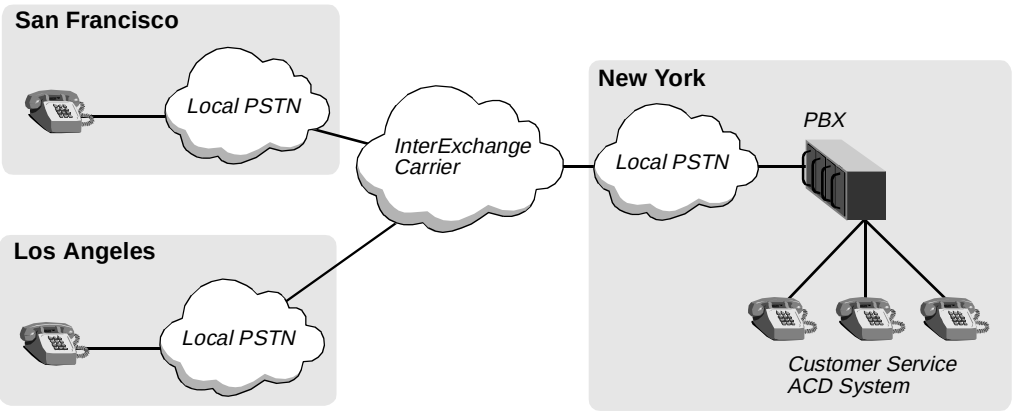
Local 800 service

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



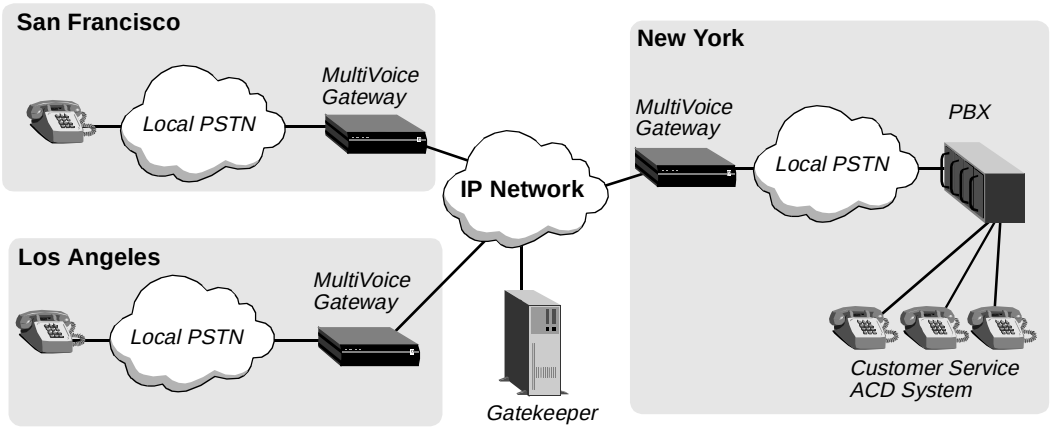
To reach a customer service representative, callers in San Francisco and Los Angeles dial an 800 or 888 phone number, which has been leased to a company's customer service department by its InterExchange Carrier (IXC).

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

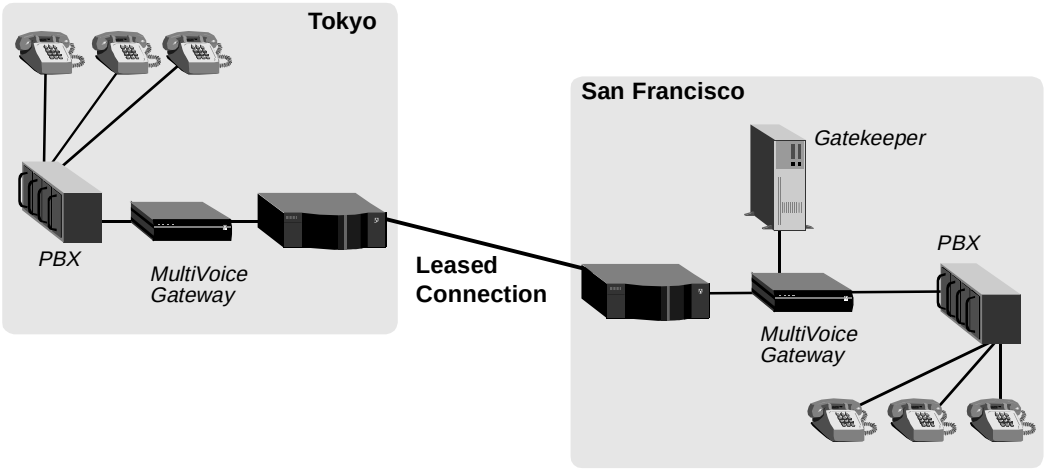


Instead of leasing traditional 800 service, the company leases local 800 service in San Francisco and Los Angeles. Each local PSTN routes local 800 calls to a local MultiVoice Gateway, which forwards them to the customer service site in New York.

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

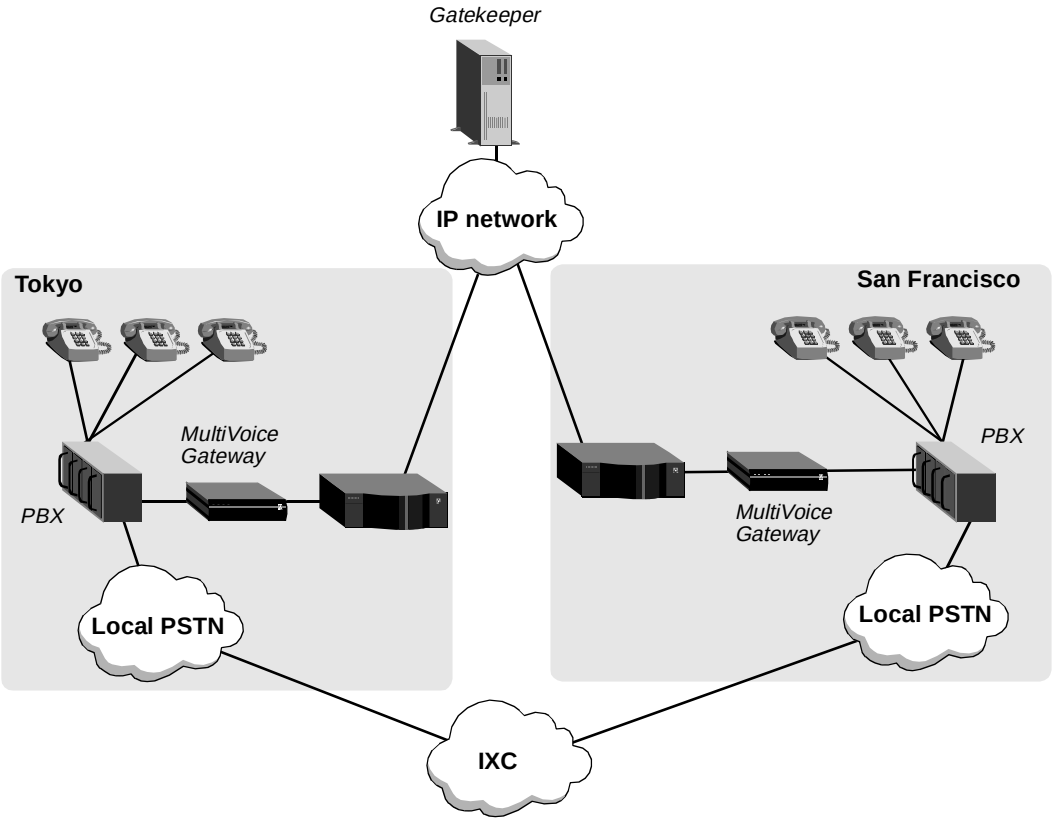


The two sites are connected by a core B-STDX network, which supports both packetized data and voice traffic. The Priority Frame standard within the B-STDX network maintains QoS.

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.

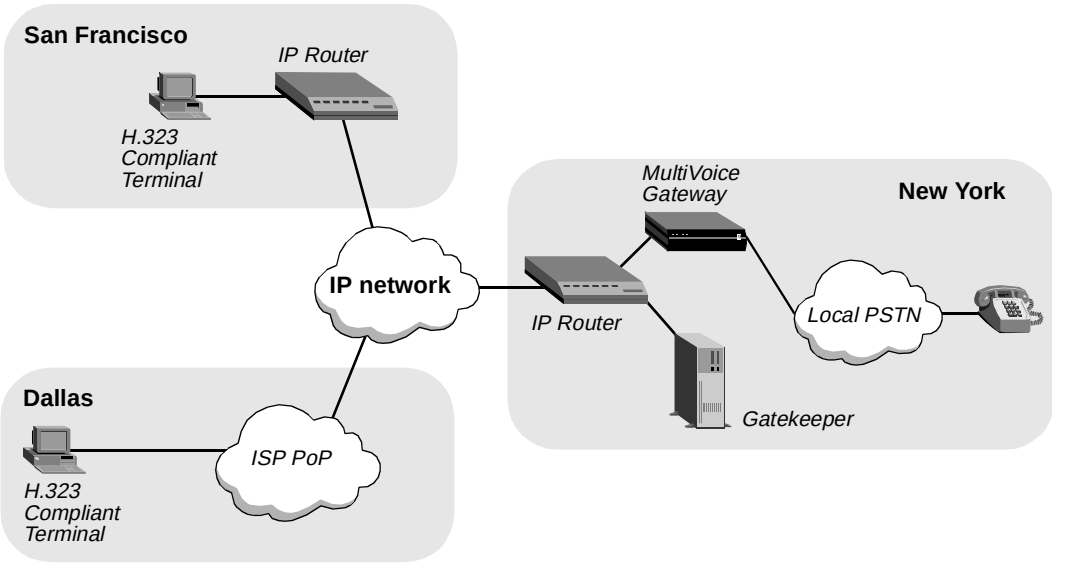
This architecture can also support PBX intraflow. The PBX can be configured to routes calls to the alternative path when all trunks between PBXs are in use. PBX

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.

Setting Up MultiVoice Access Manager

2

Before you begin

Before you install MultiVoice Access Manager (MVAM), make sure that you have everything you need. The package in which you received the product contains:

- The MultiVoice Access Manager CD-ROM.
- A MultiVoice Access Manager Warranty Registration card from which you need the product serial number.
- This manual.

System requirements

To install MVAM, you need a computer in which you have installed Windows NT 4.0 (either the Workstation or the Server version) or Solaris 2.5.l or later.

Minimum configuration for Windows NT systems

The minimum system configuration for installing MultiVoice Access Manager on a Windows NT system are:

- Pentium 100 MHz CPU
- 32 Mb of system RAM
- 2 GB hard disk
- CD-ROM drive
- 10/100 Base-T network interface card

Minimum configuration for SPARC Solaris systems

The minimum system configuration for installing the MultiVoice Access Manager on a SPARC Solaris system are:

- 64 Mb of system RAM
- 250 Kb of hard disk space
- CD-ROM drive
- 10/100 Base-T network interface

Network requirements

To use MultiVoice Access Manager, you need properly configured IP-networking software, a compatible Web browser, and a compatible Web server.

IP-networking software

Both Windows NT 4.0 and Solaris 2.5.1 include software that supports TCP/IP networking. The MVAM needs such software to communicate with MultiVoice Gateways and with external Web browsers. Make sure that the TCP/IP software has been installed and configured as directed by the system documentation for your computer and by your network administrator.

Web browser software

You have to use a Web browser to connect to MVAM so that you can configure and monitor the MultiVoice network. The browser can be on the same computer that runs MVAM or on a different computer. MVAM supports the following browsers:

- Netscape Navigator, version 3.01 or later
- Microsoft's Internet Explorer, version 3.02 or later

Web server software

To enable a Web browser to connect the MVAM Web pages, the computer running the MVAM must also be running a Web server. Any third-party Web server that supports the standard Common Gateway Interface (CGI) should be compatible with MVAM. But you might want to use one that has been tested.

On Windows NT 4.0 systems, the following Web servers have been successfully tested and proven compatible with MultiVoice Access Manager:

- Microsoft's Internet Information Server (IIS), version 3.0 or later, available from Microsoft at `http://www.microsoft.com`.
- Imatix's Xitami Web server, version 1.3c or later, available from Imatix at `http://www.imatix.com`.

On SPARC Solaris systems, the Apache Web Server, version 1.2.5 or later, available from `http://www/apache.org`, has been successfully tested and proved compatible with MultiVoice Access Manager.

Note: Microsoft's Personal Web Server (PWS) will not work with MVAM. PWS has been optimized for interactive workstation use, and does not have the system requirements of a full Web server such as IIS.

MultiVoice Gateway licensing

Depending on which package was purchased, MVAM running on a Windows NT system supports a maximum of 4, 32, or 128 MultiVoice Gateways. The MVAM running on a SPARC Solaris system supports a maximum of either 32 or 256 MultiVoice Gateways.

Installing a Web server

A local Web server must be installed and running on the system before you install the MultiVoice Access Manager. To install the server, follow the installation instructions provided by the manufacturer.

MVAM-specific configuration usually consist of:

- Setting the location of the MVAM HTML files. On a Windows NT system, the HTML files are located in the `webpages` subdirectory of the MVAM installation directory. On a SPARC Solaris system, the HTML files are located in the `htdocs` subdirectory along the selected directory path.
- Setting the location of the CGI directory. On a Windows NT system, `mvam_cgi.exe` is located in the `cgi-bin` subdirectory of the MVAM installation directory. On a SPARC Solaris system, `mvam_cgi.exe` is located in the `cgi-bin` subdirectory along the same path as the `htdocs` subdirectory.

Restart your Web server to ensure the new values are set before you launch MVAM. Configuration information for tested Web servers is in the *MultiVoice Access Manager Web Server Configuration Application Note*.

Installing MultiVoice Access Manager

Procedures for installing and launching MVAM depend on whether you use a Window NT or Solaris system.

Caution: When you have installed and configured MVAM, be sure to restrict access to it by means of firewalls, filters, or password protection. Otherwise, once MVAM is installed, anyone can connect to it with a supported Web browser.

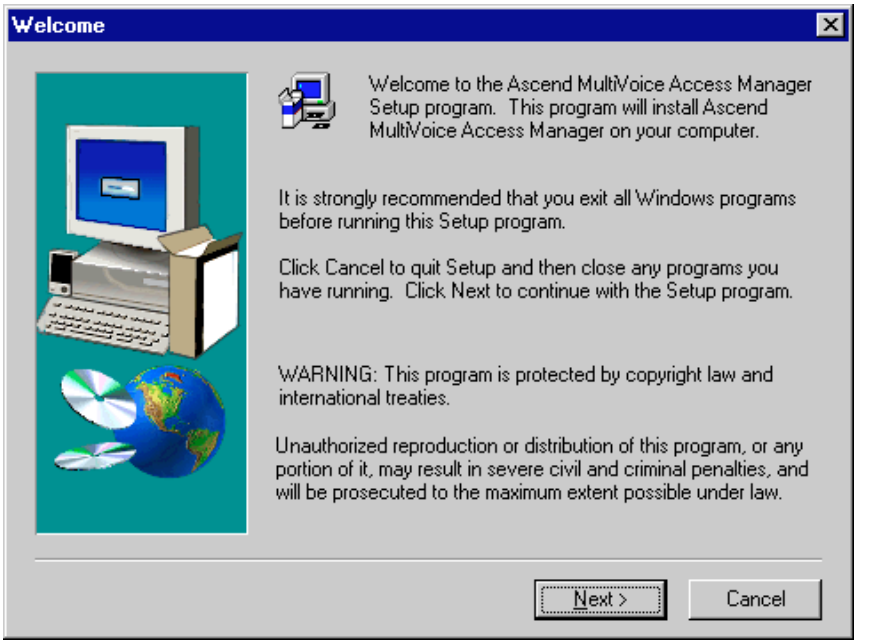
Caution: Before upgrading from MultiVoice Access Manager Release 1.0.0 to Release 2.0.0, you should back up the files in the `db` and `calls` subdirectories, including the `calls/current/calls`. You should also uninstall the Release 1.0.0 software before installing Release 2.0.0.

Installation on a Windows NT 4.0 system

To install MVAM on a computer running a Windows NT 4.0 Server or Workstation, first exit all programs, then put the MultiVoice Access Manager CD-ROM in the CD-ROM drive.The installation program should autorun. If it does not, launch the executable file named `setup.exe`, and follow the instructions which appear on your screen.

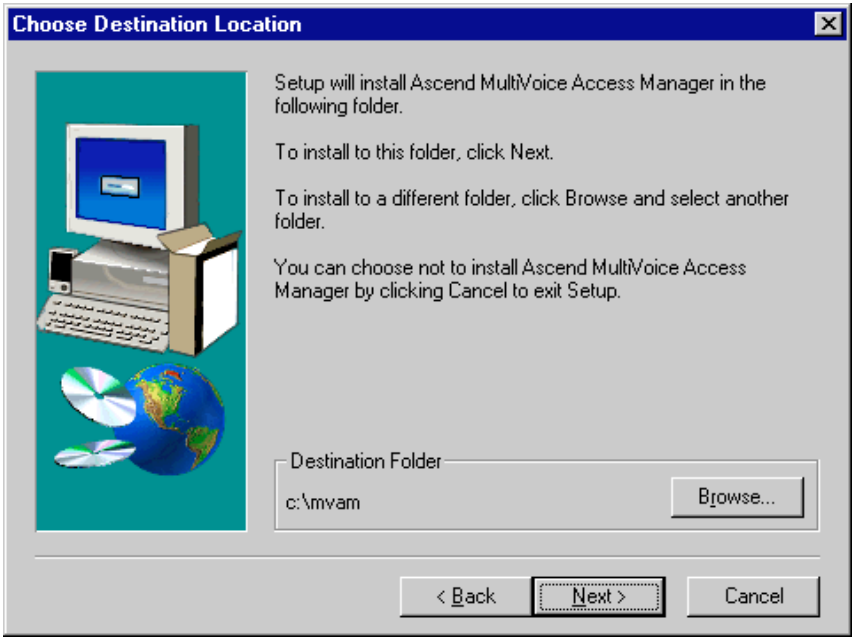
The rest of this section describes the process in more detail. (For additional information see the README file on the CD-ROM.)

A setup wizard loads the file and displays the following screen:



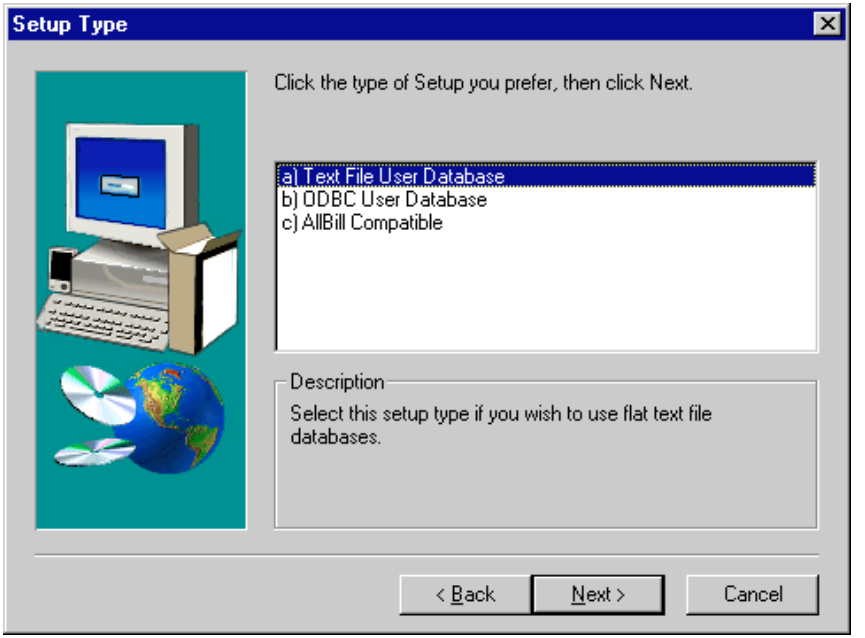
This screen is the first of several that explain the installation process and prompt you for additional information. In most circumstances, you should accept the default values.

When you click the Next button, the wizard displays the following screen:



You may specify any folder as the destination for the MVAM files.

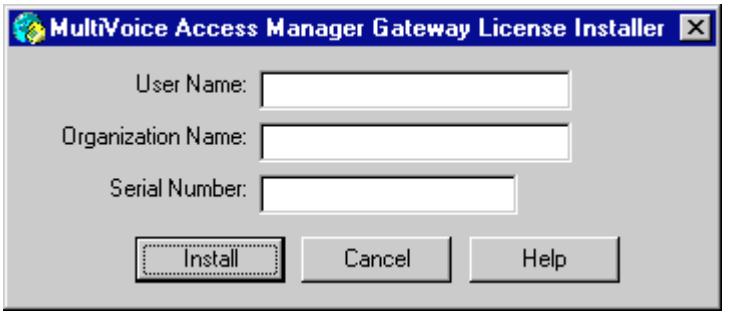
When you click the Next button, the Wizard displays the following screen:



Select one of the following types of user-database storage for the MVAM to use:

Setup type	**Description**
Text File User Database	Select this method if you will enter user information by means of the MVAM browser screens. The MVAM stores user information in an ASCII file. This is the default setting.
ODBC User Database	Select this method if you use a third-party application that uses a database compliant with Microsoft's Open DataBase Connectivity (ODBC).
AllBill Compatible	Select this method if you use the AllBill billing application to store your information.

When you select a setup type and click the Next button, the License Installer displays the following dialog box:



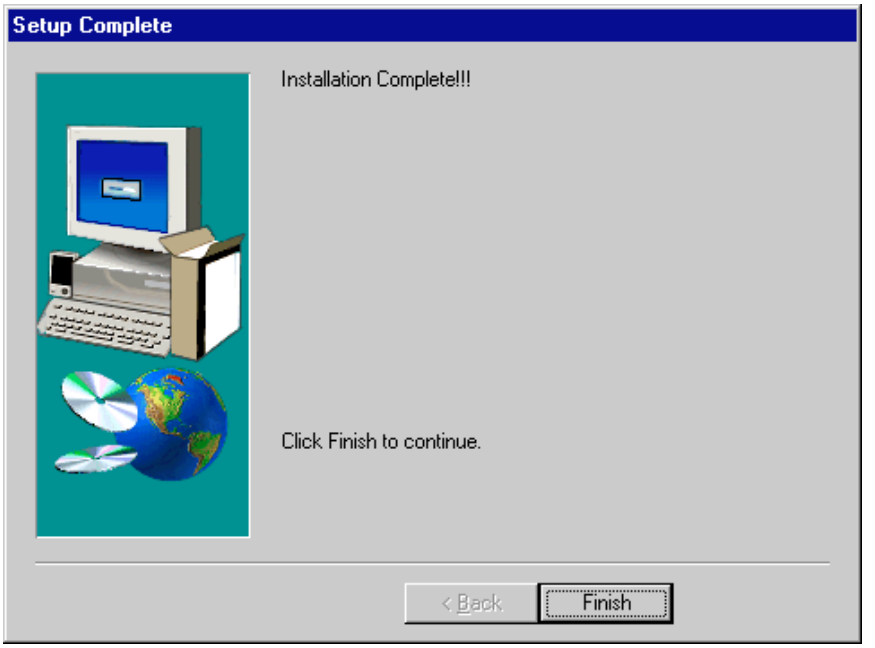
In the MVAM Gateway License Installer screen:

- Enter your name or the name of the person who would use the program.
- Enter the name of your organization.
- Enter the serial number that is printed on the registration card included in the installation package. If you enter an incorrect serial number, the Installer does not install the license, and the MVAM will not run.
- Click the Install button. The message '`Please Wait...`' appears on the screen.

Note: After installation, you can verify the results of the upgrade from a Web browser by connecting to the MVAM application and clicking `license` on the main MVAM screen.

Note: When upgrading licenses, you can run the License Installer whether or not the MVAM is running, but the upgrade does not take effect until you restart the program.

The wizard displays the following screen:



When you click the Finish button, the wizard finishes installing the application.

Note: If you upgrade from MultiVoice Access Manager Release 1.0.0 to Release 2.0.0, you should restore the files in the `db` and `calls` subdirectories, including the `calls/current/calls.txt` file, before starting the application.

Installation on a Solaris system

To install MultiVoice Access Manager (MVAM) on a SPARC workstation or server, use the UNIX `pkgadd` command. During the installation, you are asked to define the MVAM user and the installed location(s) for the MVAM software. You must perform the installation as the `root` user. The rest of this section describes the process in more detail. (For additional information see the README file on the CD-ROM.)

To install, first load the MVAM CD-ROM in the SPARC workstation or server. Ensure the CD-ROM is mounted. (The following instructions assume that `/cdrom` is the mount point.)

To install the MVAM:

1 Execute `pkgadd` from the mounted CD-ROM:

`pkgadd -d /cdrom/asndmvam ASNDmvam`

The `pkgadd` command displays a series of prompts. The first set of prompts controls administration and user access to the MVAM files. The prompts display the default values, inside parentheses, for each entry.

2 To display a brief explanation of a prompt, enter a **`?`** then press `Return`. To accept the default, press `Return`. To abort installation, enter **`q`** then press `Return`.

3 First, you are prompted to enter the name of the MVAM user, using a valid user ID (UID), who will own the MVAM files and directories:

```
MVAM user (bin) [?,q]
```

This UID must be known to the SPARC system where you are installing the software. Additional users (UIDs) may be granted access to the MVAM later. Do not enter root as the MVAM user.

4 Next, you are prompted to enter the user group associated with the MVAM user:

```
MVAM group (other) [?,q]
```

Members of this group may administer the MVAM (e.g., modify the configuration files, add or delete database information, etc.). Do not enter root as the MVAM group.

5 You are then prompted for the name of the MAVM installation directory. You may specify either a new or existing directory:

```
MVAM top level directory (/opt/mvam) [?,q]
```

The MVAM user, and any other users added after installation, must have write permission for this directory.

6 You are then prompted for the name of the MVAM Web page directory, where the Web server will find the MVAM user interface pages:

```
MVAM Web page directory (/opt/mvam/htdocs) [?,q]
```

It is recommended that you set this value to the name of your Web server's top level HTML page directory.

7 The next prompt asks for the name of the directory in which the MVAM CGI adapter will be installed. The Web server must know the location of this directory in order to execute administration requests for the MVAM:

```
MVAM CGI host directory (/usr/local/apache/cgi-bin) [?,q]
```

This prompts defaults to a value relative to the MVAM Web page directory. It is recommended that you set this value to the name of your Web server's cgi-bin directory.

8 The next prompt asks for the location of the MVAM $HOME directory. This is the value assigned to the UNIX $HOME variable when the MVAM runs:

```
MVAM $HOME directory (/opt/mvam) [?,q]
```

This is the value assigned to the UNIX $HOME variable when the MVAM runs. This prompt defaults to the same value as the MVAM top level directory.

Note: When your selected directory doesn't exist for the entries in the MVAM Web page directory, the MVAM CGI host directory or the MVAM $HOME directory prompts, the following prompt appears:

```
/usr/mvam/mvamuser does not exist; create it? y
```

Press Return to create the directory (default).

9 You are then prompted to enter the MultiVoice Gateway license information. user name, organization and serial number from the MultiVoice Access Manager registration card. For example:

```
User name :John Doe
Organization name :Generic ISP
Serial number: MVAM-200-AR-99999999
```

```
Please Wait...
```

10 The pkgadd command verifies that all values have been entered, then prompts you to confirm the MVAM installation:

```
Using </> as the package base directory.
## Processing package information.
## Processing system information.
## Verifying disk space requirements.
## Checking for conflicts with packages already
installed.
## Checking for setuid/setgid programs.

This package contains scripts which will be executed with
super-user permission during the process of installing
this package.

Do you want to continue with the installation of
<ASNDmvam> [y,n,?]
```

Enter a y and press Return.

11 The pkgadd command copies the application files to the SPARC and installs the MVAM licence(s).

```
Installing Ascend MultiVoice Access Manager as <ASNDmvam>

## Executing preinstall script.
## Installing part 1 of 1.
```

(displays list of files)

```
[ verifying class <none> ]
## Executing postinstall script.
MVAM license installed successfully.

Installation of <ASNDmvam> was successful.
```

12 To verify the software installation, execute the pkgchk command:

pkgchk -n ASNDmvam

If the installation succeeded, the system will display the command prompt. If the installation failed, the system will display any errors detected by pkgchk.

Caution: When you have installed and configured the MVAM, be sure to restrict access to it by means of firewalls, filters, or password protection.

Otherwise, once MVAM is started, anyone can connect to it with a supported Web browser.

Example of an MVAM installation on a Solaris system

The following is an example of how to install MVAM on a Solaris system using the `pkgadd` command:

```
# pkgadd -d /cdrom/asndmvam ASNDmvam

Processing package instance <ASNDmvam> from
</home/psrc/src/mvam/pkg/SPOOLDIR>

Ascend MultiVoice Access Manager
(sparc) 2.0.0
Ascend MultiVoice Access Manager
Copyright (c) 1998 Ascend Communication, Inc.
All rights reserved

MVAM user (bin) [?,q] mvamuser

MVAM group (other) [?,q] mvamgroup

MVAM top level directory (/opt/mvam) [?,q]

MVAM Web page directory (/opt/mvam/htdocs) [?,q]
/usr/local/apache/htdocs

MVAM CGI host directory (/usr/local/apache/cgi-bin) [?,q]

MVAM $HOME directory (/opt/mvam) [?,q] /usr/mvam/mvamuser

/usr/mvam/mvamuser does not exist; create it? y

User name: MVAM administrator
Organization name: VoIP networking group
Serial number: MVAM-200-AQ-99999999

Using </> as the package base directory.
## Processing package information.
## Processing system information.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.
## Checking for setuid/setgid programs.

This package contains scripts which will be executed with
super-user permission during the process of installing this
package.
```

```
Do you want to continue with the installation of <ASNDmvam>
[y,n,?] y

Installing Ascend MultiVoice Access Manager as <ASNDmvam>
## Executing preinstall script.
## Installing part 1 of 1.
/opt/mvam/README
/opt/mvam/bin/config.val
/opt/mvam/bin/daemons
/opt/mvam/bin/h323.raw
/opt/mvam/bin/mvam
/opt/mvam/bin/mvam.sh
/opt/mvam/bin/mvam_cgi
/opt/mvam/bin/textlicapp
/opt/mvam/lib.sol2/libcommctrl42.so
/opt/mvam/lib.sol2/libcommdlg42.so
/opt/mvam/lib.sol2/libgdi42.so
/opt/mvam/lib.sol2/libkernel42.so
/opt/mvam/lib.sol2/libmfc42.so
/opt/mvam/lib.sol2/libodbc42.so
/opt/mvam/lib.sol2/libole42.so
/opt/mvam/lib.sol2/libolest42.so
/opt/mvam/lib.sol2/libprnt42.so
/opt/mvam/lib.sol2/libriched42.so
/opt/mvam/lib.sol2/libshell42.so
/opt/mvam/lib.sol2/libuser42.so
/opt/mvam/lib.sol2/libwininet42.so
/opt/mvam/lib.sol2/libwinsock42.so
/opt/mvam/lib.sol2/regedit
/opt/mvam/lib.sol2/windu_client
/opt/mvam/lib.sol2/windu_clientd42
/opt/mvam/lib.sol2/windu_registry
/opt/mvam/lib.sol2/windu_registryd42
/usr/local/apache/cgi-bin/mvam_cgi.exe
/usr/local/apache/htdocs/abouth.htm
/usr/local/apache/htdocs/acodeh.htm
/usr/local/apache/htdocs/adialh.htm
/usr/local/apache/htdocs/aliastransh.htm
/usr/local/apache/htdocs/alphaih.htm
/usr/local/apache/htdocs/background.jpg
```

```
/usr/local/apache/htdocs/caccfcfh.htm
/usr/local/apache/htdocs/cacch.htm
/usr/local/apache/htdocs/cacco.htm
/usr/local/apache/htdocs/caccoh.htm
/usr/local/apache/htdocs/ccodeh.htm
/usr/local/apache/htdocs/checkb.gif
/usr/local/apache/htdocs/clogh.htm
/usr/local/apache/htdocs/cmptnumh.htm
/usr/local/apache/htdocs/crth.htm
/usr/local/apache/htdocs/cstatush.htm
/usr/local/apache/htdocs/dialih.htm
/usr/local/apache/htdocs/dprefh.htm
/usr/local/apache/htdocs/dprefmod.htm
/usr/local/apache/htdocs/dprefmodh.htm
/usr/local/apache/htdocs/e164h.htm
/usr/local/apache/htdocs/elegant_double.gif
/usr/local/apache/htdocs/error.gif
/usr/local/apache/htdocs/eventh.htm
/usr/local/apache/htdocs/formsh.htm
/usr/local/apache/htdocs/gkih.htm
/usr/local/apache/htdocs/gwadd.htm
/usr/local/apache/htdocs/gwaddh.htm
/usr/local/apache/htdocs/gwadmin.htm
/usr/local/apache/htdocs/gwadminh.htm
/usr/local/apache/htdocs/gwcah.htm
/usr/local/apache/htdocs/gwcityh.htm
/usr/local/apache/htdocs/gwcmh.htm
/usr/local/apache/htdocs/gwcmod.htm
/usr/local/apache/htdocs/gwcmodh.htm
/usr/local/apache/htdocs/gwcountryh.htm
/usr/local/apache/htdocs/gwcquery.htm
/usr/local/apache/htdocs/gwcqueryh.htm
/usr/local/apache/htdocs/gwcs.htm
/usr/local/apache/htdocs/gwdbh.htm
/usr/local/apache/htdocs/gwh.htm
/usr/local/apache/htdocs/gwloc.htm
/usr/local/apache/htdocs/gwloch.htm
/usr/local/apache/htdocs/gwloctnumh.htm
/usr/local/apache/htdocs/gwmod.htm
/usr/local/apache/htdocs/gwmodh.htm
```

```
/usr/local/apache/htdocs/gwnameh.htm
/usr/local/apache/htdocs/gwquery.htm
/usr/local/apache/htdocs/gwqueryh.htm
/usr/local/apache/htdocs/gwrem.htm
/usr/local/apache/htdocs/gwremh.htm
/usr/local/apache/htdocs/gwstateh.htm
/usr/local/apache/htdocs/gwstatquery.htm
/usr/local/apache/htdocs/gwstatqueryh.htm
/usr/local/apache/htdocs/gwstreeth.htm
/usr/local/apache/htdocs/gwtnumh.htm
/usr/local/apache/htdocs/gwtnumsh.htm
/usr/local/apache/htdocs/gwziph.htm
/usr/local/apache/htdocs/hdr_h.gif
/usr/local/apache/htdocs/helph.htm
/usr/local/apache/htdocs/incareah.htm
/usr/local/apache/htdocs/index.htm
/usr/local/apache/htdocs/lnumh.htm
/usr/local/apache/htdocs/logo.gif
/usr/local/apache/htdocs/logo2.gif
/usr/local/apache/htdocs/logsh.htm
/usr/local/apache/htdocs/pdialh.htm
/usr/local/apache/htdocs/phoneih.htm
/usr/local/apache/htdocs/ptnumh.htm
/usr/local/apache/htdocs/redball.gif
/usr/local/apache/htdocs/sec.htm
/usr/local/apache/htdocs/sech.htm
/usr/local/apache/htdocs/statush.htm
/usr/local/apache/htdocs/success.gif
/usr/local/apache/htdocs/termh.htm
/usr/local/apache/htdocs/uadd.htm
/usr/local/apache/htdocs/uaddh.htm
/usr/local/apache/htdocs/uadmin.htm
/usr/local/apache/htdocs/uadminh.htm
/usr/local/apache/htdocs/ualiash.htm
/usr/local/apache/htdocs/uauthh.htm
/usr/local/apache/htdocs/udbh.htm
/usr/local/apache/htdocs/uh.htm
/usr/local/apache/htdocs/umod.htm
/usr/local/apache/htdocs/umodh.htm
/usr/local/apache/htdocs/unameh.htm
```

```
/usr/local/apache/htdocs/upinh.htm
/usr/local/apache/htdocs/uquery.htm
/usr/local/apache/htdocs/uqueryh.htm
/usr/local/apache/htdocs/urem.htm
/usr/local/apache/htdocs/uremh.htm
/usr/local/apache/htdocs/utaliash.htm
/usr/local/apache/htdocs/utnumh.htm
/usr/mvam/mvamuser/.mvam.ini

[ verifying class <none> ]
## Executing postinstall script.

MVAM license installed successfully.

Installation of <ASNDmvam> was successful.
```

Starting MVAM

Before you start MVAM, you should familiarize yourself with the subdirectories and files created with MVAM installation. Then you can launch MVAM and configure your MultiVoice network from a supported Web browser.

MVAM directory structure

The directory you selected during MVAM installation contains the following subdirectories, which, by default, are located under `c:\mvam` on a Windows NT system, and under the `/opt/mvam` on a SPARC Solaris system:

Subdirectory	Description
`bin`	Contains the MVAM executable file.
`calls`	Stores call record files.
`cgi-bin`	Contains the Common Gateway Interface (CGI) executable. The MVAM launches the executable when needed. **Note:** For SPARC Solaris, the location of this subdirectory is set by the user during installation.

Subdirectory	Description
`db`	Contains gateway database files. During the MVAM installation, if you selected Text File User Database, the MVAM also stores user database files here.
`events`	Stores the event-log file.
`webpages` (NT) `htdocs` (Solaris)	Contains all the HTML files **Note:** For SPARC Solaris, the location of this subdirectory is set by the user during installation.
`lib.sol2`	(Solaris only) Contains shared libraries and other support files.

MVAM configuration and control files

Upon execution, MVAM obtains processing instructions by reading information contained in the following files:

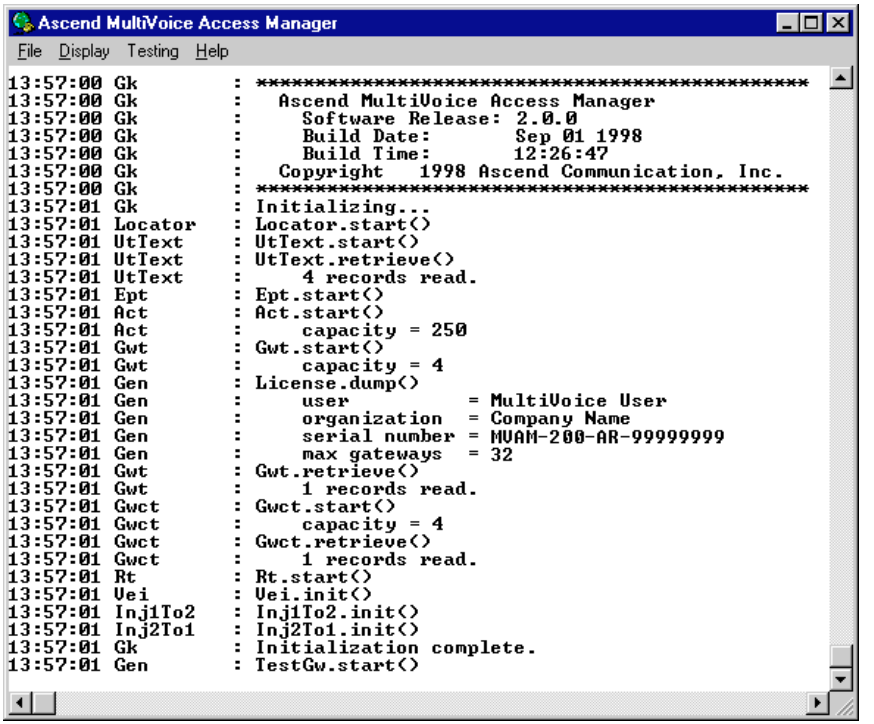
File	Description
`\Winnt\mvam.ini` (NT) `$HOME/.mvam.ini` (Solaris)	Primary configuration file. Contains all values set during installation of the MVAM. If this file is missing, nothing is displayed when MVAM is started. (For details, see Appendix A, “MVAM initialization file.”.)
`\Winnt\mvam.dat` (NT) `$HOME/mvam.dat` (Solaris)	Application data file. If this file is missing or corrupted, the MVAM will not run. It is stored in the MVAM installation directory.
`config.val`	The H.323 stack configuration file. If this file is missing, MVAM dumps core when exited. The file is stored in the MVAM subdirectory `bin`.
`h323.raw`	A binary file, describing the ASN-1 syntax of the H.323 messages. If this file is missing, MVAM returns an error message on start up and dumps core when exited. The file is stored in the MVAM subdirectory `bin`.

Launching MVAM on a Windows NT system

To launch the MVAM on a Windows NT system:

1. Make sure that your Web server is running.
2. In the lower-left section of your screen, click the Windows Start button, then select Programs > MultiVoice Access Manager.

After you launch MVAM, the following window appears:



The display includes two critical items of information:

- The version of the MVAM that you loaded
- Verification that MVAM loaded successfully

After checking the MVAM window, you can minimize it by clicking the left-most of the three boxes in the upper-right corner of the window.

Launching the MVAM on a SPARC Solaris system

The UNIX version of MultiVoice Access Manager is installed as an X-Windows program. It can be launched from the SPARC workstation on which it was installed, or launched remotely from any X-client.

Note: The $DISPLAY variable must be set appropriately before MVAM is started. This variable identifies the networked computer where MVAM displays its standard output. For more information see “Starting the MultiVoice Access Manager remotely” .

To launch MVAM:

1. Make sure that your Web server is running.
2. If `/opt/mvam` is the MVAM installation directory, at the command prompt enter the following command:

   ```
   $ /opt/mvam/bin/mvam.sh &
   ```

   When no value is specified for *$HOME* during installation, the command is invoked using the `--home` option, followed by the name of the working directory used by the MultiVoice Access Manager (i.e /opt/mvam).

   ```
   $ mvam.sh --home /opt/mvam
   ```

   Note: If the MultiVoice Access Manager was not installed in its default location, you must execute the `xhost` command from the command prompt before executing `mvam.sh`

After you launch the MVAM, the following window appears:

```
13:57:00 Gk         : ************************************************
13:57:00 Gk         :   Ascend MultiVoice Access Manager
13:57:00 Gk         :     Software Release: 2.0.0
13:57:00 Gk         :     Build Date:       Sep 01 1998
13:57:00 Gk         :     Build Time:       12:26:47
13:57:00 Gk         :   Copyright   1998 Ascend Communication, Inc.
13:57:00 Gk         : ************************************************
13:57:01 Gk         : Initializing...
13:57:01 Locator    : Locator.start()
13:57:01 UtText     : UtText.start()
13:57:01 UtText     : UtText.retrieve()
13:57:01 UtText     :     4 records read.
13:57:01 Ept        : Ept.start()
13:57:01 Act        : Act.start()
13:57:01 Act        :     capacity = 250
13:57:01 Gwt        : Gwt.start()
13:57:01 Gwt        :     capacity = 4
13:57:01 Gen        : License.dump()
13:57:01 Gen        :     user          = MultiVoice User
13:57:01 Gen        :     organization  = Company Name
13:57:01 Gen        :     serial number = MVAM-200-AR-99999999
13:57:01 Gen        :     max gateways  = 32
13:57:01 Gwt        : Gwt.retrieve()
13:57:01 Gwt        :     1 records read.
13:57:01 Gwct       : Gwct.start()
13:57:01 Gwct       :     capacity = 4
13:57:01 Gwct       : Gwct.retrieve()
13:57:01 Gwct       :     1 records read.
13:57:01 Rt         : Rt.start()
13:57:01 Vei        : Vei.init()
13:57:01 Inj1To2    : Inj1To2.init()
13:57:01 Inj2To1    : Inj2To1.init()
13:57:01 Gk         : Initialization complete.
13:57:01 Gen        : TestGw.start()
```

The window displays two crucial items of information:

- The version of the MVAM that you loaded
- Verification that the MVAM loaded successfully

After checking the MVAM window, minimize it.

Starting the MultiVoice Access Manager remotely

If MVAM is run remotely (from another computer on the network), you must take the following steps before executing `mvam.sh`:

1 On the system with the monitor (not the system running the MultiVoice Access Manager), execute the `xhost` command at the command prompt:

`/usr/openwin/bin/xhost +host`

Substitute the network name of the computer you will use to run the MultiVoice Access Manager for *`host`*. An alternative is:

`/usr/openwin/bin/xhost +`

This command will allow any system to execute X Window applications

2 On the system running the MultiVoice Access Manager, set the UNIX variable *$DISPLAY*, as in the following example:

```
$ DISPLAY=IP_address; export DISPLAY # sh/ksh
% setenv DISPLAY IP_address  # csh
```

Substitute the IP address or network name of the computer where you wish to run the application (e.g., `112.112.10.10`) for *IP address*.

3 On the system running MVAM, try running the X Window terminal emulator to see if remote graphical applications can run at all:

```
/usr/openwin/bin/xterm
```

A terminal window should appear on the system with the monitor. This is standard Unix administration, not specific to MVAM. If you can't complete this step, please consult your Unix system administrator for assistance.

Opening the user interface

With your Web server and MVAM running, you can configure MVAM from either of the two supported Web browsers:

- Netscape Navigator, version 3.01 or later, or Netscape Communicator.
- Microsoft's Internet Explorer, version 3.02 or later.

To administer the MultiVoice Access Manager through the Web-based user interface:

1 Launch your Web browser, and open the following URL:

```
http://localhost/index.htm
```

The start-up page for the MultiVoice Access Manager appears.

2 Bookmark this page for future reference.

Note: If you use a Web browser on the MVAM server to access `localhost`, the browser displays the default index or home page for the Web server. To start the MVAM application, you must specify `localhost/index.htm`

When launching a Web browser on a remote server, entering the IP address or DNS name of the MVAM server displays the default index or home page for the Web server. To start the MVAM application, you must add `index.htm` to the IP address or DNS name.

Resolving an MVAM host name with an IP address (Solaris only)

The simple (unqualified) host name of a Solaris system running the MVAM application must be mapped to an IP address, since MVAM uses the simple host name when initiating various Remote Procedure Calls (RPCs). When an IP address is not found for the simple host name, MVAM RPC processing fails.

For example, if a Solaris system has the host name foo, and its domain name is foo.bar.com, MVAM will look up an IP address for foo, not foo.bar.com. If no IP address is associated with the host name foo, MVAM will fail when it attempts to execute RPC routines with the error message: `Failed to connect to the registry server on foo`.

To prevent this problem, you may use either of these solutions:

- Create an entry for the unqualified host name and its IP address in the `/etc/host` file on the MVAM host system, for example:

```
# Internet host table
#
127.0.0.1       localhost
111.168.19.2    doc loghost
111.168.35.2    dopey
111.20.8.21     foo.bar.com    foo
```

- Create an entry for the MVAM host's domain and its name server in the `/etc/resolv.conf` file on the MVAM host system, for example:

```
domain bar.com
nameserver 111.20.8.1
nameserver 111.20.212.10
```

To test whether a name resolution problem exists, attempt to open a Telnet session, from the MVAM host, using the unqualified host name for that Solaris system. For example:

```
# telnet foo
```

If you see the error message `foo:Unknown host`, edit the `/etc/hosts` or `/etc/resolv.conf` file.

Uninstalling MVAM

Before you uninstall the MVAM, you should back up any gateway, user, or call database files. MVAM should not be running.

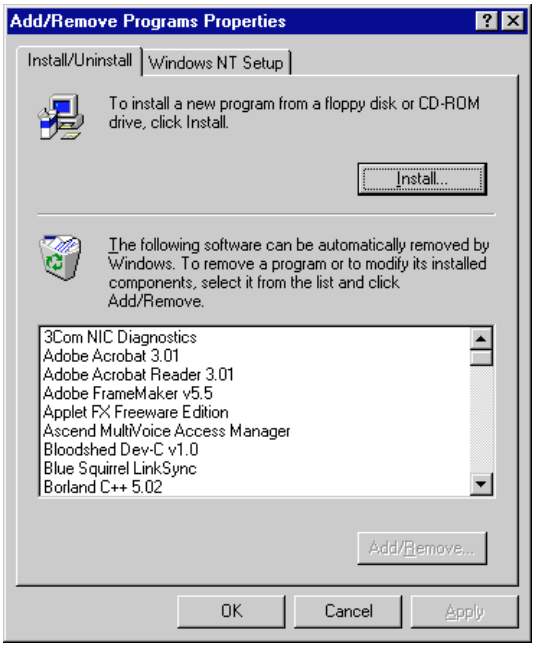
Caution: If you are uninstalling MultiVoice Access Manager in order to upgrade to the latest software release, you should first back up the files in the `db` and `calls` subdirectories, including the `calls/current/calls.txt` file.

Uninstalling MVAM from a Windows NT system

Windows NT provides the Add/Remove Software utility on the Control Panel. To uninstall MVAM, proceed as follows:

1. Make sure that MVAM is not running.
2. In the lower-left section of your screen, click the Windows Start button, then select Settings > Control Panel.
3. Select the Add/Remove Programs icon.

The following window appears.



4 Select the Ascend MultiVoice Access Manager entry.

5 Click Add/Remove to automatically uninstall the MVAM.

Uninstalling MVAM from a Solaris system

To uninstall MVAM from a SPARC workstation or server use the UNIX `pkgrm` command. The process removes only application files and empty directories created during MVAM installation. Any call logs or event logs generated by MVAM are saved in their current directories.

Note: The `pkgrm` command must be executed by `root`.

Proceed as follows:

1 Make sure that MVAM is not running.

2 Change to the root directory (/), then execute the `pkgrm` command:

```
# pkgrm ASNDmvam
```

The following prompt appears:

```
The following package is currently installed:
ASNDmvam Ascend MultiVoice Access Manager
 (sparc) 2.0.0

Do you want to remove this package?
```

Enter **y**, and press Return to continue.

3 The `pkgrm` command inventories the installed application, then prompts for verification to continue:

```
## Removing installed package instance <ASNDmvam>

This package contains scripts which will be executed with
super-user permission during the process of removing this
package.

Do you want to continue with the removal of this package
[y,n,?,q]
```

Enter **y**, and press Return to continue

The `pkgrm` command removes the application and license files from the SPARC.

```
## Verifying package dependencies.
## Processing package information.
## Removing pathnames in class <none>
```

(list of files omitted)

```
## Executing postremove script.
## Updating system information.

Removal of <ASNDmvam> was successful.
```

Example of how MVAM is uninstalled from a Solaris system

The following is an example of how to uninstall MVAM on a Solaris system using the `pkgrm` command:

```
# pkgrm ASNDmvam

The following package is currently installed:
ASNDmvam        Ascend MultiVoice Access Manager
              (sparc) 2.0.0c1
```

```
Do you want to remove this package? y

## Removing installed package instance <ASNDmvam>
This package contains scripts which will be executed with
super-user permission during the process of removing this
package.

Do you want to continue with the removal of this package
[y,n,?,q] y

## Verifying package dependencies.
## Processing package information.
## Executing preremove script.
## Removing pathnames in class <none>
/usr/mvam/mvamuser/.mvam.ini
/usr/mvam/mvamuser/.WindU
/usr/local/apache/htdocs/utnumh.htm
/usr/local/apache/htdocs/utaliash.htm
/usr/local/apache/htdocs/uremh.htm
/usr/local/apache/htdocs/urem.htm
/usr/local/apache/htdocs/uqueryh.htm
/usr/local/apache/htdocs/uquery.htm
/usr/local/apache/htdocs/upinh.htm
/usr/local/apache/htdocs/unameh.htm
/usr/local/apache/htdocs/umodh.htm
/usr/local/apache/htdocs/umod.htm
/usr/local/apache/htdocs/uh.htm
/usr/local/apache/htdocs/udbh.htm
/usr/local/apache/htdocs/uauthh.htm
/usr/local/apache/htdocs/ualiash.htm
/usr/local/apache/htdocs/uadminh.htm
/usr/local/apache/htdocs/uadmin.htm
/usr/local/apache/htdocs/uaddh.htm
/usr/local/apache/htdocs/uadd.htm
/usr/local/apache/htdocs/termh.htm
/usr/local/apache/htdocs/success.gif
/usr/local/apache/htdocs/statush.htm
/usr/local/apache/htdocs/sech.htm
/usr/local/apache/htdocs/sec.htm
/usr/local/apache/htdocs/redball.gif
/usr/local/apache/htdocs/ptnumh.htm
/usr/local/apache/htdocs/phoneih.htm
```

```
/usr/local/apache/htdocs/pdialh.htm
/usr/local/apache/htdocs/logsh.htm
/usr/local/apache/htdocs/logo2.gif
/usr/local/apache/htdocs/logo.gif
/usr/local/apache/htdocs/lnumh.htm
/usr/local/apache/htdocs/index.htm
/usr/local/apache/htdocs/incareah.htm
/usr/local/apache/htdocs/helph.htm
/usr/local/apache/htdocs/hdr_h.gif
/usr/local/apache/htdocs/gwziph.htm
/usr/local/apache/htdocs/gwtnumsh.htm
/usr/local/apache/htdocs/gwtnumh.htm
/usr/local/apache/htdocs/gwstreeth.htm
/usr/local/apache/htdocs/gwstatqueryh.htm
/usr/local/apache/htdocs/gwstatquery.htm
/usr/local/apache/htdocs/gwstateh.htm
/usr/local/apache/htdocs/gwremh.htm
/usr/local/apache/htdocs/gwrem.htm
/usr/local/apache/htdocs/gwqueryh.htm
/usr/local/apache/htdocs/gwquery.htm
/usr/local/apache/htdocs/gwnameh.htm
/usr/local/apache/htdocs/gwmodh.htm
/usr/local/apache/htdocs/gwmod.htm
/usr/local/apache/htdocs/gwloctnumh.htm
/usr/local/apache/htdocs/gwloch.htm
/usr/local/apache/htdocs/gwloc.htm
/usr/local/apache/htdocs/gwh.htm
/usr/local/apache/htdocs/gwdbh.htm
/usr/local/apache/htdocs/gwcs.htm
/usr/local/apache/htdocs/gwcqueryh.htm
/usr/local/apache/htdocs/gwcquery.htm
/usr/local/apache/htdocs/gwcountryh.htm
/usr/local/apache/htdocs/gwcmodh.htm
/usr/local/apache/htdocs/gwcmod.htm
/usr/local/apache/htdocs/gwcmh.htm
/usr/local/apache/htdocs/gwcityh.htm
/usr/local/apache/htdocs/gwcah.htm
/usr/local/apache/htdocs/gwadminh.htm
/usr/local/apache/htdocs/gwadmin.htm
/usr/local/apache/htdocs/gwaddh.htm
```

```
/usr/local/apache/htdocs/gwadd.htm
/usr/local/apache/htdocs/gkih.htm
/usr/local/apache/htdocs/formsh.htm
/usr/local/apache/htdocs/eventh.htm
/usr/local/apache/htdocs/error.gif
/usr/local/apache/htdocs/elegant_double.gif
/usr/local/apache/htdocs/e164h.htm
/usr/local/apache/htdocs/dprefmodh.htm
/usr/local/apache/htdocs/dprefmod.htm
/usr/local/apache/htdocs/dprefh.htm
/usr/local/apache/htdocs/dialih.htm
/usr/local/apache/htdocs/cstatush.htm
/usr/local/apache/htdocs/crth.htm
/usr/local/apache/htdocs/cmptnumh.htm
/usr/local/apache/htdocs/clogh.htm
/usr/local/apache/htdocs/checkb.gif
/usr/local/apache/htdocs/ccodeh.htm
/usr/local/apache/htdocs/caccoh.htm
/usr/local/apache/htdocs/cacco.htm
/usr/local/apache/htdocs/cacch.htm
/usr/local/apache/htdocs/caccfcfh.htm
/usr/local/apache/htdocs/background.jpg
/usr/local/apache/htdocs/alphaih.htm
/usr/local/apache/htdocs/aliastransh.htm
/usr/local/apache/htdocs/adialh.htm
/usr/local/apache/htdocs/acodeh.htm
/usr/local/apache/htdocs/abouth.htm
/usr/local/apache/cgi-bin/mvam_cgi.exe
/opt/mvam/lib.sol2/windu_registryd42
/opt/mvam/lib.sol2/windu_registry
/opt/mvam/lib.sol2/windu_clientd42
/opt/mvam/lib.sol2/windu_client
/opt/mvam/lib.sol2/regedit
/opt/mvam/lib.sol2/libwinsock42.so
/opt/mvam/lib.sol2/libwininet42.so
/opt/mvam/lib.sol2/libuser42.so
/opt/mvam/lib.sol2/libshell42.so
/opt/mvam/lib.sol2/libriched42.so
/opt/mvam/lib.sol2/libprnt42.so
/opt/mvam/lib.sol2/libolest42.so
```

```
/opt/mvam/lib.sol2/libole42.so
/opt/mvam/lib.sol2/libodbc42.so
/opt/mvam/lib.sol2/libmfc42.so
/opt/mvam/lib.sol2/libkernel42.so
/opt/mvam/lib.sol2/libgdi42.so
/opt/mvam/lib.sol2/libcommdlg42.so
/opt/mvam/lib.sol2/libcommctrl42.so
/opt/mvam/lib.sol2
/opt/mvam/db/user.txt
/opt/mvam/db/gwc.txt
/opt/mvam/db/gw.txt
/opt/mvam/bin/textlicapp
/opt/mvam/bin/mvam_cgi
/opt/mvam/bin/mvam.sh
/opt/mvam/bin/mvam
/opt/mvam/bin/h323.raw
/opt/mvam/bin/daemons
/opt/mvam/bin/config.val
/opt/mvam/bin
/opt/mvam/README

## Executing postremove script.
## Updating system information.

Removal of <ASNDmvam> was successful.
```

Configuring the MultiVoice Access Manager

3

Connecting to MVAM

You access MVAM from a Web browser, which can be on the same computer or on any computer that can access the computer running MVAM.

Caution: When you have installed and configured MVAM, be sure to restrict access by means of firewalls, filters, or password protection. Otherwise, once MVAM is installed, anyone can connect to it using a supported Web browser.

Connecting from the computer on which MVAM is running

To connect to MVAM from the computer on which MVAM is running, use an MVAM-supported browser to access one of the following four locations.

- `http://localhost/index.htm`
- `http://name/index.htm`
  where `name` is the network name of the computer on which MVAM is running.
- `http://127.n.n.n/index.htm`
  where `127.n.n.n` can be any IP address that has 127 as the first octet, identifying it as an IP address for `localhost`. The remaining octets can be any value from 0 (zero) to 255.
- `http://n.n.n.n/index.htm`
  where `n.n.n.n` is the network IP address of the computer on which MVAM is running.

If you use a Web browser on the MVAM server to access `localhost`, the browser displays the default index or home page for the Web server. To start the MVAM application, you must specify `localhost/index.htm`.

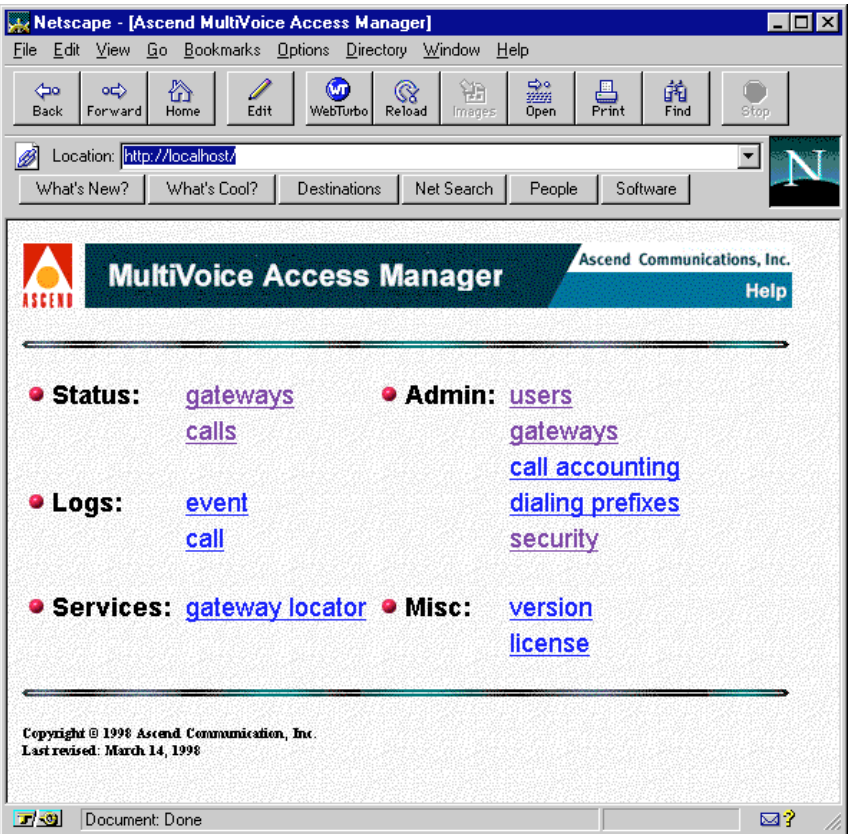
Connecting from another computer

To connect to the MVAM from a different computer, use an MVAM-supported browser to access the MVAM interface. In the browser, enter the IP address of the computer on which MVAM is running. For example:

`http://10.1.1.3/index.htm`

When you launch a Web browser on a remote server, entering the IP address or DNS name of the MVAM server displays the default index or home page for the Web server. To start the MVAM application, you must add `index.htm` to the IP address or DNS name.

When you connect to MVAM, its main screen appears. For example, if you use the Netscape browser, the following screen appears:



The MVAM main screen includes links to all configuration screens, unless you selected the AllBill type database during setup.

About on-line help

On-line help displays information about screens and their fields. When you click a Help button (if present), MVAM displays information about the currently displayed screen. If you click an underlined field name, the MVAM displays complete information about that command.

If you want access to the complete help system, click either:

- The word `Help` on the main title bar of the MVAM main screen
- The underlined text `Help Topics Index` on any on-line help screen

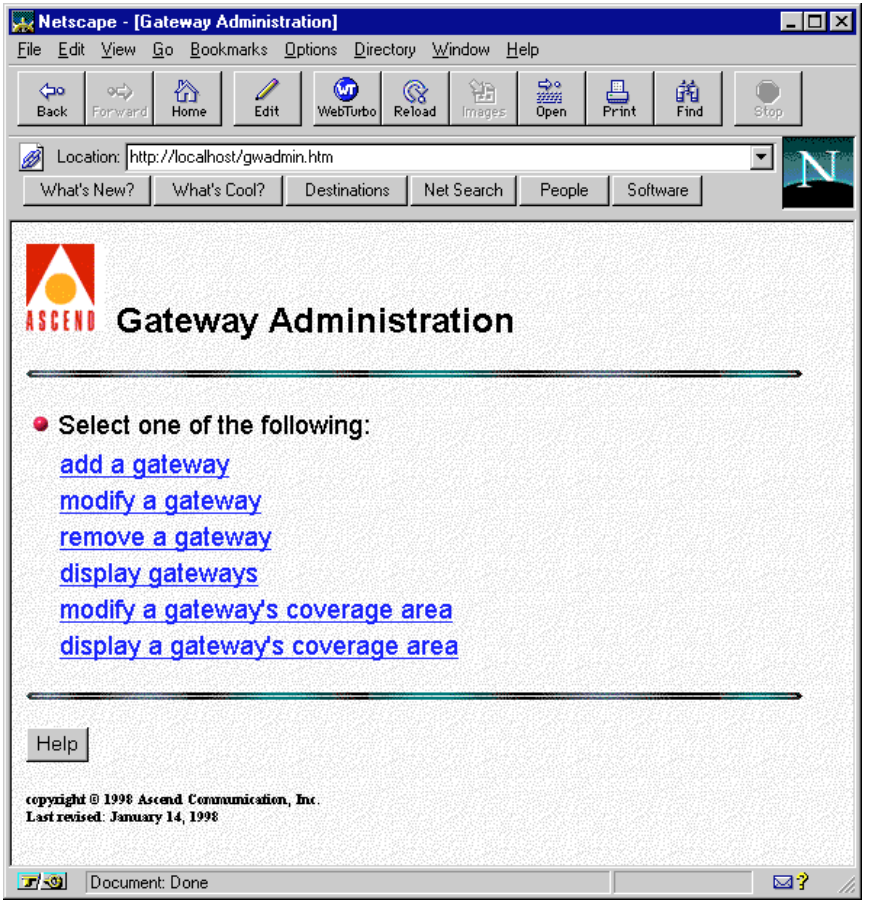
Configuring MultiVoice Gateways

From the MVAM, you can:

- Add Gateways to the MultiVoice network
- Modify Gateway information
- Remove Gateways from the MultiVoice network
- Display Gateway information

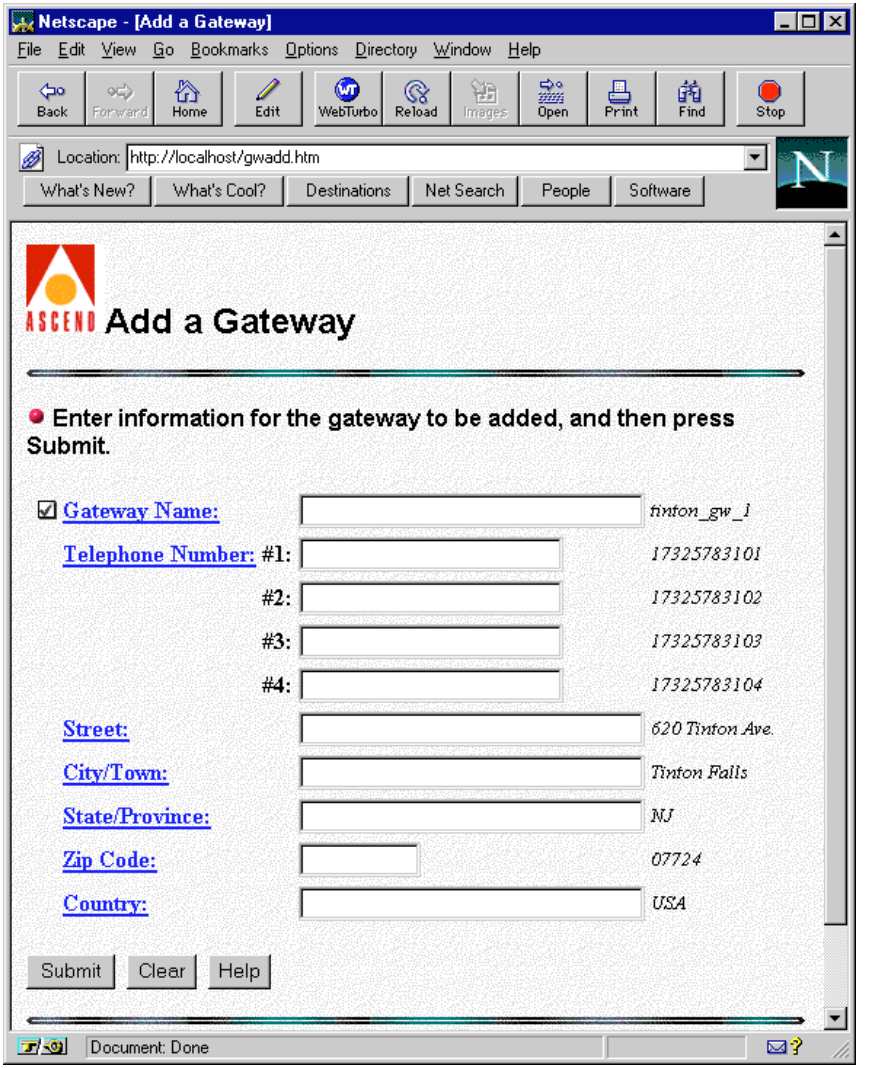
Note: When you add, modify, or delete Gateways in MVAM, the Gateway Name denotes the physical MultiVoice Gateways in your network. MVAM cannot register a MultiVoice Gateway that is using a DNS alias.

In the Administration section of the MVAM main screen, click `gateways`. The Gateway Administration screen appears:



Adding Gateway records

To add a Gateway to the MultiVoice network, click `add a gateway` on the Gateway Administration screen. The Add a Gateway screen appears:



Note: You can get on-line help for the screen by clicking the Help button, or for specific fields by clicking on any underlined field name.

The screen displays sample entry data to the right of each text field. A check box to the left of any field name indicates that you must enter a value for the field before you click the Submit button.

Understanding the Gateway fields

The Gateway fields include values for the name, telephone number, and address of a MultiVoice Gateway. For complete information about each field, see the MVAM on-line help.

Gateway Name

As indicated by the animated check box to the left of the field name, Gateway Name is the only required field for which you must enter a value to add a Gateway to the MultiVoice network.

Optional telephone and address information

You can enter telephone numbers that users dial to reach the Gateway, as well as the address at which the Gateway is physically located.

The carrier assigns phone numbers to the lines connecting to the MultiVoice Gateway, so you are not required to enter a phone number in a Gateway record. However, you might find the information helpful should you need to quickly look up a MultiVoice Gateway phone number for a user.

Saving the settings

The MVAM settings you configure do not take effect until you save them to the MVAM database files. To save the settings, click the Submit button in the lower-left section of the Add a Gateway screen.

If the MVAM displays the message `Couldn't add the gateway. The database is full`, you must either delete an unused Gateway before you

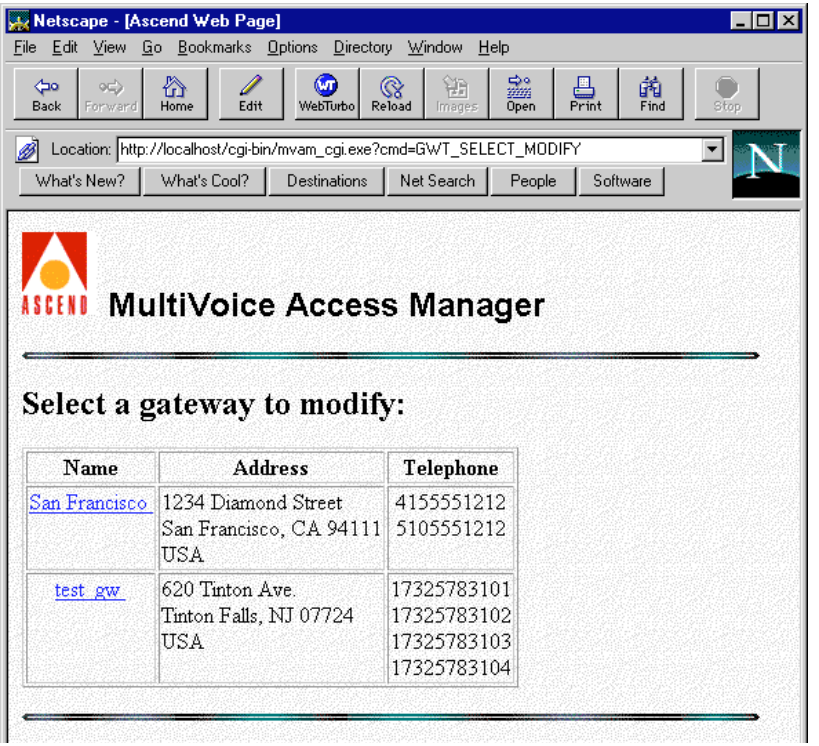
can add a Gateway, or upgrade the user license of your MVAM. For details about upgrading the MVAM license, contact an authorized Ascend representative.

Note: After adding MultiVoice Gateway information to MVAM, make sure you have installed and configured the MultiVoice Gateways on the MultiVoice network, as described in the *MultiVoice Gateway for the MAX—User Guide*. For the MultiVoice Gateway to successfully register with the MVAM, the name of the physical MultiVoice Gateway must match the Gateway Name field in the MVAM Gateway record.

Modifying Gateway information

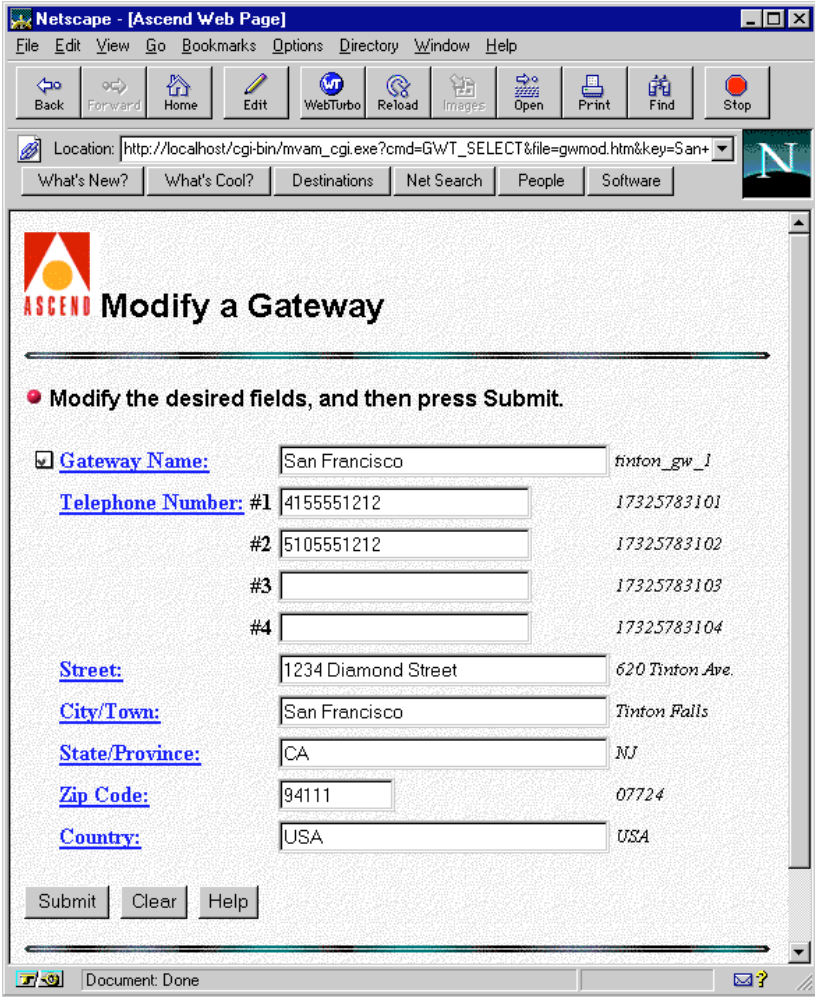
To modify a Gateway record:

1 From the Gateway Administration screen, click `modify a gateway`. A list of all Gateways appears. For example:



2 Click the underlined Name of a displayed Gateway. (For a longer list, the screen has a scroll bar at its right edge.)

MVAM displays the Gateway record. For example:



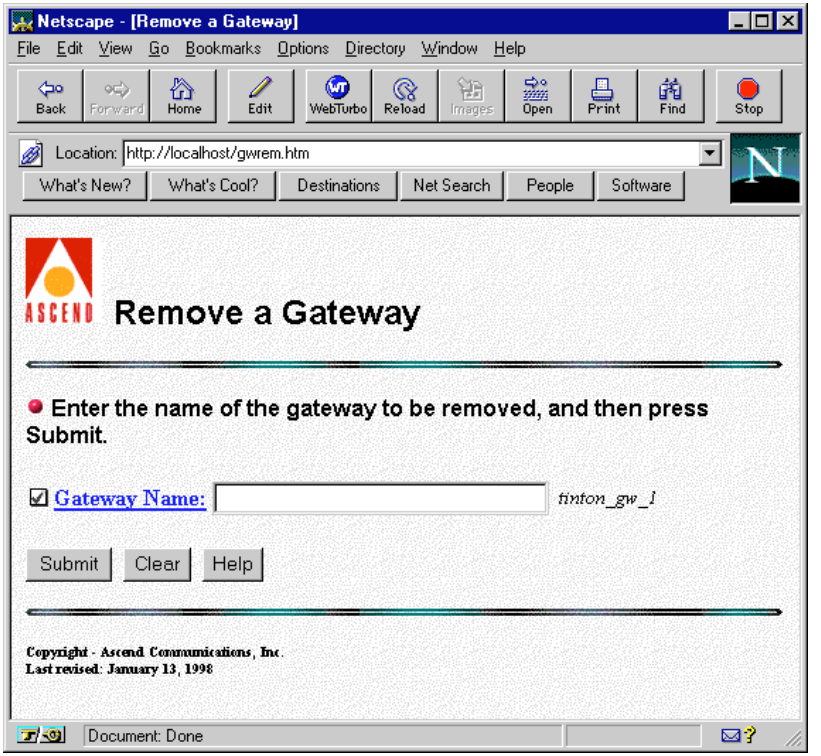
3 Modify any field by typing in the new information.

4 To save the settings, click the Submit button in the lower-left corner of the screen.

Removing a gateway

To remove a gateway record:

1 From the Gateway Administration screen, click `remove a gateway`. The Remove a Gateway screen appears:

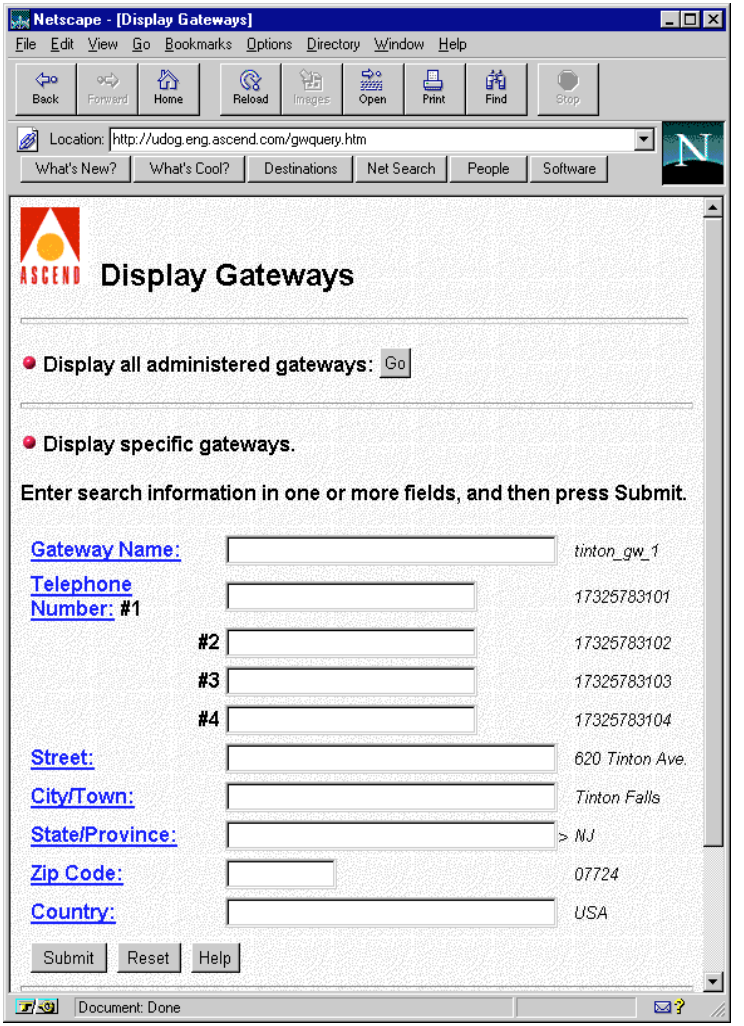


2 In the Gateway Name field, enter the name of the Gateway to remove.

3 Click the Submit button in the lower-left section of the screen.

Displaying gateway information

You can direct MVAM to display information from a specific record or from all records. On the Gateway Administration screen, click `display gateways` to access the Display Gateways screen.



To display a list of all currently configured user records, click the Go button.

To display a specific record or set of records, enter search information in one or more of the fields in the `Display specific gateways` area, and click the Submit button.

Coverage areas

You must configure a coverage area for each MultiVoice Gateway. When callers dial into a local MultiVoice Gateway, MVAM determines which MultiVoice Gateway supports the destination phone number by comparing the caller's dialed number to the coverage area for each MultiVoice Gateway.

A coverage area consists of up to 2,000 Inclusion Areas, each of which are from one to 24 digits in length. Each Inclusion Area represents a complete or partial telephone number, which may be routed through a MultiVoice Gateway.

The more digits you specify, the fewer the phone numbers that qualify for an Inclusion Area. For example, if you specify an Inclusion Area of 1732555, the phone number 1-732-555-1212 is a member of the Inclusion Area. If you specify an Inclusion Area of 1732, *all* phone numbers in the 732 area code of the United States are members of the Inclusion Area. If you specify an Inclusion Area of 1, all calls to number in North America are members of the inclusion area.

If more than one Inclusion Area supports a specific phone number, MVAM matches the phone number to the most specific Inclusion Area.

Overlapping coverage areas

Overlapping coverage areas are created by assigning the same, or similar, Inclusion Areas to two or more MultiVoice Gateways administered by the same Gatekeeper.

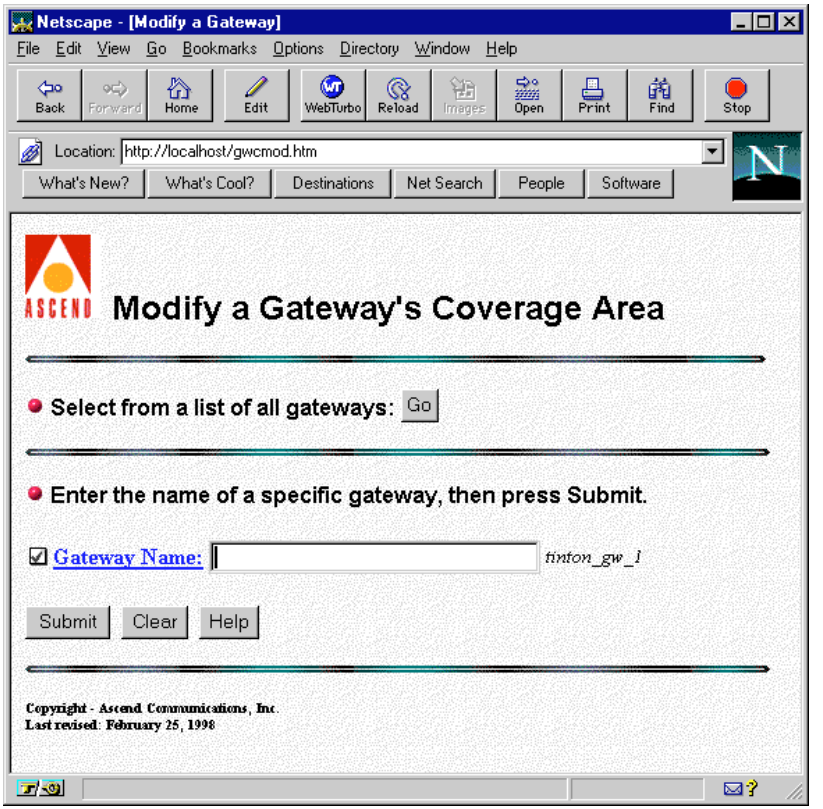
To configure and display coverage areas, use the Gateway Administration screen.

Configuring a coverage area

To add, modify, or delete Inclusion Areas for a Gateway:

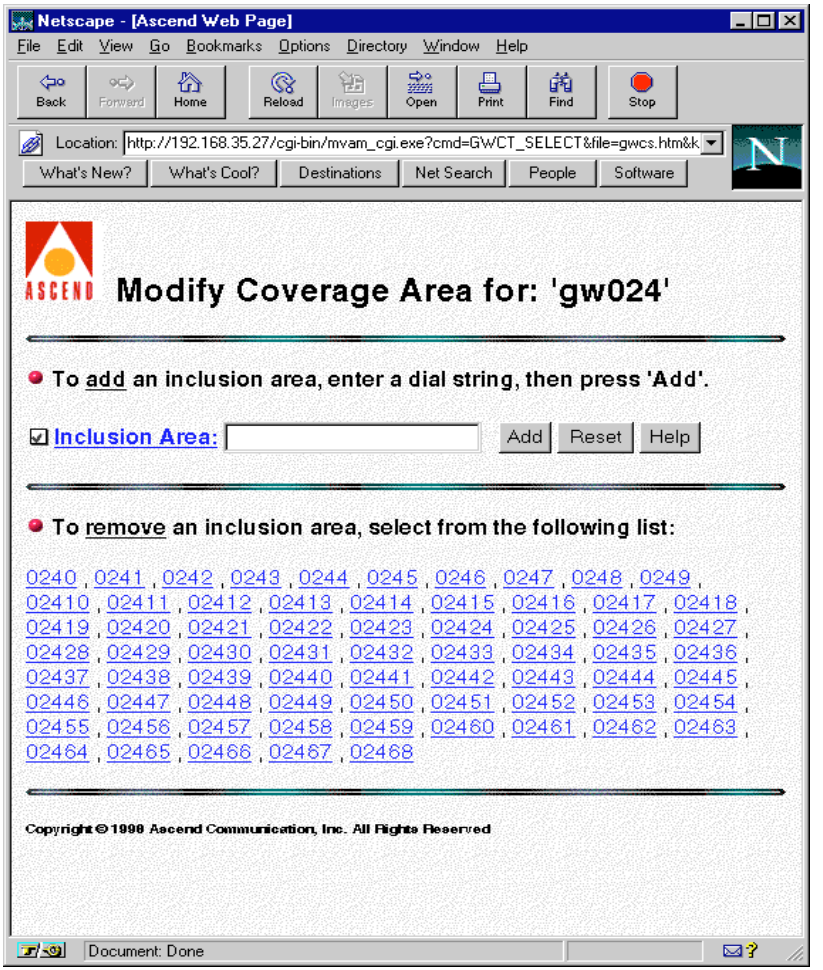
1 From the Gateway Administration screen, click `modify a gateway's coverage area`.

The Modify a Gateway's Coverage Area screen appears:



2 Either enter the Gateway's name in the Gateway Name field and click the Submit button, or click the Go button and select the name from the list of all Gateways.

The screen changes to display the Gateway's coverage area. For example:

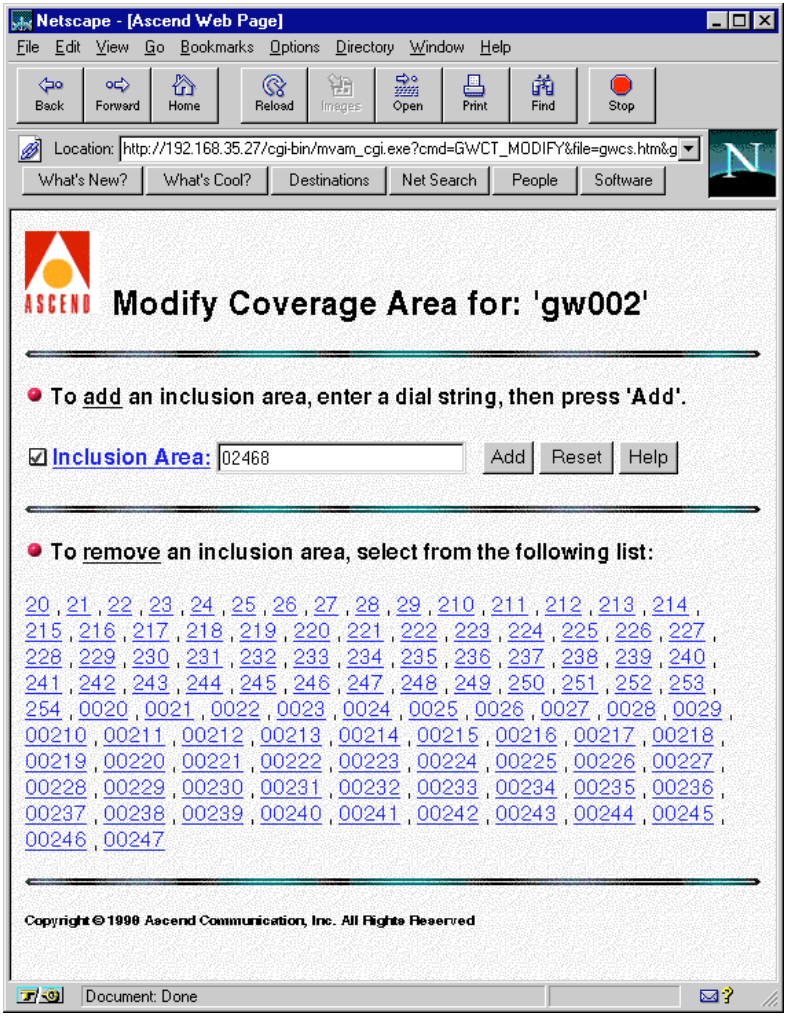


From this screen, you may add or delete Inclusion Areas for the selected Gateway.

Adding an Inclusion Area to a Gateway

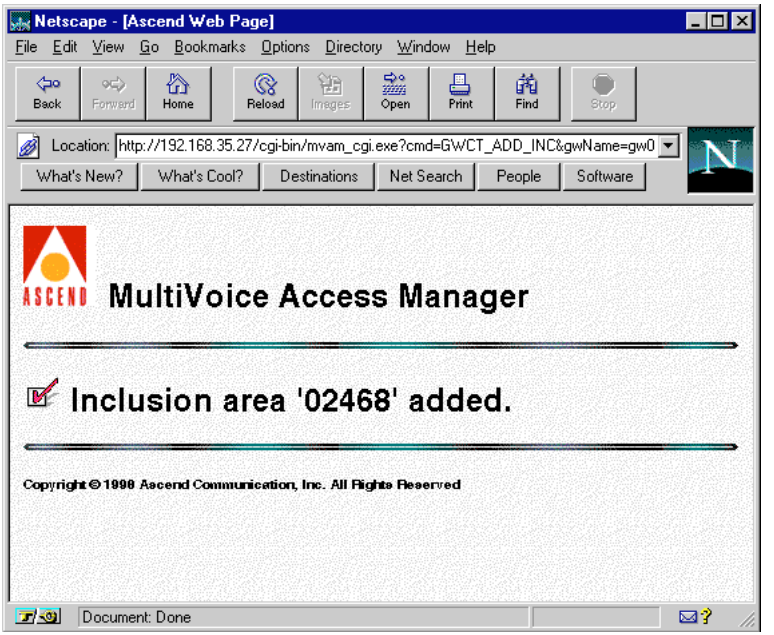
To add an Inclusion Area to a Gateway's coverage area:

1 Enter a full or partial telephone number in the Inclusion Area edit field:



2 To the right of the edit field, click the Add button.

The MVAM confirms the change to this Gateway's coverage area:



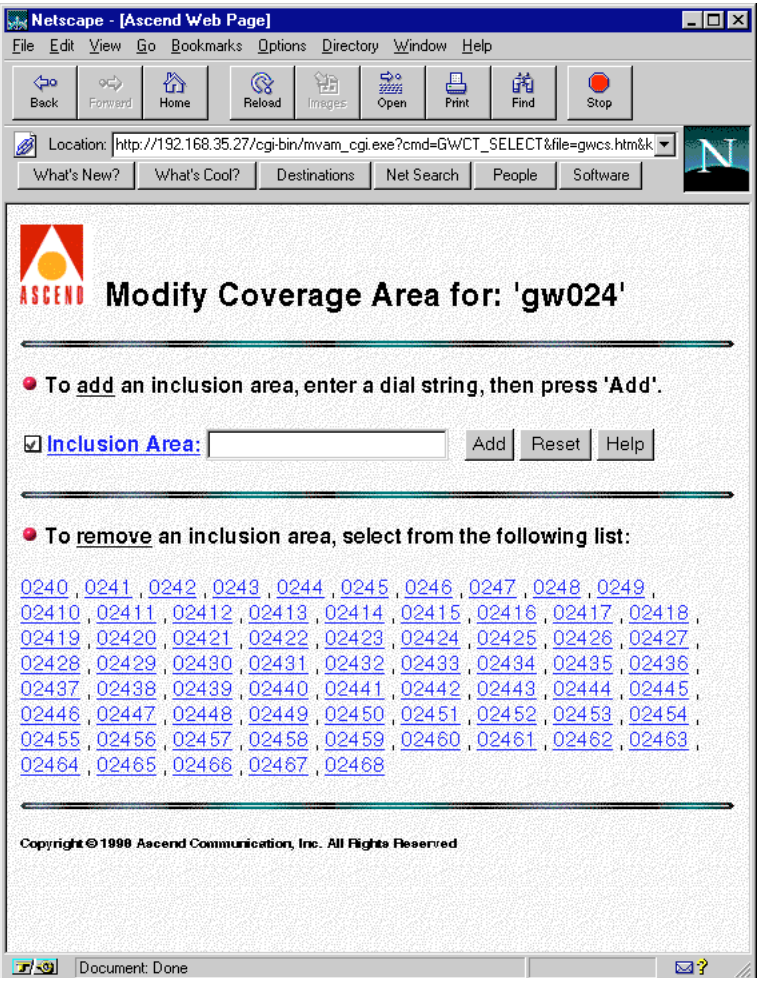
Click on your broswer's Back button to display the list of coverage areas for the selected Gateway. Changes to a Gateway's coverage area are not displayed until this Gateway is again selected from the Modify a Gateway's Coverage Area screen.

Note: When you modify a coverage area for a Gateway, by either adding or removing Inclusion Areas, clicking the browser's Back button should display an updated list of Inclusion Areas. However, for some older browsers (Release 3 and some earlier Release 4 browsers) you must click the Refresh button to correctly display the updated list.

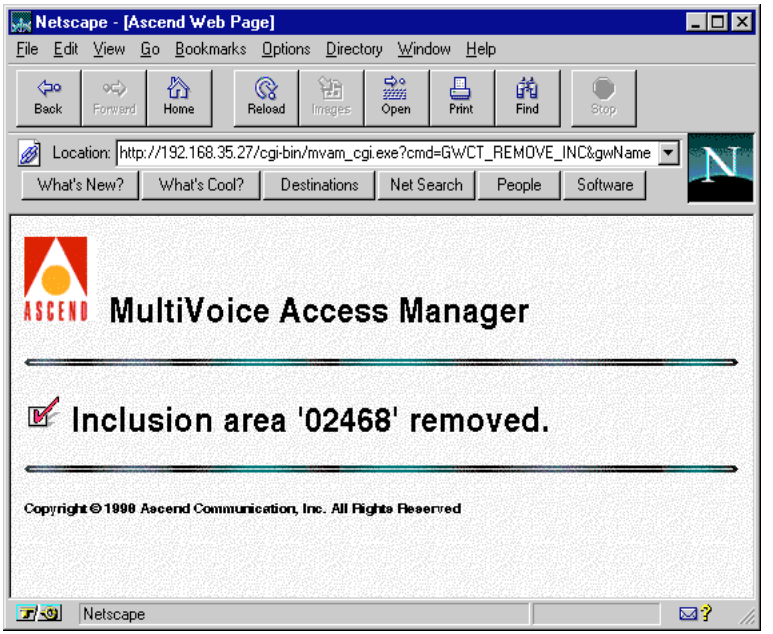
Deleting an Inclusion Area from a Gateway

To delete an Inclusion Area from a Gateway's coverage area:

1 Click on the Inclusion Area from the list displayed on the bottom half of this screen:



The MVAM removes the selected Inclusion Area, then confirms the change to this Gateway's coverage area:



Click on your broswer's Back button to display the list of coverage areas for the selected Gateway. Changes to a Gateway's coverage area are not displayed until this Gateway is again selected from the Modify a Gateway's Coverage Area screen.

Note: When you modify a coverage area for a Gateway, by either adding or removing Inclusion Areas, clicking the browser's Back button should display an updated list of Inclusion Areas. However, for some older browsers (Release 3 and some earlier Release 4 browsers) you must click the Refresh button to correctly display the updated list.

Displaying coverage areas

From the Gateway Administration screen, you can direct the MVAM to display the Inclusion Areas for a specific MultiVoice Gateway or to list all configured Gateways and coverage areas.

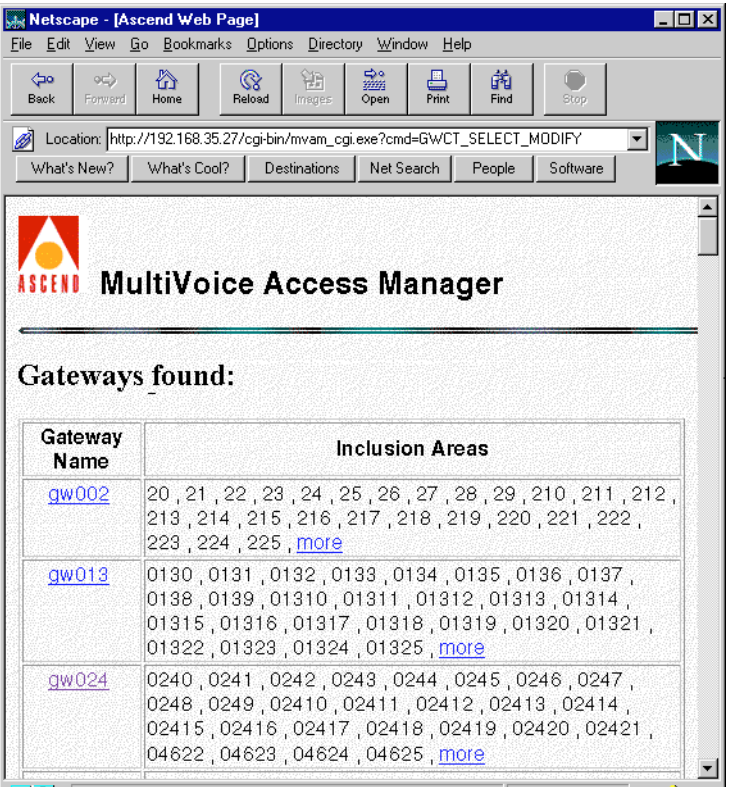
To display the coverage areas for a list of Gateways:

1. From the Gateway Administration screen, click `display a gateway's coverage area`.

   The Display a Gateway's Coverage Area screen appears.

2. Either enter the Gateway's name in the Gateway Name field and click the Submit button, or click the Go button to display all gateways.

   The screen changes to display the coverage areas. For example:



When modifying or displaying coverage areas, the application may display an abbreviated list of Inclusion Areas for each for each Gateway. Click on `more` to display the remaining Inclusion Areas for each Gateway.

You can quickly locate the local MultiVoice Gateway for any caller by using the MVAM Gateway Locator, as described in "Locating MultiVoice Gateways for callers" on page 4-11.

coverage area size

The maximum number of inclusion areas which may be assigned to a Gateway coverage area is controlled by the `inclusionListCapacity` parameter in the MVAM initialization file. Valid values for this variable range between one and 2,000. By default the size of a Gateway coverage area is limited to 2,000 Inclusion Areas.

This value is changed by editing the initialization file, `mvam.ini` on Windows NT systems, or `.mvam.ini` on SPARC Solaris systems. Changes to the `inclusionListCapacity` parameter are applied by stopping and restarting MVAM.

coverage area display

The maximum number of Inclusion Areas displayed for a Gateway coverage area, on lists of all Gateways, is controlled by the `inclusionListDisplayCapacity` parameter in the MVAM initialization file. Valid values for this variable range between one and 2,000. By default the size of a Gateway coverage area is limited to 26 Inclusion Areas.

This value is changed by editing the initialization file, `mvam.ini` on Windows NT systems, or `.mvam.ini` on SPARC Solaris systems. Changes to the `inclusionListDisplayCapacity` variable are applied by stopping and restarting MVAM. (For details, see Appendix A, "MVAM initialization file.".)

Configuring telephone aliases and dialing prefixes

To reduce the number of digits that users must dial, you can create telephone aliases. A caller can reach another user by dialing either the full phone number or the telephone alias.

To allow MVAM to differentiate between a full phone number and a telephone alias, you must configure a dialing prefix consisting of two characters that callers must prepend to the dialed number.

When the MultiVoice Gateway receives a call with a dialed telephone alias, it searches the user database for a user record that includes the alias. MVAM converts the dialed telephone alias to the full telephone number specified in the user record. The MVAM searches for a coverage area on the basis of the full telephone number.

If a matching user record has no full telephone number, or if there is a full telephone number but no supporting coverage area, the call disconnects.

The default dialing prefix for the telephone alias is `*2`, but you can set it to an asterisk (*) followed by any number from 1 to 9.

You can also specify a dialing prefix for the full telephone number. When MVAM receives a call prepended with the dialing prefix for a full telephone number, it strips the dialing prefix from the number and searches for a coverage area on the basis of the dialed telephone number. MVAM does not search the user database unless a caller dials a telephone alias (or MVAM requires PIN or ANI authentication).

Example of dialing prefix and telephone alias

Bob has a phone number of 1-415-555-1212 and a telephone alias of 1212. The dialing prefix for telephone aliases is `*2`. To reach Bob across the MultiVoice network, Mary dials her local MultiVoice Gateway, then dials one of the following numbers:

- 14155551212—Bob's full phone number
- *21212—The dialing prefix, followed by Bob's telephone alias

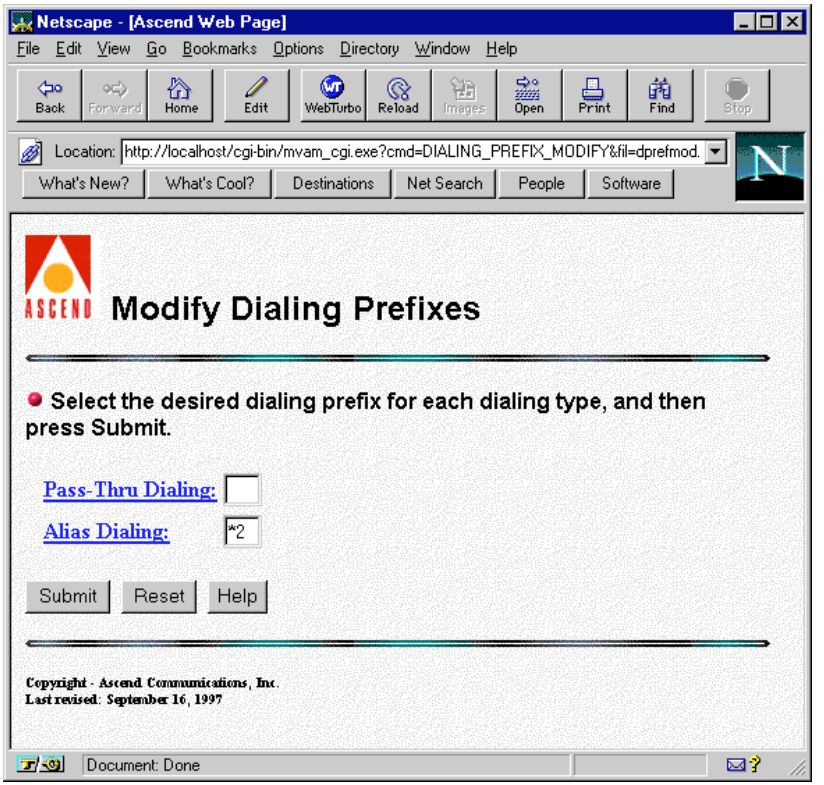
The dialing prefix informs MVAM that a telephone alias follows `*2`. MVAM then uses the alias of 1212 to search for the user in the user database, finds Bob's record, and dials 14155551212.

Configuring dialing prefixes

To configure a dialing prefix:

1. From the main MultiVoice Access Manager screen, click `dialing prefixes`.

   The Modifying Dialing Prefixes screen appears. For example:



2. Set Pass-Thru Dialing to the dialing prefix that callers use to indicate to MVAM that it should dial the entered phone number as-is (after removing the dialing prefix).

3 Set Alias Dialing to the dialing prefix that callers use to instruct MVAM to search its user database for the full-number equivalent of the telephone alias.

4 In the lower-left section of the screen, click the Submit button.

In the Modify Dialing Prefixes screen shown in the example, MVAM assumes that any received number is a full phone number unless it is prepended by a `*2`. You can configure either Pass-Thru Dialing *or* Alias Dialing with no dialing prefix. Because dialing prefixes must be unique, you cannot configure both fields with blank values.

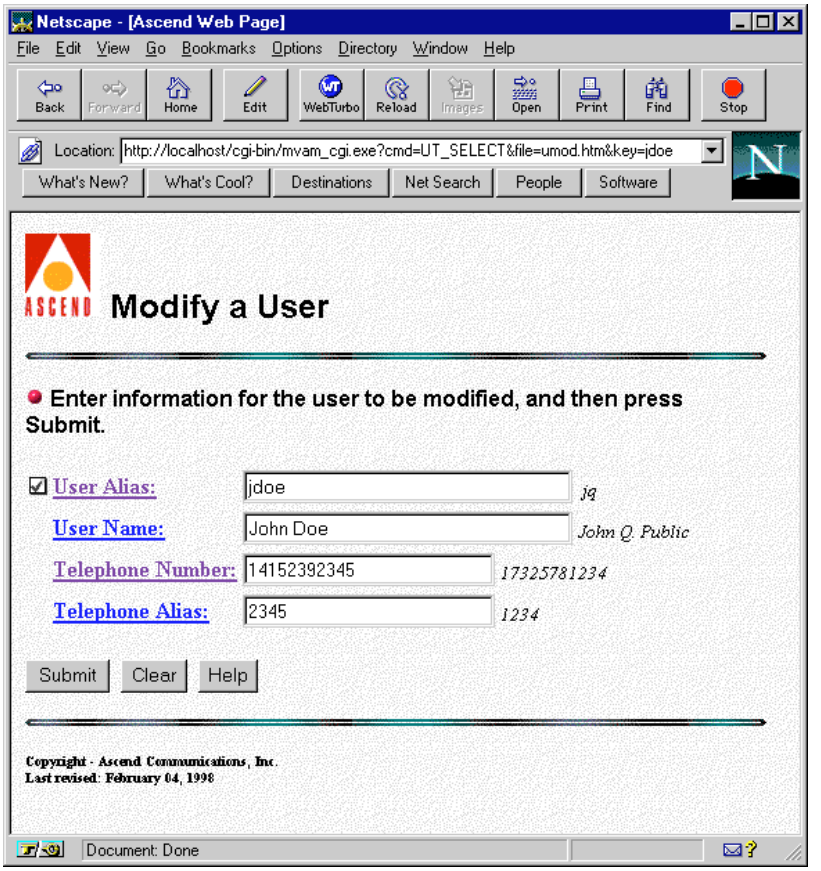
Configuring a user's telephone alias

To configure a telephone alias for a user:

1 From the main MultiVoice Access Manager screen, click `users`.

2 Add a new user by clicking `add user`, or edit a currently configured user by clicking `modify a user`.

3 Enter a full phone number and a telephone alias. For example:



4 In the lower-left section of the screen, click the Submit button.

Note: If you are planning to use ANI authentication, the User Alias field must contain the Calling Line ID (CLID) of the user's telephone number. The CLID is either the 10-digit phone number, for North American telephone numbers, or the full localized telephone number for locations outside of North America.

Configuring security

MultiVoice Access Manager provides two methods for authenticating users when they place calls:

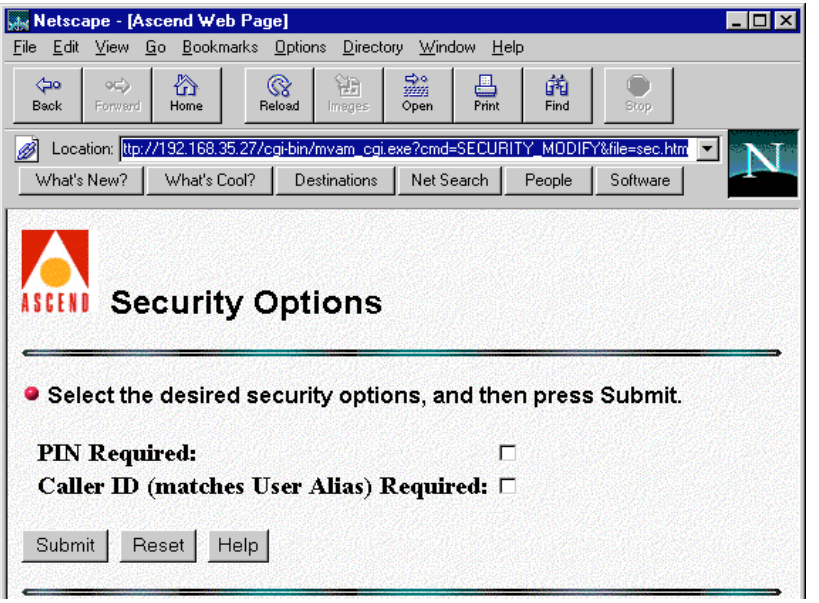
- Personal Identification Number (PIN) entry
- Automatic Number Identification (ANI) authentication

You may configure ANI authentication, PIN authentication, or both.

Configuring call authentication

To require either PIN or ANI, proceed as follows:

1 From the main MultiVoice Access Manager screen, click `security`.
The Security Options screen appears:



2 Select either the PIN Required check box or the Caller ID Required check box, or both.

3 In the lower-left section of the Security Options screen, click the Submit button.

Note: Neither PIN nor ANI authentication will work for calls originating from PCs.

If you do not require authentication

If you do not configure authentication, MultiVoice Access Manager 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 Gatekeeper running MVAM and passes the destination phone number to it.

5 MultiVoice Access Manager selects the IP address of the destination MultiVoice Gateway, selected 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.

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 whether it approved the call.

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

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 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 second, 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 within several seconds, the local MultiVoice Gateway sends a *tick-tock* sound to the caller to indicate 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.

If 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 MVAM to determine whether it approved 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.

MVAM creates the PINs automatically when you create the user records.

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.

If 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 for 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 MVAM to determine whether it approved the call.

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

ANI authentication uses the Automatic Number Identifier associated with the calling telephone number to verify the caller as a valid user. The MultiVoice Gateway collects the ANI and forwards it, in the Admission Request (ARQ) message, along with the destination phone number, to MVAM. If the ANI matches the information in the user database, MVAM continues with call setup.

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.

The MultiVoice Gateway can detect ANI for three network signal types:

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

In order to detect Caller ID over each of these supported trunks, the MultiVoice Gateways must have the following line parameters set as shown:

T1 inband:

```
Net/T1->line config->factory
    Sig Mode=In-Band
    Rob Ctl=wink-inc-200 or wink-inc-400
    Collect DNIS/ANI = yes
```

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

E1 R2:

```
Net/E1->line config->factory
    Sig Mode=R2
```

PRI:

```
Net/T1->line config->factory
    Sig Mode=ISDN
```

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.

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

Configuring MultiVoice users

This section describes functions you can perform if you selected Text File User Database or ODBC User Database as your setup type during MVAM installation. If you selected AllBill Compatible, configure user records as described in the third-party ODBC or AllBill documentation.

From the MVAM main screen, select the link `users` to display the User Administration screen. It provides options for:

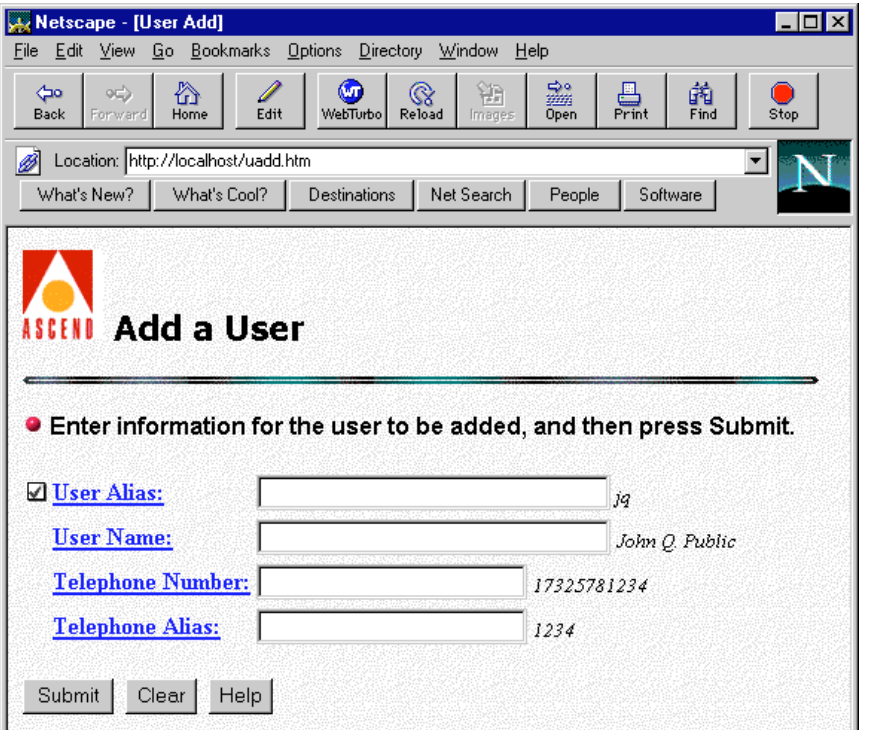
- Adding user records
- Modifying user information
- Removing user records
- Displaying user information

ODBC User Database administration is currently supported only on Windows NT systems.

Note: If your selected AllBill Compatible or ODBC User Database, you will need to install the appropriate Microsoft ODBC drivers for the program you will use to administer the user database. Current ODBC drivers are available from the Microsoft Web site.

Adding user records

To add user records, on the User Administration screen, click `add a user`. The Add a User screen appears. For example:



The screen displays sample entry data to the right of each text field. A check box to the left of any field name indicates that you must enter a value for the field before you click the Submit button.

Understanding the Add a User fields

This section provides background information about the Add a User fields. For complete information about each field, see the MVAM on-line help. You can get on-line help for the screen by clicking the Help button, or for specific fields by clicking on any underlined field name.

User alias and name

As indicated by the animated check box to the left of the field name, User Alias is the only required field for which you must enter a value to add a user. Typically, you would enter the user's email name or employee identification number. For informational purposes, optionally enter the user's full name in the User Name field.

Note: If you plan to use ANI authentication, the User Alias field must contain the CLID for the user's telephone number. The CLID is either the 10-digit phone number, for North American telephone numbers, or the full localized telephone number for locations outside the North American continent

Telephone number and alias

If applicable, enter the telephone number that the *destination* MultiVoice Gateway dials to reach the user in the Telephone Number field. If the user has a company-internal extension, enter the extension in the Telephone Alias field. Enter only numeric digits in the Telephone Number and Telephone Alias fields.

Personal Identification Number (PIN)

MVAM automatically creates a Personal Identification Number (PIN) when you add a user. If you do not require PIN authentication, when MVAM places calls, it does not prompt users for their PIN numbers, even if they have been assigned PIN numbers.

Caution: MVAM displays the PINs of all users. Make sure that you restrict access to MVAM by means of firewalls, filters, or password protection. Once MVAM is installed, anyone with a supported Web browser can connect to it. When PIN information becomes compromised, you may assign new user PINs through the Modify user screen. This will render the compromised information obsolete.

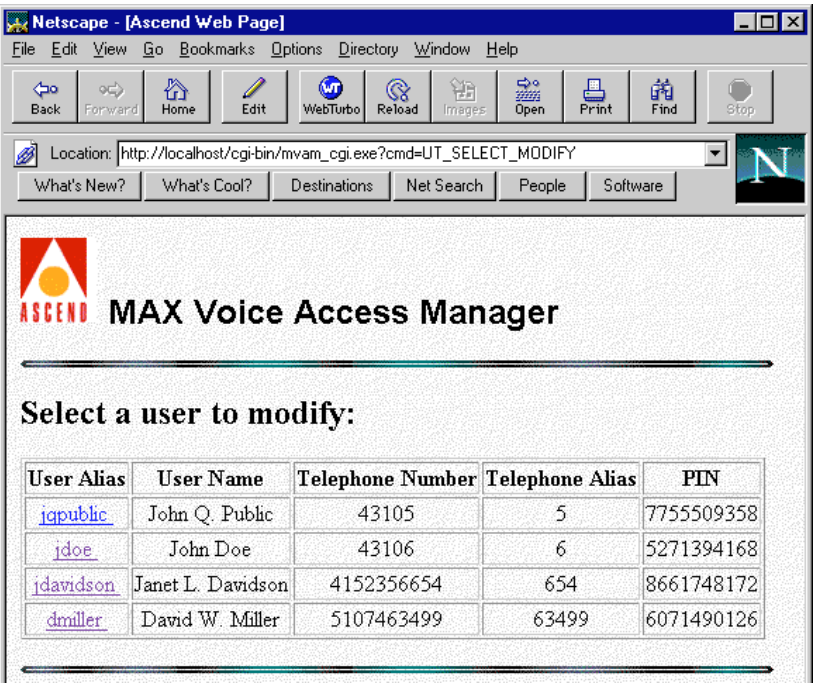
Saving the settings

The MVAM settings you configure do not take effect until you save them to the MVAM database files. To save the settings, click the Submit button in the lower-left section of the Add a User screen.

Modifying user information

To modify a user record:

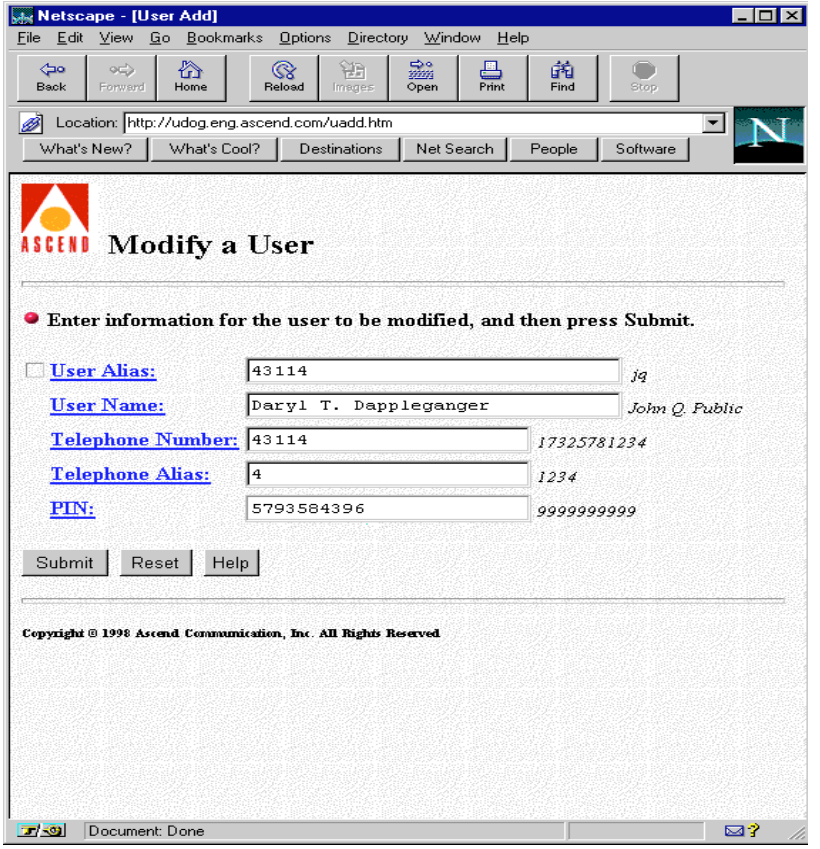
1 From the User Administration screen, click `modify a user`. A list of all users appears. For example:



(An actual list would probably be much longer, and the screen would include a scroll bar on the right side of the screen.)

2 Click the underlined User Alias for the user whose record you wish to modify.

MVAM displays the user's record. For example:



3 Modify any of the fields by typing in new information.

4 To save the settings, click the Submit button in the lower-left section of the Modify a User screen.

Modifying user PINs

In Release 2.0.0 generated PINs may be modified through the Modify user screen.

To modify a user PIN, highlight the entry in the `PIN` edit field. Type in the new PIN for this user, then click the Submit button in the lower-left section of the page.

The Modified user page appears, displaying the updated user record.

The following constraints apply to modification of user PINs:

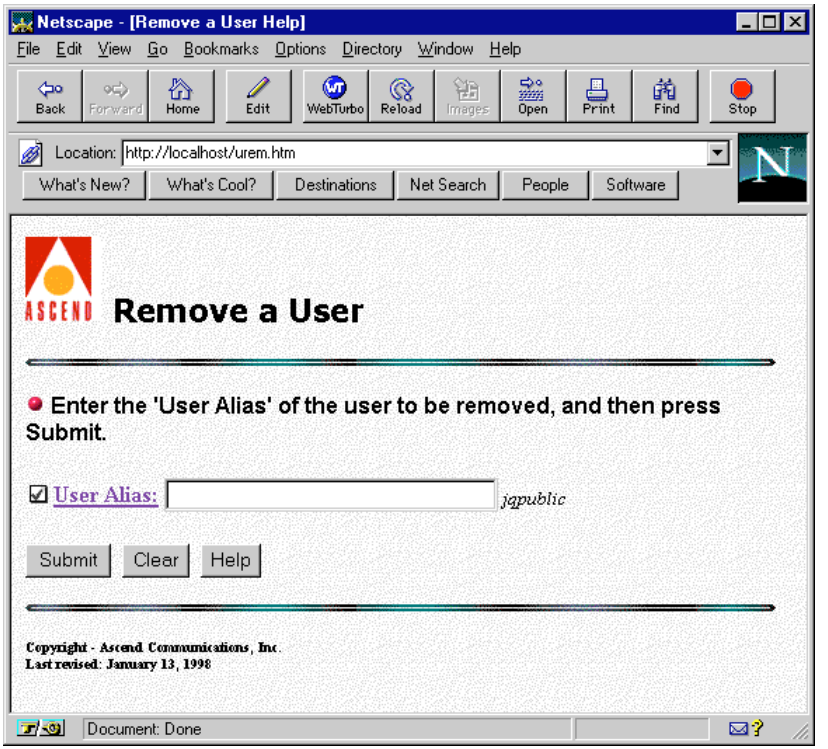
- A PIN may only contain digits.
- The PIN length cannot be greater than 24 digits.

The new PIN must be unique relative to all users in the database.

Removing user records

To remove a user record:

1 From the User Administration screen, click `remove a user`. The Remove a User screen appears:



2 In the User Alias field, enter the alias of the user whose record is to be removed.

3 Click the Submit button in the lower-left section of the screen.

Displaying user information

You can direct MVAM to display information from specific records or from all records. On the User Administration screen, click `display users` to access the Display Users screen.

To display a list of all currently configured user records, click the Go button on the Display Users screen.

To direct MVAM to display specific user records, enter search information in one or more of the fields on the Display Users screen, and click the Submit button.

Configuring PC-to-phone operations

Configuring MVAM to route calls from PCs over the MultiVoice Network, requires the following:

- Both PIN and ANI authentication must be turned off.
- Both the `allowUnknownEndpointRegistrations` and `allowTerminals` parameters in the MVAM initialization file must be enabled. This lets MVAM accepts calls from any PC on the network. MVAM does not have to know about the PC in order to accept a call request.
- The `agedRegistration` parameter in the MVAM initialization file must be disabled. This eliminates the need to have the PC perform keep-alive registration with MVAM. Once MVAM acknowledges the call request, the PC remains registered.
- The `useArqToStart` parameter in the MVAM initialization file must be enabled. This directs MVAM to record the start of the PC call from the time the call request is acknowledged, when MVAM sends an Admission Confirmed (AFC) message.
- The `forceDialStringInAcfNonStd` parameter in the MVAM initialization file must be disabled. By default, MVAM includes the destination telephone number with the nonstandard data in the Admission Confirmed (AFC) message sent to the MultiVoice Gateway that connects the call.

Authentication is enabled/disabled through the Security Options screen. The other parameters are changed by editing the initialization file, `mvam.ini` on

Windows NT systems, or `.mvam.ini` on SPARC Solaris systems. Changes to these parameters are applied by stopping and restarting MVAM. (For details, see Appendix A, “MVAM initialization file.”.)

MultiVoice Gateway Administration 4

Monitoring the status of configured MultiVoice Gateways

When you add MultiVoice Gateways, as described in "Configuring MultiVoice Gateways" on page 3-4, they are unregistered. To be available for voice calls, MultiVoice Gateways must register themselves with the Gatekeeper running MVAM. MVAM maintains a list of all MultiVoice Gateways, and a separate list of those that are registered. Active MultiVoice Gateways keep in constant contact with the MVAM by sending registration requests every two minutes. To change this interval, edit the Ethernet > Mod Config > VOIP Options > Keepalive Timer parameter on the MultiVoice Gateways, a TAOS Release 7.0.0 feature, specifying the time, in seconds, to wait between registration requests.

To direct a MultiVoice Gateway to begin sending registration requests, you must configure it to establish an administrative session with MVAM. Set the Ethernet > Mod Config > VOIP Options > GK IP Adrs parameter to the IP address of the

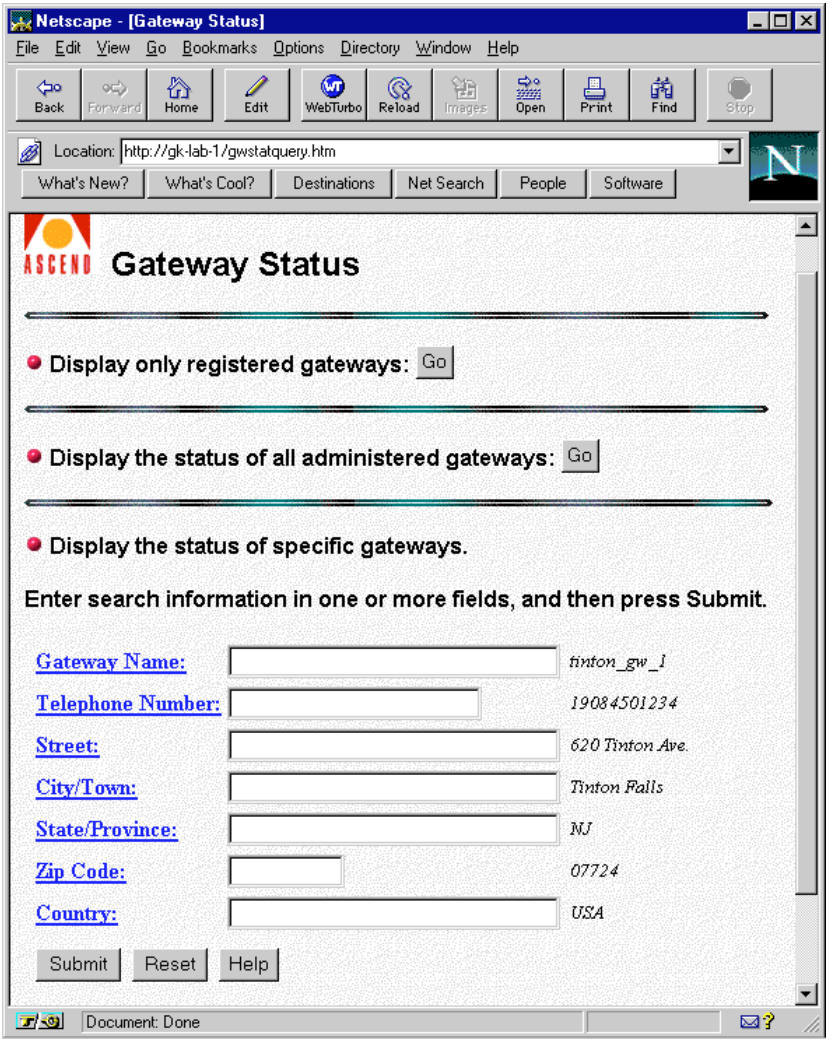
Gatekeeper running MVAM. Make sure that System > Sys Config > Name on the MultiVoice Gateway matches the value you specify in the Gateway Name field in MVAM. Then restart the MultiVoice Gateway.

If the MultiVoice Gateway supports use of a secondary Gatekeeper, a TAOS Release 7.0.0 feature, set the Ethernet > Mod Config > VOIP Options > 2ndGK IP parameter to the IP address of the secondary MVAM.

When the MultiVoice Gateway boots, it sends a registration request to the MVAM, and sends additional registration requests every two minutes. The continual requests ensure that the MultiVoice Gateway remains registered even if you restart MVAM.

Note: By default, a MultiVoice Gateway cannot register itself unless you have added it to the MVAM Gateway database, as described in “Adding Gateway records” on page 3-6. You can enable unknown MultiVoice Gateways to register themselves by modifying the allowUnknownEndpointRegistrations parameter in the MVAM initialization file. You must enable unknown Gateway registration when using a MultiVoice network to support PC-to-phone calls. For more information, see Appendix A, “MVAM initialization file.”

To display the status of any or all MultiVoice Gateways, access the main MVAM screen and click `Status: Gateways`. The Gateway Status screen appears. For example:

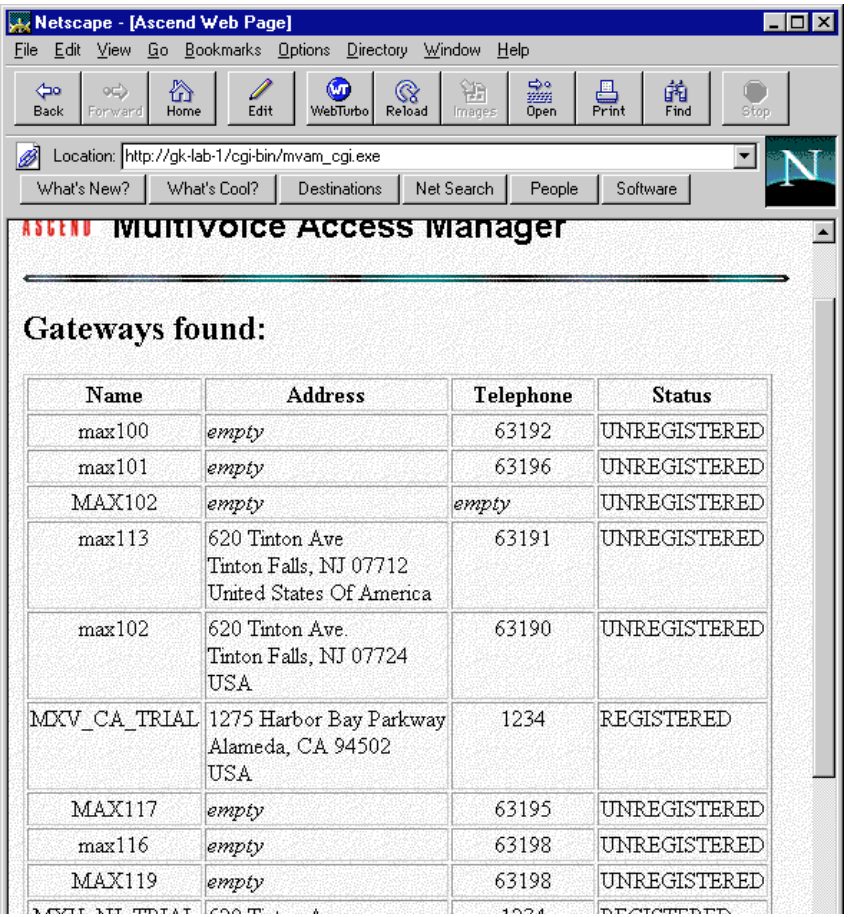


From the Gateway Status screen, you can:

- Display a list of all registered MultiVoice Gateways.

- Display a list of all MultiVoice Gateways, both registered and unregistered, stored in the MVAM gateway database.
- Display the name, address, and telephone number for an individual gateway.
- Enter information in any field and click the Submit button to have MVAM retrieve all Gateways that match the entered information.

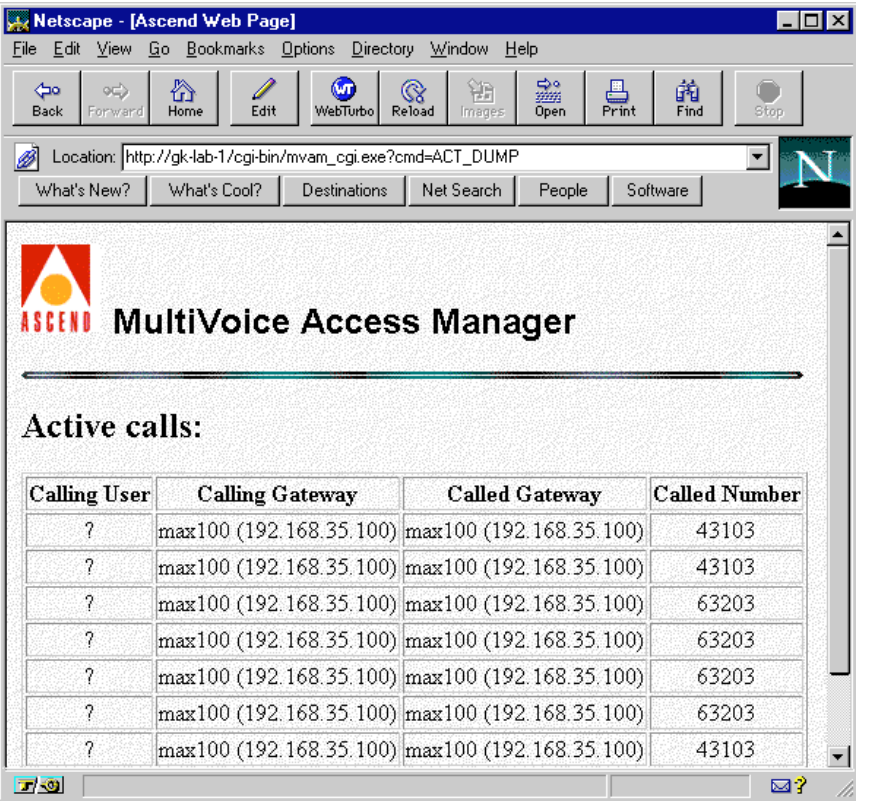
For example, clicking the Go button to the right of `Display the status of all administered gateways:` could display the following information:



Name	Address	Telephone	Status
max100	*empty*	63192	UNREGISTERED
max101	*empty*	63196	UNREGISTERED
MAX102	*empty*	*empty*	UNREGISTERED
max113	620 Tinton Ave Tinton Falls, NJ 07712 United States Of America	63191	UNREGISTERED
max102	620 Tinton Ave. Tinton Falls, NJ 07724 USA	63190	UNREGISTERED
MXV_CA_TRIAL	1275 Harbor Bay Parkway Alameda, CA 94502 USA	1234	REGISTERED
MAX117	*empty*	63195	UNREGISTERED
max116	*empty*	63198	UNREGISTERED
MAX119	*empty*	63198	UNREGISTERED

Monitoring the status of active calls

To display information about all active calls managed by MVAM, click `Status: Calls` on the main MVAM screen. The information appears on a screen similar to the following:



Calling User	Calling Gateway	Called Gateway	Called Number
?	max100 (192.168.35.100)	max100 (192.168.35.100)	43103
?	max100 (192.168.35.100)	max100 (192.168.35.100)	43103
?	max100 (192.168.35.100)	max100 (192.168.35.100)	63203
?	max100 (192.168.35.100)	max100 (192.168.35.100)	63203
?	max100 (192.168.35.100)	max100 (192.168.35.100)	63203
?	max100 (192.168.35.100)	max100 (192.168.35.100)	63203
?	max100 (192.168.35.100)	max100 (192.168.35.100)	43103

If you do not require either PIN or ANI authentication, the Calling User column contains question marks.

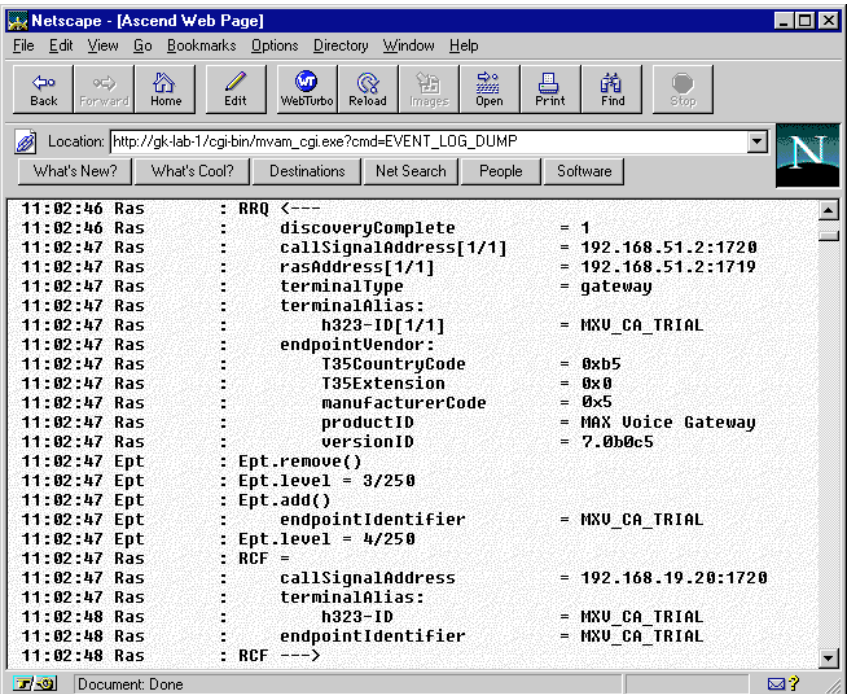
Logging event and call information

To enable you to keep historical information, the MVAM maintains an event log and call logs. The event log contains H.323-specific information from each call. Call logs are text files, containing start and stop records for each call, which you can analyze to produce billing records.

Event log

The gatekeeper running MVAM creates the event log when it boots, and maintains the log as long as MVAM is running. The event log contains H.323-specific information about communications between the MVAM and MultiVoice Gateways.

For example, the log might display following information when a MultiVoice Gateway registers itself with MVAM:



In the display:

- The MultiVoice Gateway, MXV_CA_TRIAL, sends an H.323 Registration Request (RRQ) packet to MVAM.
- MVAM uses the gateway name as an Endpoint Identifier to uniquely identify sessions with MXV_CA_TRIAL.
- MVAM sends an H.323 Registration Confirmation to MXV_CA_TRIAL.

If registration fails, MVAM sends a Registration Reject (RRJ) packet to the MultiVoice Gateway.

Communication between Gatekeepers and MultiVoice Gateways should be very similar to the above example. If you experience problems, contact Ascend Customer Service, as described in "Ascend Customer Service" at the beginning of this manual.

Call logs

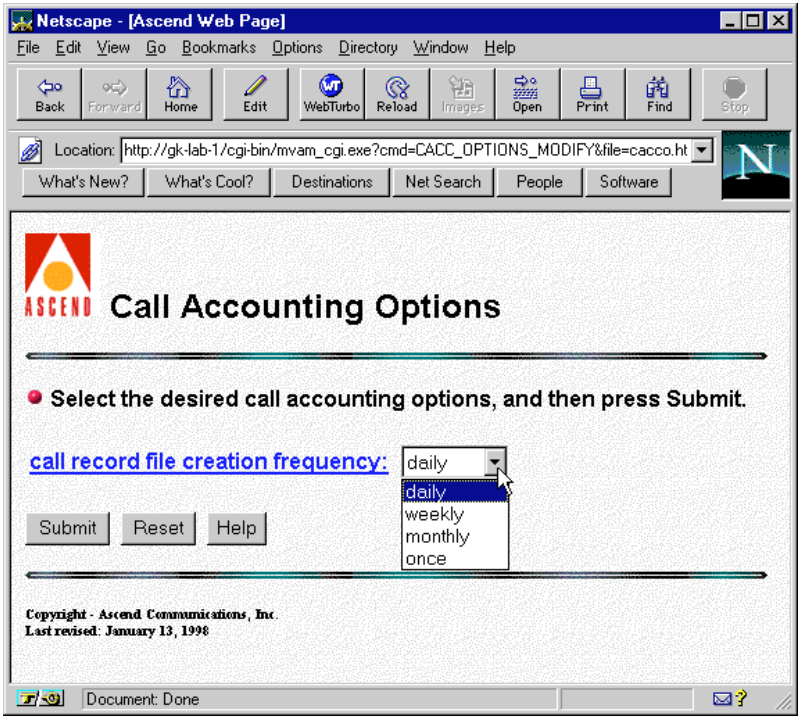
Call logs are text files containing start and stop records for each call. You can analyze them to produce billing records. You specify whether the MVAM maintains one call log or creates and maintains call logs daily, weekly, or monthly. The data in the call logs is comma delimited, so you can parse it to produce billing records.

Setting call-log frequency

To set call-log frequency:

1 From the main MVAM screen, select `call accounting`.
The Call Accounting Options screen appears.

2 On the right side of the `call record file creation frequency` field, click the Down arrow to display available selections. For example:



3 Select a value.

4 On the lower-left section of the screen, click the Submit button.

Note: To reset `call record file creation frequency` to its default value of daily, click the Reset button.

To determine where one call-log file ends and the next begins, MVAM makes the following assumptions:

- Months begin on the first day of the month
- Weeks begin on Sunday.
- Days begin at midnight.

Call log files

MVAM writes call-log information to the `calls.txt` file, which is located in `c:\mvam\calls\current` on a Windows NT system and `/opt/mvam/calls/current` on a SPARC Solaris system.

File Creation

If you set the `call record file creation frequency` field to Once on the Call Accounting Options screen, the `calls.txt` file continues to grow as long as the computer running MVAM has available storage space. If you select one of the other options, MVAM saves `calls.txt` to a new file at the frequency you specify. The filename has the following format:

```
mmddyyyy.txt
```

where:

- `mm` is the month (01 to 12) the MVAM saves the file.
- `dd` is the day (01 to 31) the MVAM saves the file.
- `yyyy` is the year the MVAM saves the file.

Example

The following file, `03121998.txt`, was created March 12, 1998:

```
version,1.0.0
start,03/26/1998,13:46:15,727bc000-5824-0002-212b-d61d70f99b
32,128000,14155551212:dmiller,10.10.10.123:max123:gw,10.10.1
0.124:max124:gw,85996:jdavidson
stop,03/26/1998,13:46:16,727bc000-5824-0002-212b-d61d70f99b3
2,10.10.10.123:max123:gw,normalDrop,1
start,03/26/1998,13:58:25,727bc000-5824-0002-212b-d31d70f99b
9e,128000,?:?,10.10.10.123:max123:gw,10.10.10.124:max124:gw,
85996:?
stop,03/26/1998,13:58:26,727bc000-5824-0002-212b-d31d70f99b9
e,10.10.10.123:max123:gw,normalDrop,1
```

Start Record Contents

Each start record contains the following information:

- The word `start`.
- The date and time the call started.
- A unique identifier (to enable you to match start records with stop records).
- The bandwidth used by the call.
- Calling-party identifier, in the format *`Calling telephone number:user alias`* (MVAM records calling-party information if it performs PIN or ANI authentication. Otherwise, MVAM does not match the calling-party to its user database, and the call-log files list the calling-party indentifier as `?:?`)

  Note: For PC-to-phone calls, MVAM does not record a calling telephone number or user alias.
- Calling MultiVoice Gateway identifier, in the format *`IP address:Name:Type`* (this is either `gw`—MultiVoice Gateway; or `tm`—terminal.)
- Called MultiVoice Gateway identifier, in the format *`IP address:Name:Type`* (this is either `gw` —MultiVoice Gateway; or `tm`—terminal.)
- Called-party identifier, in the format *`Called telephone number:user alias`*. (MVAM records the called party user alias if the caller dials a telephone alias. In place of a full telephone number. When a caller dials a telephone alias, MVAM searches in the user database for the dialed telephone alias. When it matches the telephone alias to a user record, MVAM logs the user alias. Otherwise, MVAM logs the called-party user alias as `?`)

Stop Record Contents

Each stop record contains the following information:

- The word `stop`.
- The date and time the call ended.
- A unique call identifier (to enable you to match start records with stop records).

- Disconnecting MultiVoice Gateway identifier, in the format *IP address:Name:Type* (this is either gw—MultiVoice Gateway; or tm—terminal.)
- H.323 call-disconnect reason. (The MVAM reports one of the three following H.323 disconnect reasons: forcedDrop, normalDrop, or gatewayFailure.)
- Length of call, in seconds.

The way in which calls are terminated provides the MultiVoice network administrator with one indication of how well MultiVoice Gateways are working.

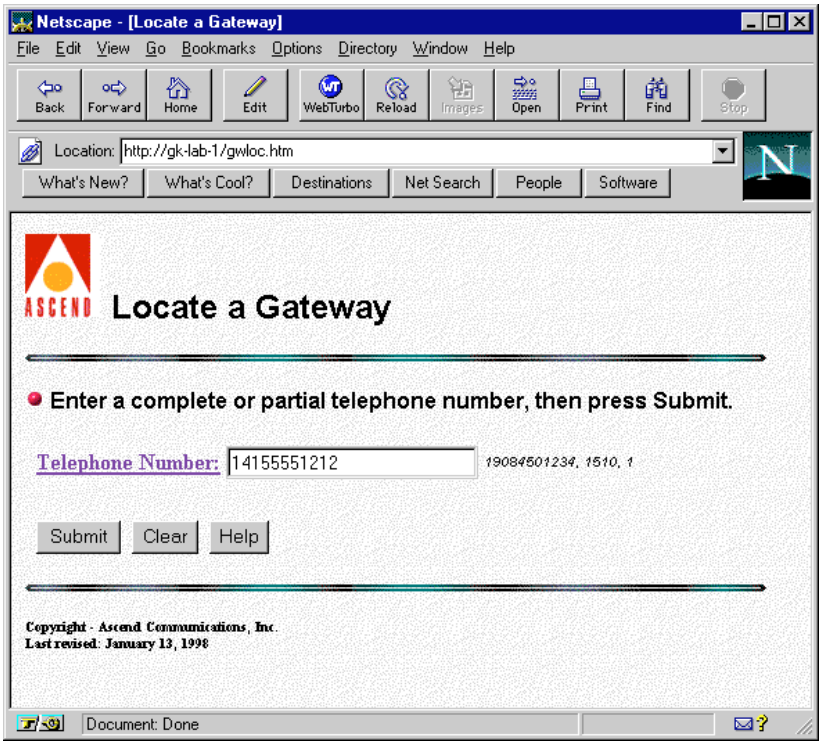
Disconnect Reason	Condition
normalDrop	The call ended normally. Call progress signals are being processed correctly by the MultiVoice Gateways.
gatewayFailure	The call was dropped when one of the MultiVoice Gateways failed to reregister.
forcedDrop	(Reserved for future use.) A command was issued from the MultiVoice Access Manager to terminate the call connection.

Locating MultiVoice Gateways for callers

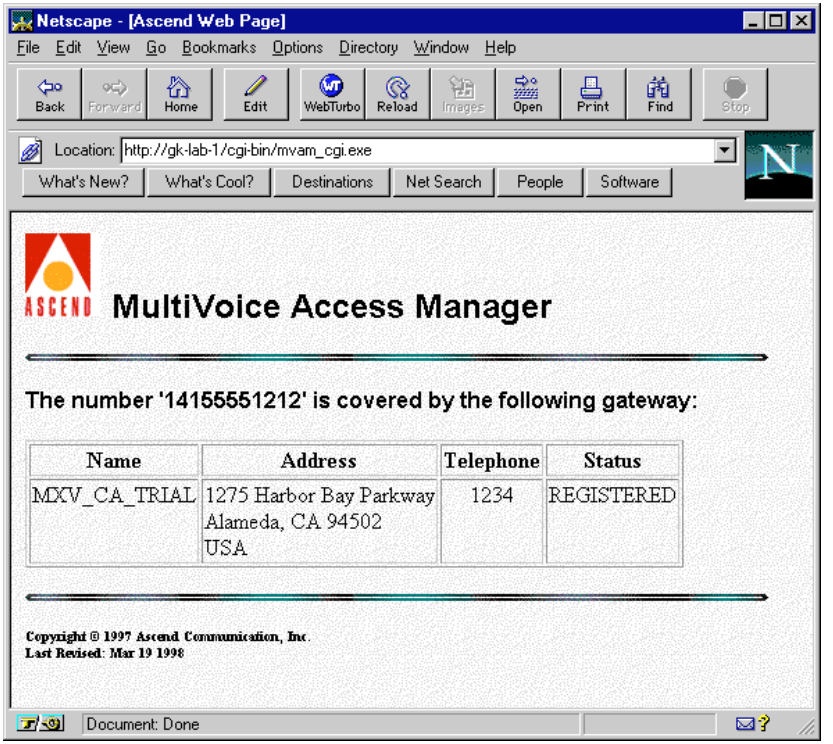
A complex MultiVoice network may include several MultiVoice Gateways, each supporting a coverage area with ten or more Inclusion Areas. To find the name and phone number of a specific MultiVoice Gateway that supports a specific Inclusion Area, you can use the MVAM's Gateway Locator feature.

To locate a MultiVoice Gateway supporting a specific inclusion area, click gateway locator on the main MVAM screen. The Locate a Gateway screen appears.

Enter a partial or complete phone number. For example:

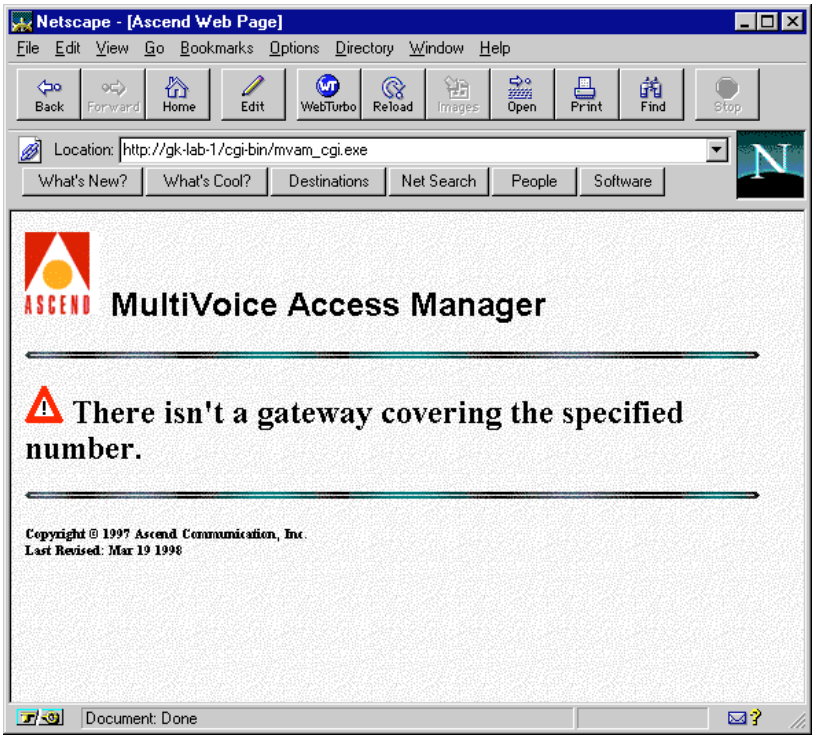


When you click the Submit button, MVAM searches its Gateway database. When it finds a MultiVoice Gateway that supports the telephone number, MVAM displays the phone number and address of the MultiVoice Gateway. For example:



In this example, the MultiVoice network administrator could tell the caller at 14155551212 that the local MultiVoice Gateway can be reached by dialing 1234.

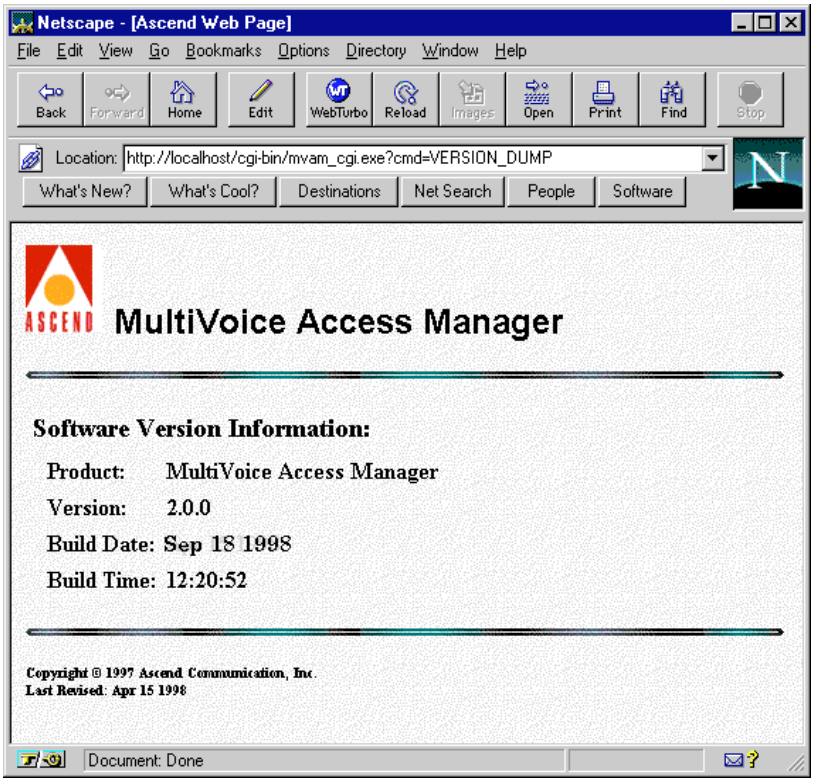
If no registered MultiVoice Gateway has a coverage area that supports the phone number you enter, MVAM displays the following message:



Make sure that the phone number is correct and that any covering MultiVoice Gateway is registered with the MVAM application.

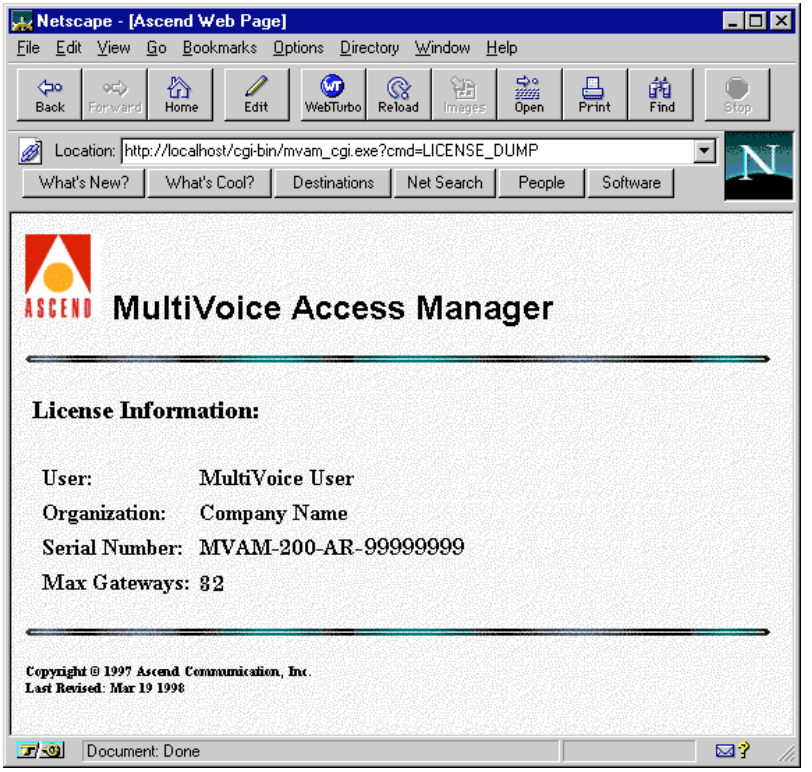
Displaying MVAM version and license

To display MVAM software version information, click `version` on the main MVAM screen. A screen similar to the following appears:



The machine in this example, is running MVAM version 2.0.0. The software was created on September 18, 1998 at 12:20 p.m.

To display the MVAM licensing information, click `license` on the main MVAM screen. A screen similar to the following appears:



In this example, the program's serial number is MVAM-200-AR-99999999, and it supports a maximum of 32 registered MultiVoice Gateways.

Licenses for MVAM installed on a Windows NT system support a maximum of 4, 32, or 128 MultiVoice Gateways. Licenses for MVAM installed on a SPARC Solaris system support a maximum of 32 or 256 MultiVoice Gateways. For details about upgrading an MVAM license, contact an authorized Ascend representative.

Troubleshooting

5

Ensure the MultiVoice environment is set up correctly

For calls to connect successfully when MVAM does not require either ANI or PIN authentication, make sure that:

- You installed a MultiVoice Gateway license on the MVAM.
- The MultiVoice Gateway is on. (For details about configuring MultiVoice Gateways, see the *MultiVoice Gateway for the MAX—Users Guide*.)
- On each MultiVoice Gateway, the Ethernet > Mod Config > VOIP Options > GK IP Adrs parameter specifies the IP address of the Gatekeeper running MVAM.
- On each MultiVoice Gateway, the Ethernet > Mod Config > VOIP Options > VPN Mode parameter is set to Yes.
- The Ethernet > Mod Config > VOIP Options > Pkt Audio Mode parameter is identical for all MultiVoice Gateways.

- The setting on the MultiVoice Gateway for the System > Sys Config > Name parameter matches the name of the MultiVoice Gateway as specified in the MVAM.
- MultiVoice Gateways are registered in MVAM.
- You have configured a MultiVoice Gateway with a coverage area that supports the called number.
- Callers are dialing phone numbers correctly.
- For callers dialing telephone aliases, their user records specify both telephone aliases, and full telephone numbers.
- The network is free of problems.

When MVAM requires PIN authentication, make sure that:

- On each MultiVoice Gateway, you set the Ethernet > Mod Config > VOIP Options > VPN Mode parameter to No.
- In MVAM, you select the PIN Authentication check box on the Security Options screen.
- Each caller enters a correct PIN number and phone number.

When MVAM requires ANI authentication, make sure that:

- On each MultiVoice Gateway, you set the options under Net/T1 > Line Config > Factory for ANI collection.
- In MVAM, you select the ANI Authentication check box on the Security Options screen.
- In MVAM, you set User Alias on the Add a User screen to specify the CLID for the user's telephone number.

Possible problems and solutions

This section lists a few specific problems that might occur, and describes how to resolve them. (For details about configuring MultiVoice Gateways, see the *MultiVoice Gateway for the MAX—Users Guide*.)

The Web browser wants to download mvam.exe

While attempting to configure MVAM through the Web interface; your Web browser asks if you want to download `mvam.exe`. If this happens:

- Check your Web server configuration. Make sure is was properly configured to support CGI scripts.
- Check the URL you're using to access MVAM. Make sure you have not opened a file URL.

MVAM is started, but nothing appears in the interface

If you launch MVAM, and the MVAM interface screen appears, but the window is empty, check the following sections of the `mvam.ini` file. on Windows NT systems or `.mvam.ini` on SPARC Solaris systems to ensure the values are set correctly. (For a description of the MVAM Interface screen, see “MVAM interface screen” on page 5-15.)

Section	Parameter(s)	Setting
[supserve]	integratedWindow	Must be any value greater than 0. Default value is 2.
[insertIntoWin]	(all parameters)	The appropriate parameters must be set to 1 to display information in the MVAM interface screen. Default value is 0, or show nothing.

For more information on setting these values, see Appendix A, “MVAM initialization file”.

MVAM doesn't create an event log

If you successfully started MVAM, and MVAM didn't create an event log (e.g., `/mvam/event/log.txt`), check the following sections of the `mvam.ini` file on Windows NT systems or `.mvam.ini` on SPARC Solaris systems to ensure the values are set correctly.

Section	Parameters	Setting
[supserve]	msgfile	Must be any value greater than 0. Default value is 2.
[insertIntoFile]	(all parameters)	The appropriate parameters must be set to 1 to record information in the event-log. Default value is 0, or write nothing to the event-log.

For more information on setting these values, see Appendix A, "MVAM initialization file" for more information.

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 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, check that the correct CLID is entered for this user's User Alias, and that the network supports delivery of ANI signals.

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.

For details about testing for DNIS signals on a MultiVoice Gateway, see the *MultiVoice Gateway for the MAX—Users Guide*.

MVAM does not register a correctly configured gateway

IP-network congestion can cause Registration Request (RRQ) packets to be lost before they reach the Gatekeeper. In this case:

- To verify connectivity, Ping the MultiVoice Gateway and the MVAM from any IP host on the network. Many Ping utilities record the delay between the time the Ping request is sent and the time a response is received. Long delays can indicate network congestion problems.
- Make sure the settings for Reg Retry and Keepalive Timer are appropriate for the operating conditions on you network, and the registrationDuration setting on MVAM is set appropriately. Assign a value to registrationDuration which adds a 30-second buffer to the interval specified by Keepalive Timer, increasing the MVAM registration time interval. Reducing the value for Keepalive Timer will cause the MultiVoice Gateways to register more frequently. Increasing the value of Reg Retry will force the MultiVoice Gateway to make additional attempts to register if the first registration attempt fails.

You cannot connect to the MVAM from the Web browser

If your cannot connect to MVAM, make sure you are using either of the following supported Web browsers:

- Microsoft Internet Explorer, version 3.02 or later.
- Netscape Navigator, version 3.01 or later, or Netscape Communicator.

Make sure you have installed and configured a Web server on the computer running MVAM, and that proper access permissions have been set.

Make sure you set the HTML document path and `cgi` path correctly. Unless you changed the defaults when you installed MVAM, the HTML document path points to the `webpages` subdirectory under the MVAM installation directory, and the `cgi` path points to the `cgi-bin` subdirectory under the MVAM installation directory.

If MVAM is installed on a Windows NT system, maker sure you have disabled any other Web server that might be enabled by default in Windows NT > Control Panel > Services.

Error messages

This section lists common MVAM error messages and explains their possible causes.

You don’t have a valid gateway license

The MVAM stopped at start-up because it could not find a valid MultiVoice Gateway license.

Run the MultiVoice Access Manager License Installer (Windows NT) or `textlicapp` (SPARC Solaris) to install a MultiVoice Gateway license. (See Appendix B, “Upgrading the MVAM License” for instructions.) You will need the serial number from your MultiVoice Access Manager Warranty Registration card.

The Gatekeeper application is not running

You are connecting to a network workstation or server that is not running MVAM.

Make sure that:

- The MVAM application is started before you open the Web-based user interface.
- You entered the correct IP address of the Gatekeeper from your Web browser.
- There are no network problems that might prevent your Web browser from connecting to the network workstation or server running MVAM.

If you still experience problems, restart the computer that is running MVAM, then restart MVAM and the Web browser.

There are no registered gateways

MVAM does not have any configured MultiVoice Gateways with a status of Registered. MultiVoice Gateways must register themselves with an MVAM Gatekeeper to be available for calls. MVAM does not forward a call to an

unregistered MultiVoice Gateway, even if the MultiVoice Gateway's coverage area supports the call. MVAM rejects any requests from unregistered MultiVoice Gateways.

To register a MultiVoice Gateway:

1. On the MultiVoice Gateway, set the Ethernet > Mod Config > VOIP Options > GK IP Adrs parameter to the IP address of the MVAM Gatekeeper.
2. In MVAM, add the MultiVoice Gateway to the Gateway database by clicking `Admin: Gateways` on the main MVAM screen and then clicking `add a gateway`.

When a correctly configured MultiVoice Gateway boots, it sends an H.323 Registration Request (RRQ) packet to MVAM. When MVAM registers the MultiVoice Gateway, it sends a Registration Confirmation (RCF).

No matching gateways found

MVAM could not find in its Gateway database a MultiVoice Gateway that contains the values you entered.

Make sure you entered the values correctly, and that the MultiVoice Gateway records in MVAM contain correct information.

There are no active calls

If you click `Status: calls` on the main MVAM screen, MVAM displays only currently active calls. This error message appears if there are none.

No calls have been made

If you click `Logs: call` on the main MVAM screen, MVAM displays an archive of previous calls. This error message appears if MVAM has never set up any MultiVoice calls.

There isn't a gateway covering the specified number

MVAM could find no MultiVoice Gateway that supports the number you entered on the Locate a Gateway screen.

Make sure you entered the number correctly, and that the MultiVoice Gateways configured in MVAM contain correct coverage areas.

'Gateway Name' is not unique

You have attempted to add a MultiVoice Gateway with a name that you have specified for another MultiVoice Gateway.

MultiVoice Gateways cannot share identical names.

The specified gateway is not administered

There is no MultiVoice Gateway with the name you entered.

Make sure that you entered the name correctly, and that you added the MultiVoice Gateway to MVAM.

The specified user is unknown

There is no user with the name you entered.

Make sure that you entered the name correctly, and that you added the user to MVAM.

'User Alias' is not unique

You have attempted to added a user with a name that you have specified for another user.

Users cannot share identical User Alias values.

The dialing prefixes must be unique

You have attempted to assign the same dialing prefix to both the telephone alias and the full telephone number. The dialing prefix must be unique, because the MVAM must be able to differentiate between an alias and a full number.

Failed to connect to the registry server (Solaris only)

You started the MVAM using `mvam.sh`, but one of following errors occurred:

- No IP address is mapped to the simple (unqualified) host name of the MVAM Gatekeeper. This prevented MVAM from initiating RPC processing.

  Make sure that the simple (unqualified) host name of the server resolves to an IP address. To test whether a name resolution problem exists, attempt to open a Telnet session, from the MVAM Gatekeeper, using the simple host name for the Solaris system. For example:

  `# telnet` *`foo`*

  If you see the error message `foo:Unknown host`, edit the `/etc/hosts` or `/etc/resolv.conf` file on foo.

- The `daemons` script did not start. The script initializes a server library that supports the MVAM application. To initialize the server library, you must execute the following command:

  `$HOME/bin/daemons start`

  $HOME is the MVAM installation directory. Wait until the shell prompt appears, then execute `mvam.sh`. If this problem persists, contact Ascend Customer Service for assistance.

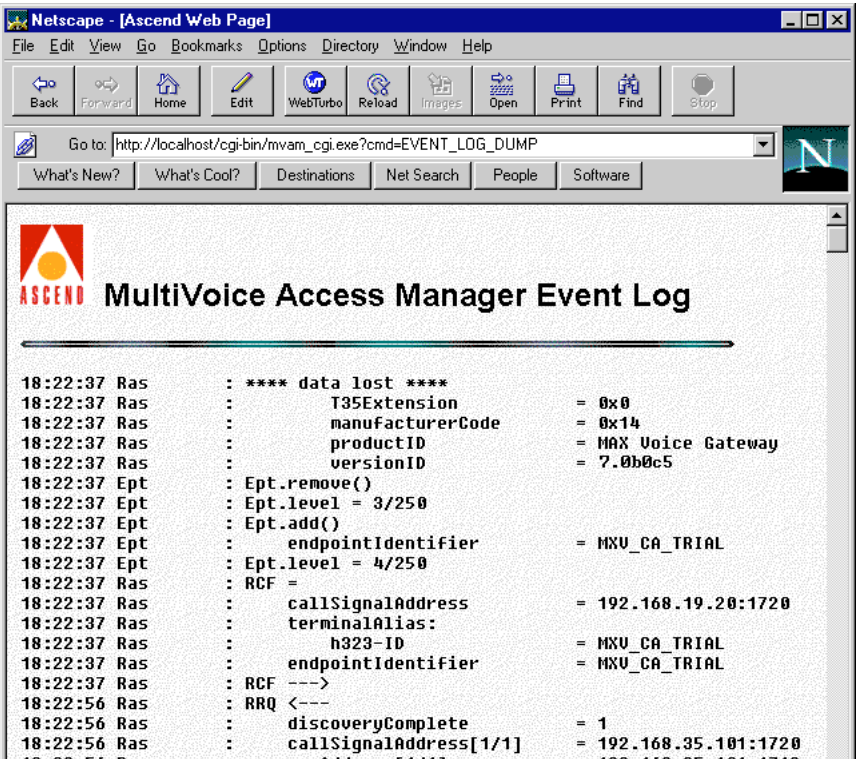
Additional troubleshooting resources

You can use the MVAM event log to troubleshoot problems on the MultiVoice network. You can also use the MVAM interface screen, which appears on the computer running MVAM when MVAM starts.

Event logs

By viewing the event log, you can research possible problems with MultiVoice Gateway registration and call establishment.

From the main MVAM screen, click `event` to display the event log. The event log lists the communications between MultiVoice Gateways and MVAM. For example:



Because the event-log file can become very large, the MVAM initialization file specifies the maximum size the event-log file can become. When the maximum size is reached, MVAM clears the earliest messages from the file and adds the new messages. When it clears messages, MVAM displays the message `****data lost ****`, as shown in the preceding example.

Troubleshooting MultiVoice Gateway registration

The event log shows communication as MultiVoice Gateways register with MVAM. The following sequence of messages show the MultiVoice Gateway `max101` (with an IP address of 10.10.10.1) registering itself with the MVAM Gatekeeper (IP address 20.20.20.1):

```
13:25:20 Ras   : RRQ <---
13:25:20 Ras   :   discoveryComplete       = 1
13:25:20 Ras   :   callSignalAddress[1/1]  = 10.10.10.1:1720
13:25:20 Ras   :   rasAddress[1/1]         = 10.10.10.1:1719
13:25:20 Ras   :   terminalType            = gateway
13:25:20 Ras   :   terminalAlias:
13:25:20 Ras   :       h323-ID[1/1]        = max101
13:25:20 Ras   :   endpointVendor:
13:25:20 Ras   :       T35CountryCode      = 0xb5
13:25:20 Ras   :       T35Extension        = 0x0
13:25:20 Ras   :       manufacturerCode    = 0x14
13:25:20 Ras   :       productID         = MAX Voice Gateway
13:25:20 Ras   :       versionID           = 7.0b05
13:25:20 Ept   : Ept.remove()
13:25:20 Ept   : Ept.level = 2/250
13:25:20 Ept   : Ept.add()
13:25:20 Ept   :     endpointIdentifier    = max101
13:25:20 Ept   : Ept.level = 3/250
13:25:20 Ras   : RCF =
13:25:20 Ras   :     callSignalAddress     = 20.20.20.1:1720
13:25:20 Ras   :     terminalAlias:
13:25:20 Ras   :         h323-ID           = max101
13:25:20 Ras   :     endpointIdentifier    = max101
13:25:20 Ras   : RCF --->
```

The MultiVoice Gateway sends an H.323 Register Request (RRQ) packet to MVAM. MVAM verifies that the MultiVoice Gateway is in its database, then sends a Register Confirmation (RCF) packet to the MultiVoice Gateway.

Troubleshooting call establishment

The event log shows messages from successful and unsuccessful calls.

Example of a successful call

The following messages show an example of communication between MVAM and a MultiVoice Gateway as a call connects:

```
13:25:20 Ras   : ARQ --->
13:25:20 Ras   : ARQ <---
13:25:20 Ras   :   endpointIdentifier        = test_gw
13:25:20 Ras   :   destinationInfo.e164[1/1] = 43105
13:25:20 Ras   :   srcCallSignalAddress    = 10.10.10.1:1720
13:25:20 Ras   :   srcInfo:
13:25:20 Ras   :       h323-ID[1/1]          = test_gw
13:25:20 Ras   :   bandWidth                 = 64000
13:25:20 Ras   :   conferenceID          = 3030303-3030-3030
13:25:20 Ras   :   answerCall                = 0
13:25:20 Ras   :   pin                       = encrypted
13:25:20 Ras   : Arq.process<>
13:25:20 Ras   : terminalType                = gateway
13:25:20 Ras   : >>> proxy near-end adminssion request
13:25:20 Ept   : >>> PIN not reqd, all users are authorized
13:25:20 Ept   : Locator.resolve<>
13:25:20 Ept   :     pass_thru_dialing<43105>
13:25:20 Ept   :     destination ip address  = 20.20.20.1
13:25:20 Ept   :     destination dial string =43105
13:25:20 Ras   : ACF --->
13:25:20 Ras   :     bandWidth               = 64000
13:25:20 Ras   :     callModel               = direct
13:25:20 Ras   :     destCallSignalAddress = 20.20.20.1:1720
13:25:20 Ras   :     destDialString          = 43105
13:25:20 Ras   : ACF <---
13:25:20 Ras   :     bandWidth               = 64000
13:25:20 Ras   :     callModel               = direct
```

```
13:25:20 Ras   :     destCallSignalAddress = 20.20.20.1:1720
13:25:20 Ras   :     destDialString          = 43105
```

The MultiVoice Gateway sends an H.323 Admission Request (ARQ) packet to MVAM. MVAM searches for a destination MultiVoice Gateway in its database, then sends information and an Admission Confirmation (ACF) packet to the MultiVoice Gateway.

When a call disconnects, the following messages appear:

```
13:25:20 Ras  : DRQ --->
13:25:20 Ras  : DRQ <---
13:25:20 Ras  :    endpointIdentifier     = test_gw
13:25:20 Ras  :    conferenceID      = 30303030-3030-3030
13:25:20 Ras  :    callReferencValue      = 1
13:25:20 Ras  :    disengageReason        = normalDrop
13:25:20 Ras  : Act.remove<>
13:25:20 Ras  : Act.level = 0/250
13:25:20 Ras  : DCF --->
13:25:20 Ras  : DCF<---
```

MVAM sends an H.323 Disconnect Request (DRQ) packet to the MultiVoice Gateway. The MultiVoice Gateway sends an Disconnect Confirmation (DCF) packet to MVAM.

If you experience call connection or disconnection problems, the call logs might display possible errors.

Example of an unsuccessful call

In the following example, MVAM could not find a registered MultiVoice Gateway to which to route a received call:

```
14:31:35 Ras   : ARQ <---
14:31:35 Ras   :    endpointIdentifier    = MXV_CA_TRIAL
14:31:35 Ras   :    destinationInfo.e164[1/1]  = 01234
14:31:35 Ras   :    srcCallSignalAddress    = 192.168.51.2:0
14:31:35 Ras   :    srcInfo:
14:31:35 Ras   :       h323-ID[1/1]          = MXV_CA_TRIAL
```

```
14:31:35 Ras   :   bandWidth               = 128000
14:31:35 Ras   :   confID=34343456-ef34-0007-212b-fa1f38
14:31:35 Ras   :   answerCall              = 0
14:31:35 Ras   : Arq.process()
14:31:35 Ras   :   terminalType            = gateway
14:31:35 Ras   :   >>> proxy near-end admission request
14:31:35 Ras   :   >>>PIN not reqd, all users are authorized
14:31:35 Locator: Locator.resolve()
14:31:35 Locator:   pass_thru_dialing(01234)
14:31:35 Locator:
14:31:35 Locator: *** WARNING ***>>>
14:31:35 Locator: There isn't a covering gateway.
14:31:35 Locator:
14:31:35 Locator:     destination ip address     =
14:31:35 Locator:     destination dial string    = 01234
14:31:35 Ras   :
14:31:35 Ras   : *** ERROR ***>>>
14:31:35 Ras   : can't translate far-end address
14:31:35 Ra    :
14:31:35 Ra    : ARJ =
14:31:35 Ras   :   rejectReason = calledPartyNotRegistered
14:31:35 Ras   : ARJ --->
```

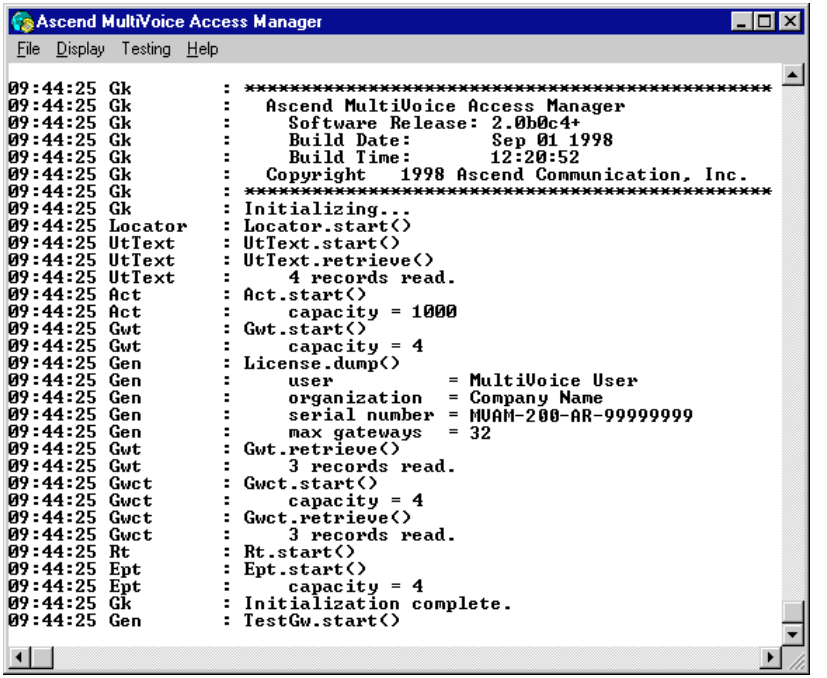
MVAM interface screen

The MVAM Interface screen displays real-time information and enables you to test communication with the MVAM application.

Viewing real-time information

The MVAM Interface screen displays real-time information when the MVAM starts, when MultiVoice Gateways register, and when calls connect and disconnect. The registration and call connection messages are similar to those that MVAM sends to call logs.

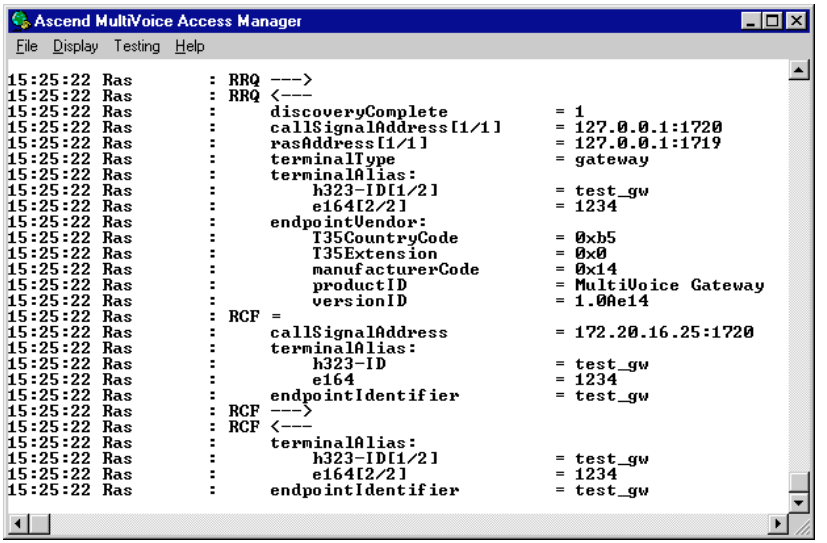
When you launch MVAM, the MVAM interface screen appears. For example, when MVAM starts up correctly, messages similar to the following appear:



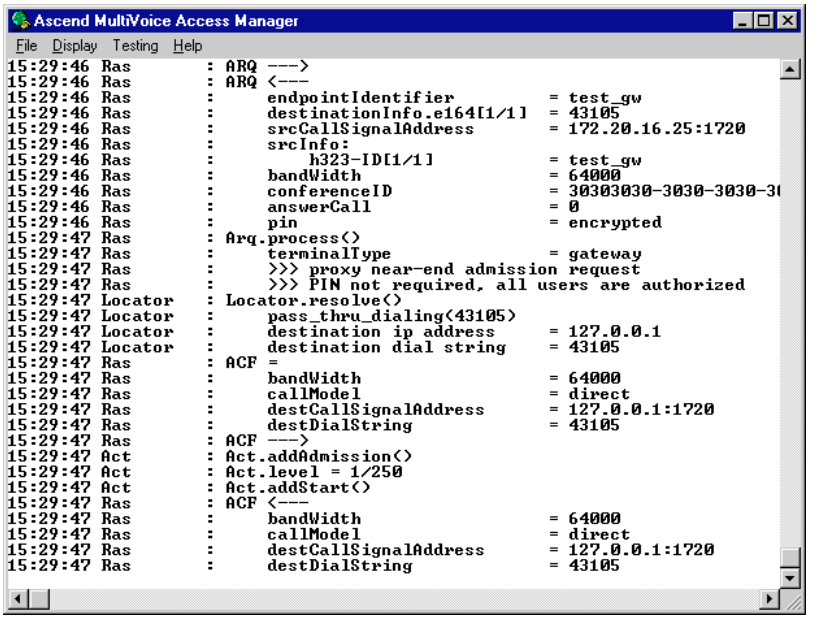
If you suspect MVAM problems, look for error messages on the MVAM interface screen.

Testing MVAM communication

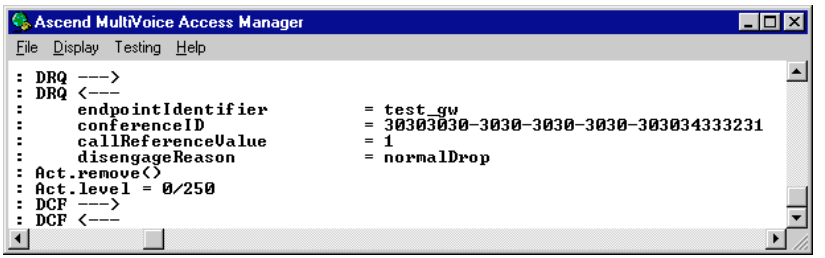
The MVAM interface screen enables you to test MVAM communication by viewing the results of simulated registration and call requests. The following screen displays the results from a successful MultiVoice Gateway registration test:



The following screen displays the results from a successful call establishment test:



The following screen displays the results from a successful call disconnection test:



MVAM initialization file

A

When you install MVAM, the MVAM installer creates the initialization file `mvam.ini` for Windows NT systems, or `.mvam.ini` for SPARC Solaris systems. The initialization file contains parameters that MVAM loads at start-up. When you make changes to the initialization file, the changes are applied when you restart the MVAM application.

You should not have to change any settings in the file. You configure the most common settings in MVAM through the Web browser connection, or during installation.

Caution: Copy the original initialization file (`mvam.ini` on Windows NT, or `.mvam.ini` on SPARC Solaris) to `mvam.ini.old` before modifying the file.

Table A-1 shows the parameters stored in the MVAM initialization file, including the default settings. Parameters followed by an asterisk (*) are configured through the MVAM installation program.

Table A-1. MVAM initialization file parameters

Section	Parameter	Description	Default Value
Gk	debugPrinting	Enables/disables application level event logging: 0 = No 1 = Yes	1

Table A-1. MVAM initialization file parameters (continued)

Section	Parameter	Description	Default Value
Gwt[a]	file	Path and filename of the MultiVoice Gateway database.	c:\mvam\db\gwt.txt (WinNT) /opt/mvam/db/gwt.txt (Solaris)
Gwct[a]	file	Path and filename of the MultiVoice Gateway coverage-area database.	c:\mvam\db\gwct.txt (WinNT) /opt/mvam/db/gwct.txt (Solaris)
Gwct[a]	inclusionListCapacity	Defines the maximum number of Inclusion Areas allowed per MultiVoice Gateway. Valid values are 1 through 2000 (maximum)	2000
Gwct[a]	inclusionList DisplayCapacity	Defines the maximum number of Inclusion Areas displayed per MultiVoice Gateway on screens that display Inclusion areas. Valid values are 1 through the value of inclusionListCapacity	26
UtOdbc[b]	prompt	Determines if the user is prompted for data source information. If you set it to No, MVAM uses the parameters dataSourceName, tableName, userName, and password: Yes No	No

Table A-1. MVAM initialization file parameters (continued)

Section	Parameter	Description	Default Value
UtOdbc[b]	dataSourceName	Data source name (DSN) of the ODBC-compliant database.	mvamUser
UtOdbc[b]	tableName	Name of the table in the ODBC-compliant database.	mvamUser
UtOdbc[b]	userName	Login user name for the ODBC-compliant database.	NULL
UtOdbc[b]	password	Login password for the ODBC-compliant database.	NULL
UtOdbc[b]	userAlias ColumnName	Name of the column containing the User Alias field.	userAlias
UtOdbc[b]	userName ColumnName	Name of the column containing the User Name field.	userName
UtOdbc[b]	phoneNum ColumnName	Name of the column containing the Telephone Number field.	phoneNum
UtOdbc[b]	phoneAlias ColumnName	Name of the column containing the Telephone Alias field.	phoneAlias
UtOdbc[b]	pinColumnName	Name of the column containing the PIN field.	pin
UtText[a]	file	Path and filename of the user database.	c:\mvam\db\user.txt (WinNT) /opt/mvam/db/user.txt (Solaris)

Table A-1. MVAM initialization file parameters (continued)

Section	Parameter	Description	Default Value
UtText	capacity	Maximum number of records allowed in the user database. Valid entries are 1 through 1,000 (maximum)	1000
Ept	capacity	Number of endpoints allowed to register. This is limited to the number of installed Gateway licenses.	number of installed Gateway licenses
Ept	agedRegistration	Determines whether MultiVoice Gateways must perform keep-alive registrations: 0 = False 1 = True	1
Ept	registrationDuration	Sets the Gateway reregistration time interval, in seconds. By default, includes a 30-second buffer to reduce the frequency of expired Gateway registrations.	150
Ept	dropCallsOn ExpiredGateways	Determines whether MVAM logs active calls on an unregistered MultiVoice Gateway as dropped calls: 0 = False 1 = True (default)	1

Table A-1. MVAM initialization file parameters (continued)

Section	Parameter	Description	Default Value
Act	enabled	Determines whether MVAM logs calls in the Active Call table: 0 = False 1 = True (default)	1
Act	capacity	Maximum number of calls that MVAM can monitor.	1000
Act[b]	frequency	Specifies how often MVAM creates a new call-log file: once daily (default) weekly monthly	daily
Act[a]	filePath	Path to the MVAM call-log file.	c:\mvam\calls\ (WinNT) /opt/mvam/calls (SPARC Solaris)
Gkcp[a]	webPagePath	Path to the MVAM Web pages.	c:\mvam\webpages\ (WinNT) /opt/mvam/htdocs/ (SPARC Solaris)
EventLog	size	Maximum number of lines allowed in the event-log.	1000
EventLog[a]	file	Path and name of the event-log file.	c:\mvam\events\log.txt (WinNT) /opt/mvam/events/log.txt (SPARC Solaris)

Table A-1. MVAM initialization file parameters (continued)

Section	Parameter	Description	Default Value
RtEventLog	size	Determines how many events that MVAM can queue in the real-time event log (viewed via Web browsers).	1000
RtEventLog	synchronous	Determines whether or not MVAM writes events synchronously to the real-time event log: 0 = False (default) 1 = True	0
CallLog	size	Maximum number of lines allowed in the MVAM call-log file.	1000
Sec	proxyPinRequired	Determines whether or not the MVAM performs PIN authentication: 0 = False (default) 1 = True	0
Sec	callerIdRequired	Determines whether or not the MVAM performs ANI authentication: 0 = False (default) 1 = True	0

Table A-1. MVAM initialization file parameters (continued)

Section	Parameter	Description	Default Value
Sec	displayPinInEventLog	Determines whether or user PINs are included in the event log displayed on the screen: 0 = False (default) 1 = True	0
Sec	pinSize	Determines whether or not the MVAM performs PIN authentication. Valid values are 1 through 24.	10
Locator	passThruPrefix	Pass-Through dialing prefix. Valid entries are *1 through *9.	(*No Value assigned*)
Locator	aliasPrefix	Telephone Alias dialing prefix. Valid entries are *1 through *9.	*2
Ras	useArqToStart	Determines whether to use the ARQ message or the BRQ message to signify the beginning of a call. Basically, the ARQ message signifies a call attempt. The BRQ signifies a call connect: 0 = BRQ (default) 1 = ARQ	0

Table A-1. MVAM initialization file parameters (continued)

Section	Parameter	Description	Default Value
Ras	allowUnknown EndpointRegistrations	Determines whether or not unknown MultiVoice Gateways are allowed to register themselves with MVAM: 0 = No (default) 1 = Yes	0
Ras	forceDialString InAcfNonStd	Determines whether or not MVAM puts the destination dial string in the nonstandard data parameter of an ACF, even if there has been no address translation: 0 = False 1 = True (default)	1
Ras	allowTerminals	Determines whether or not unknown H.323 terminals (PCs) are allowed to register themselves with MVAM: 0 = No (default) 1 = Yes	0

Table A-1. MVAM initialization file parameters (continued)

Section	Parameter	Description	Default Value
supserve	deblevel	Determines the amount of stack information MVAM sends to Event log. Valid values for this parameter are 0 through 3. A value of 0 specifies that the MVAM sends no information. A 3 specifies that the MVAM sends the maximum amount of information.	1 (WinNT) 0 (SPARC Solaris)
supserve	integratedWindow	Four possible values provide the following specifications: 0—MVAM sends no events to the Events Log screen. 1—MVAM sends all events to the Events Log screen, except for those sources listed in the removeFromWin section. 2—MVAM sends only the sources listed in the inserIntoWin section to the Events Log screen. 3—MVAM sends all events to the Events Log screen.	2

Table A-1. MVAM initialization file parameters (continued)

Section	Parameter	Description	Default Value
supserve	msgfile	Four possible values provide the following specifications: 0—MVAM sends no events to the Events Log file. 1—MVAM sends all events to the Events Log file, except for those sources listed in the removeFromWin section. 2—MVAM sends only the sources listed in the inserIntoWin section to the Events Log file. 3—MVAM sends all events to the Events Log file.	0
removeFrom Win	PDLCOMM	Determines whether the PDLCOMM information is excluded from the Events Log screen when integratedWindow = 1: 0=False (default) 1=True	0
insertIntoWin	PDLPRNERR	Determines whether the PDLPRNERR information is displayed in the Events Log screen when integratedWindow = 2: 0=False (default) 1=True	0

Table A-1. MVAM initialization file parameters (continued)

Section	Parameter	Description	Default Value
insertIntoWin	Gk	Determines whether the source information is displayed in the Events Log screen when integratedWindow = 2: 0=False 1=True	0 (WinNT) 1 (SPARC Solaris)
insertIntoWin	Gen	Determines whether the source information is displayed in the Events Log screen when integratedWindow = 2: 0=False 1=True (default)	1
insertIntoWin	UtText	Determines whether the source information is displayed in the Events Log screen when integratedWindow = 2: 0=False 1=True (default)	1
insertIntoWin	UtOdbc	Determines whether the source information is displayed in the Events Log screen when integratedWindow = 2: 0=False 1=True (default)	1

Table A-1. MVAM initialization file parameters (continued)

Section	Parameter	Description	Default Value
insertIntoWin	Prdb	Determines whether the source information is displayed in the Events Log screen when integratedWindow = 2: 0=False 1=True (default)	1
insertIntoWin	Gwidb	Determines whether the source information is displayed in the Events Log screen when integratedWindow = 2: 0=False 1=True (default)	1
insertIntoWin	Ras	Determines whether the source information is displayed in the Events Log screen when integratedWindow = 2: 0=False 1=True (default)	1
insertIntoWin	Ept	Determines whether the source information is displayed in the Events Log screen when integratedWindow = 2: 0=False 1=True (default)	1

Table A-1. MVAM initialization file parameters (continued)

Section	Parameter	Description	Default Value
insertIntoWin	Act	Determines whether the source information is displayed in the Events Log screen when integratedWindow = 2: 0=False 1=True (default)	1
insertIntoWin	Gwt	Determines whether the source information is displayed in the Events Log screen when integratedWindow = 2: 0=False 1=True (default)	1
insertIntoWin	Gwct	Determines whether the source information is displayed in the Events Log screen when integratedWindow = 2: 0=False 1=True (default)	1
insertIntoWin	Gui	Determines whether the source information is displayed in the Events Log screen when integratedWindow = 2: 0=False 1=True (default)	1

Table A-1. MVAM initialization file parameters (continued)

Section	Parameter	Description	Default Value
insertIntoWin	Locator	Determines whether the source information is displayed in the Events Log screen when integratedWindow = 2: 0=False 1=True (default)	1
insertIntoWin	Rt	Determines whether the source information is displayed in the Events Log screen when integratedWindow = 2: 0=False 1=True (default)	1
insertIntoWin	Odbc	Determines whether the source information is displayed in the Events Log screen when integratedWindow = 2: 0=False 1=True (default)	1
insertIntoFile	Gk	Determines whether the source information is included in the Events Log file when msgFile =2: 0=False 1=True (default)	1

Table A-1. MVAM initialization file parameters (continued)

Section	Parameter	Description	Default Value
insertIntoFile	Gen	Determines whether the source information is included in the Events Log file when msgFile =2: 0=False 1=True (default)	1
insertIntoFile	UtText	Determines whether the source information is included in the Events Log file when msgFile =2: 0=False 1=True (default)	1
insertIntoFile	UtOdbc	Determines whether the source information is included in the Events Log file when msgFile =2: 0=False 1=True (default)	1
insertIntoFile	Prdb	Determines whether the source information is included in the Events Log file when msgFile =2: 0=False 1=True (default)	1
insertIntoFile	Gwidb	Determines whether the source information is included in the Events Log file when msgFile =2: 0=False 1=True (default)	1

Table A-1. MVAM initialization file parameters (continued)

Section	Parameter	Description	Default Value
insertIntoFile	Ras	Determines whether the source information is included in the Events Log file when msgFile =2: 0=False 1=True (default)	1
insertIntoFile	Ept	Determines whether the source information is included in the Events Log file when msgFile =2: 0=False 1=True (default)	1
insertIntoFile	Act	Determines whether the source information is included in the Events Log file when msgFile =2: 0=False 1=True (default)	1
insertIntoFile	Gwt	Determines whether the source information is included in the Events Log file when msgFile =2: 0=False 1=True (default)	1
insertIntoFile	Gwct	Determines whether the source information is included in the Events Log file when msgFile =2: 0=False 1=True (default)	1

Table A-1. MVAM initialization file parameters (continued)

Section	Parameter	Description	Default Value
insertIntoFile	Gui	Determines whether the source information is included in the Events Log file when msgFile =2: 0=False 1=True (default)	1
insertIntoFile	Locator	Determines whether the source information is included in the Events Log file when msgFile =2: 0=False 1=True (default)	1
insertIntoFile	Rt	Determines whether the source information is included in the Events Log file when msgFile =2: 0=False 1=True (default)	1
insertIntoFile	Odbc	Determines whether the source information is included in the Events Log file when msgFile =2: 0=False 1=True (default)	1

a. These parameters are configured through the MVAM installation program

b. ODBC database support currently available only for MVAM running on a Windows NT system. These parameters are not configured for MVAM running on SPARC Solaris.

Upgrading the MVAM License

B

During the MultiVoice Access Manager installation process, the MultiVoice Gateway license upgrade utility is also installed on your Windows NT or SPARC Solaris system. You can user this utility to increase the number of licenses, thus support additional MultiVoice Gateways.

Before you upgrade a MultiVoice Gateway license, make sure that you have the updated product serial number for the MultiVoice Gateway license upgrade from your MultiVoice Access Manager Warranty Registration card.

Note: The serial number from the MultiVoice Access Manager Warranty Registration card is a required entry. Without it the MVAM license will not be upgraded. If you enter an incorrect serial number, the MVAM license will not be upgraded.

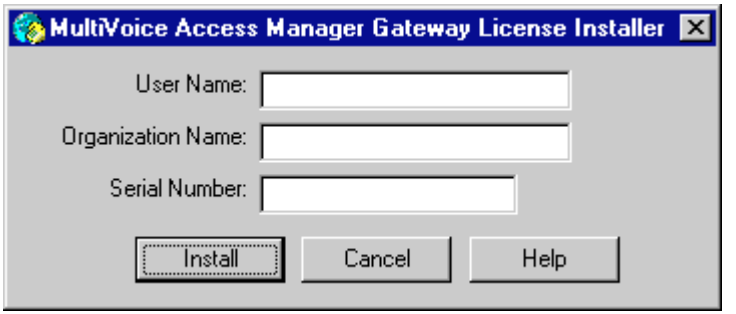
You may install the MVAM license whether or not MVAM is running, but the license upgrade is not applied until you re-start MVAM.

Window NT license upgrades

The Windows NT license upgrade utility displays a single data entry window, where users will enter updated license information.

1 From the Start Menu, select MVAM License Application.

When selected, the licensing executable file opens, and the following screen appears:

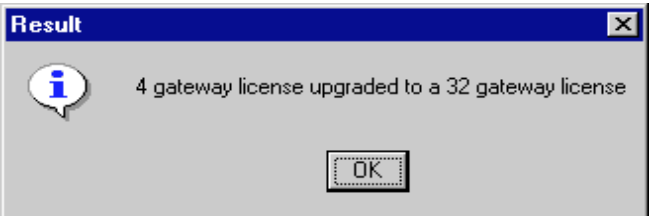


2 Enter any updated information for the User Name and Organization Name fields:

- If you enter a User Name different from the User Name you entered when you originally installed MVAM, the Installer updates MVAM with the new User Name.
- If you enter an Organization Name different from the Organization Name you entered when you originally installed MVAM, the Installer updates MVAM with the new Organization Name.

3 Enter the updated serial number printed on the MVAM Warranty Registration card.

4 Click the Install button. The MVAM License Application should display a message similar to the following:



Click OK. The license upgrade is installed.

SPARC Solaris license upgrades

The SPARC Solaris upgrade utility for MultiVoice Access Manager is the `textlicapp` program. Located in the `bin` subdirectory of the MVAM $HOME directory. This script is run from the shell prompt.

Note: The `mvam_license` script should be executed by `root`.

To perform the upgrade, use the following procedure:

1 At the shell prompt, execute `mvam_license`

You are prompted to enter the information for your installation of MultiVoice Access Manager.

```
MultiVoice Access Manager Gateway License Installer

This package will upgrade the number of MultiVoice Gate-
way licenses purchased for installation on this network.

Do you want to continue with license installation
[y,n,?]
```

2 Enter `y` and press [RETURN] to continue.

`textlicapp` prompts for the site information, including the serial number from the MVAM Warranty Registration card.

3 Enter the MVAM User Name:

```
User name:John Doe
```

If you enter a User name different from the User name you entered when you originally installed MVAM, the `mvam_license` updates MVAM with the new User name. Press [RETURN] to continue.

4 Enter an Organization Name:

```
Organization name:Generic ISP
```

If you enter an Organization name different from the Organization name you entered when you originally installed MVAM, the `textlicapp` updates the MVAM with the new Organization name. Press [RETURN] to continue.

5 Enter the Serial Number that appears on the MVAM Warranty Registration card:

```
Serial number:MVAM-200-AT-99999999
```

6 Press [RETURN] to continue. `mvam_license` continues, displaying the following message:

```
Please Wait...
```

(Be patient, this operation may take a minute.)

```
MVAM license installed successfully.
```

Warranty

C

Ascend end user agreement

The term *Software* includes all Ascend and third party (*Supplier*) software provided to you with this Ascend product, and includes any accompanying documentation (the *Documentation*). The term *Software* also includes any updates of the Software provided to you by Ascend at its option. Subject to the terms of this Agreement, Ascend grants to you, and you accept, a personal, non exclusive, and nontransferable (except as set forth below) license to use the object code version of the Software on a single computer.

The Software is *in use* on a computer when it is loaded into the temporary memory (i.e. RAM) or installed into the permanent memory (e.g. hard drive, CD-ROM, or other storage device) of that computer, except that a copy installed on a network server for the sole purpose of distribution to other computers is not *in use*. If you permanently install the Software on the hard disk or other storage device of a computer (other than a network server) and you use that computer more than 80% of the time it is in use, then you may also use the Software on a portable or home computer. You may make a reasonable number of copies of the Software and Documentation for backup or archival purposes only, so long as Ascend's and its licensors' copyright notices are reproduced on such copies.

Limitations on use

You may not copy, rent, lease, sell, sublicense, assign, loan, time-share, or otherwise transfer or distribute copies of the Software or Documentation to others, except as set forth in this agreement. You may physically transfer the Software from one computer to another, provided that you do not retain any copies of the Software, including any copies stored on a computer. You may

permanently transfer this license to another user, but only if you transfer or destroy all copies of the Software and Documentation, and the recipient agrees in writing to be bound by all of the terms of this agreement.

You agree that you will not decompile, disassemble, or otherwise reverse engineer the Software, and you will use your best efforts to prevent your employees and contractors from doing so, except to the extent that such restriction is expressly prohibited by applicable law. You may not modify, adapt, create a derivative work, merge, or translate the Software or the Documentation without the prior written consent of Ascend.

Specific Suppliers may be identified in the Documentation. You agree to any additional terms and conditions specific to particular Suppliers or Products, as described in the Documentation, which are incorporated herein by reference.

Intellectual property rights

You acknowledge that Ascend or its Suppliers retain exclusive ownership of all copyrights, trademarks, patents and/or other intellectual property rights in the Software and the Documentation. You are not granted any rights in the Software or Documentation other than the license rights expressly set forth above.

Term and termination

The term of this license is for the duration of any copyright in the Software. This license automatically terminates if you fail to comply with any of the terms and conditions of this agreement. You agree that, upon such termination, you will either destroy (or permanently erase) all copies of the Software and Documentation, or return the original Software and Documentation to Ascend. You may terminate this license at any time by destroying the Software and Documentation and any permitted copies.

Limited warranty and limited remedy

Ascend warrants to the original end user purchaser only that the Software as delivered at the time of purchase will substantially conform to the Documentation, and that the original diskettes and Documentation are free from defects in material and workmanship under normal use, for a period of ninety

(90) days from the original end user's purchase thereof (the *Limited Warranty Period*), provided the Software is used with compatible computer hardware and operating systems. This limited warranty is void if failure of the Software has resulted from accident, abuse, or misapplication.

Ascend's entire liability, and your sole and exclusive remedy shall be, at Ascend's option, either to (a) correct or help you work around or avoid a reproducible Error, (b) replace defective diskettes or Documentation or (b) authorize a refund, so long as the Software and Documentation are returned with a copy of your receipt within ninety (90) days of your date of purchase, together with a brief written statement describing the alleged Error. An *Error* is a defect in the Software that causes it not to perform substantially in accordance with the limited warranty set forth above. Any replacement Software or Documentation will be warranted for the remainder of the original warranty period only.

No liability of suppliers

You acknowledge that your rights under this Agreement, in the nature of warranty or otherwise, are solely against Ascend. NO SUPPLIER MAKES ANY WARRANTY, ASSUMES ANY LIABILITY, OR UNDERTAKES TO FURNISH TO YOU ANY SUPPORT OR INFORMATION CONCERNING PRODUCTS OR ANY PORTION OF PRODUCTS. You hereby release all Suppliers from any claims, damages or losses arising from the use of Products, regardless of the form of action.

Disclaimer of warranties

EXCEPT AS SPECIFICALLY PROVIDED ABOVE, THE SOFTWARE AND THE DOCUMENTATION IS PROVIDED *AS IS*, WITHOUT WARRANTY OF ANY KIND. ALL OTHER WARRANTIES ARE DISCLAIMED, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, OR THAT THE SOFTWARE'S FUNCTIONS WILL MEET YOUR REQUIREMENTS OR THAT ITS OPERATION WILL BE UNINTERRUPTED OR ERROR FREE. EXCEPT AS SET FORTH IN THIS AGREEMENT, THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE AND THE DOCUMENTATION IS WITH YOU. IF THEY PROVE DEFECTIVE AFTER

THEIR PURCHASE, YOU, AND NOT ASCEND OR ITS SUPPLIERS, ASSUME THE ENTIRE COST OF SERVICE OR REPAIR.

If a disclaimer of implied warranties is not permitted by law, the duration of any such implied warranty is limited to ninety (90) days from the date of purchase by the original end user purchaser. Some jurisdictions do not allow the exclusion of implied warranties or limitations on how long an implied warranty may last, so such limitations or exclusions may not apply to you. This limited warranty gives you specific legal rights, and you may also have other rights which vary from jurisdiction to jurisdiction.

Liability exclusions and limitations

IN NO EVENT SHALL ASCEND OR ANY SUPPLIER BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES OF ANY KIND (INCLUDING LOST PROFITS, LOSS OF USE, OR INTERRUPTION OF BUSINESS), OR FOR LEGAL FEES, ARISING OUT OF THE USE OF THE SOFTWARE OR THE DOCUMENTATION, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT PRODUCT LIABILITY OR OTHERWISE, EVEN IF ASCEND HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL ASCEND'S AGGREGATE LIABILITY FOR ANY CLAIM EXCEED THE LICENSE FEE PAID BY YOU. This limitation shall apply notwithstanding any failure or inability to provide the limited remedies set forth above. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the above limitation(s) or exclusion(s) may not apply to you.

Proprietary rights-contracts with certain U.S. government agencies

If the Software is acquired under the terms of a Department of Defense or civilian agency contract, the Software is *commercial item* as that term is defined at 48 C.F.R. 2.101 (Oct. 1995), consisting of *commercial computer software* and *commercial computer software documentation* as such terms are used in 48 C.F.R. 12.212 of the Federal Acquisition Regulations and its successors and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995) of the DoD FAR Supplement

and its successors. All U.S. Government end users acquire the Software and the Documentation with only those rights set forth in this agreement.

Export restrictions

You acknowledge that the laws and regulations of the United States restrict the export and re-export of certain commodities and technical data of United States origin, including the Software and the Documentation, in any medium. You agree that you will not knowingly, without prior authorization if required, export or re-export the Software or the Documentation in any medium without the appropriate United States and foreign government licenses.

Severability

You acknowledge and agree that each provision of this agreement that provides for a disclaimer of warranties or an exclusion or limitation of damages represents an express allocation of risk, and is part of the consideration of this agreement. Invalidity of any provision of this Agreement shall not affect the validity of the remaining provisions of this Agreement.

General

This Agreement is the entire agreement between you and Ascend relative to the Software and Documentation, and supersedes all prior written statements, proposals, or agreements relative to its subject matter. It may be modified only by a writing executed by an authorized representative of Ascend. No Ascend dealer or sales representative is authorized to make any modifications, extensions, or additions to this agreement. This Agreement is governed by the laws of the State of California as applied to transactions taking place wholly within California between California residents, without application of its conflicts of law principles. The United Nations Convention on Contracts for the International Sale of Goods is specifically excluded from application to this Agreement.

Questions

If you have any questions, write or call Ascend Communications, Inc., One Ascend Plaza, 1701 Harbor Bay Parkway, Alameda, CA 94502.

Index

Numerics

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X