Lucent Technologies
Bell Labs Innovations



MultiVoice Access Manager User's Guide

Part Number: 7820-0584-004
For software version 3.0.0
March 2000

Copyright (c) 1997-1999 Ascend Communications, Inc., a subsidiary of Lucent Technologies Inc. All rights reserved. Copyright (c) 2000 Lucent Technologies Inc. All rights reserved.

This material is protected by the copyright laws of the United States and other countries. It may not be reproduced, distributed, or altered in any fashion by any entity (either internal or external to Lucent Technologies), except in accordance with applicable agreements, contracts, or licensing, without the express written consent of Lucent Technologies.

Notice

Every effort was made to ensure that the information in this document was complete and accurate at the time of printing. However, information is subject to change.

Trademarks

MultiVoice Gateway, MultiVoice Access Manager, MultiVoice for the MAX and MAX are trademarks of Lucent Technologies Inc. Other trademarks and trade names mentioned in this publication belong to their respective owners.

Ordering Information

To order copies of this document, contact your Lucent Technologies representative or reseller.

Support Telephone Numbers

For a menu of support and other services, call (800) 272-3634. Or call (510) 769-6001 for an operator.

Customer Service

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

Finding information and software on the Internet

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

Visit the 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, modem, or regular mail, as well as over the Internet.

Enabling Lucent to assist you

If you need to contact Lucent 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 Lucent product.
- Type of computer you are using.
- Description of the problem.

Calling Lucent from within the United States

In the United States, you can take advantage of Priority Technical Assistance or you can call to request assistance.

Priority Technical Assistance

If you need to talk to an engineer right away, call (900) 555-2763 to reach the 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.

Other telephone numbers

For a menu of Lucent's services, call (800) 272-363. Or call (510) 769-6001 for an operator.

Calling Lucent from outside the United States

You can contact Lucent 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 the Asia Pacific Region, you can find additional support resources at `http://apac.ascend.com`

Obtaining assistance through correspondence

Lucent 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 Lucent's U.S. offices. Following are the ways in which you can reach 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 Lucent at the following address:

Attn: Customer Service
Lucent Technologies
1701 Harbor Bay Parkway
Alameda, CA 94502-3002

Contents

Customer Service iii

About This Guide xxiii

How to use this guide xxiii
What you should know xxv
Documentation conventions xxv
Related publications xxvii

Introducing MultiVoice Concepts 1-1

The Public Switched Telephone Network (PSTN) 1-1
The MultiVoice network 1-2
MultiVoice Packet processing 1-3
Supported audio codecs 1-3
H.323 implementation 1-5
Integrating PSTN and packet networks 1-5
Using primary and secondary gatekeepers 1-7
Increasing Gatekeeper reliability 1-8
Overlapping gateway coverage areas 1-13
How calls are assigned to a MultiVoice gateway 1-15
MultiVoice networks supporting multizone call routing 1-16
Routing across H.323 zones 1-17
Implementing call routing 1-17
Gatekeeper virtual zones 1-19
MultiVoice applications 1-21
Basic public long-distance service 1-22
Local 800 service 1-23
Traditional 800 service 1-24

Using MultiVoice and local 800 service 1-24
Point-to-point PBX trunk extension 1-25
PBX trunk intraflow 1-26
PC-to-Phone calls 1-27
Gateway-to-client keep-alive registration 1-28

Setting Up MultiVoice Access Manager 2-1

Before you begin 2-1
System requirements 2-2
Minimum configuration for Windows NT systems 2-2
Minimum configuration for SPARC Solaris 2.5.1 systems 2-2
Minimum configuration for HP-UX 10.20 systems 2-3
Network requirements 2-3
Web browser software 2-3
Web server software 2-3
MultiVoice Access Manager per-port licensing 2-4
Installation sequence 2-4
Installing a Web server 2-5
Installing MultiVoice Access Manager 2-5
Installation on a Windows NT 4.0 system 2-6
Installation procedure 2-6
Configuring system software 2-15
Installation on a Solaris system 2-16
Installation for boot-up operation 2-16
Installation procedure 2-17
Sample Solaris installation script for upgrading from Release 2.2.0 to MVAM Release 3.0.0 2-17
Sample Solaris installation script for MVAM Release 3.0.0 2-19
Configuring system software 2-21
Installation on an HP-UX system 2-22
Installation procedure 2-23
Sample HP-UX installation script for MVAM Release 3.0.0 2-24
Configuring system software 2-25
Starting MVAM 2-25
MVAM directory structure 2-26
MVAM configuration and control files 2-27
Launching MVAM on a Windows NT system 2-27
Changing window properties 2-28
Launching the MVAM on a SPARC Solaris system 2-29

Launching the MVAM on an HP-UX system 2-30
Opening the user interface 2-31
Stopping MVAM 2-32
Stopping MVAM on a Windows NT system 2-32
Stopping MVAM on a Solaris or HP-UX system 2-32
Uninstalling MVAM 2-33
Uninstalling MVAM from a Windows NT system 2-33
Uninstalling MVAM from a Solaris system 2-34
Uninstalling MVAM from an HP-UX system 2-35

Configuring the Access Manager 3-1

Connecting to MVAM 3-1
Connecting to a local MVAM installation 3-1
Connecting to a remote MVAM installation 3-2
About on-line help 3-4
Control buttons 3-5
Configuring MVAM options 3-5
Configuring security 3-8
Configuring PIN authentication 3-10
Configuring ANI authentication 3-10
Enabling PC-to-phone operations 3-17
Enabling PC-to-phone operations 3-18
Configuring event log generation 3-18
Configuring Registration 3-20
Enable terminal registration 3-21
Aging terminal registration 3-22
Setting keep alive registration time intervals 3-22
Setting call accounting options 3-25
Modifying dialing prefixes 3-26
Configuring Gatekeeper virtual zones 3-28
Definition of an Access Manager (Gatekeeper) virtual zone 3-28
Call routing using virtual zones 3-28
VIrtual zone call processing 3-29
Virtual zone support files 3-30
Virtual zone configuration files and parameters 3-31
Using virtual zones 3-35
Virtual zone main page (frame.htm) 3-35
Virtual zone administration 3-37

Configuring Gateway Databases 4-1

Adding Gateway records 4-4
Adding multiple gateways 4-5
Displaying and modifying a Gateway's general information 4-6
Understanding the Gateway database records 4-8
Selecting from a list of all gateways 4-9
Selecting a gateway using wildcard searches 4-11
Modifying and saving Gateway data 4-11
Displaying and modifying Gateway number translation tables 4-12
Selecting from a list of all gateways with number translation tables . 4-15
Modifying assigned number translation tables 4-16
Modifying number translation rules 4-17
Displaying and modifying coverage areas 4-18
Overlapping coverage areas 4-19
Modifying a coverage area 4-19
Adding an Inclusion Area 4-22
Removing an Inclusion Area 4-23
Viewing modified coverage areas 4-25
Coverage area size 4-25
Coverage area display 4-25
Removing a Gateway 4-26
Removing multiple gateways 4-27

Configuring Logical Gateways 5-1

How MLG and ADMA Rules Work 5-2
ADMA Rules 5-4
Adding an ADMA Rule 5-6
Saving the settings 5-9
Displaying and modifying ADMA Rules 5-9
Selecting from a list of all ADMA Rules 5-11
Selecting an ADMA Rule using wildcard searches 5-13
Removing an ADMA Rule 5-13
ADMA Rule Sets 5-15
Adding an ADMA Rule Set 5-16
Saving the settings 5-18
Displaying and modifying ADMA Rule Sets 5-18
Selecting from a list of all ADMA Rule Sets 5-19
Selecting an ADMA Rule Set using wildcard searches 5-22

Removing an ADMA Rule Set 5-22
ADMA Gateway/Trunk Rules 5-24
Adding an ADMA Gateway/Trunk Rule 5-26
Saving the settings 5-28
Displaying and modifying ADMA Gateway/Trunk Rules 5-29
Selecting from a list of all ADMA Gateway/Trunk Rules 5-31
Selecting an ADMA Gateway/Trunk Rule using wildcard searches 5-34
Removing an ADMA Gateway/Trunk Rule 5-34

Peer Gatekeeper Administration 6-1

Gatekeeper-to-Gatekeeper communications 6-1
Definition of an H.323 zone 6-2
Definition of an Access Manager (Gatekeeper) virtual zone 6-2
Adding a Gatekeeper 6-4
Saving the settings 6-6
Understanding Gatekeeper databases 6-6
Gatekeeper table 6-7
Gatekeeper coverage table 6-8
Displaying and modifying Gatekeeper information 6-8
Selecting from a list of all gatekeepers 6-10
Selecting a gatekeeper using wildcard searches 6-13
Displaying and modifying Gatekeeper coverage areas 6-13
Selecting from a list of all Gatekeeper coverage areas 6-14
Adding an Inclusion Area 6-17
Removing an Inclusion Area 6-18
Viewing modified coverage areas 6-19
Removing a Gatekeeper 6-19
Removing multiple gatekeepers 6-21

Terminal Administration 7-1

Adding a Terminal 7-3
Understanding Terminal databases 7-5
Displaying and modifying Terminal information 7-6
Removing a Terminal 7-11

Using Number Translations 8-1

Digit stripping and number translations 8-1
Number translation processing 8-2
Number translation table administration 8-2
Number Translation Administration page 8-3
Adding Number Translation Tables 8-4
Adding multiple number translation tables 8-6
Understanding number translation databases 8-7
Number translation table list 8-7
Number translation tables 8-8
Displaying and modifying a Number Translation Table 8-9
Selecting from a list of all translation tables 8-12
Removing translation rules 8-14
Re-ordering translation rules 8-14
Remove a Number Translation Table 8-15
Removing an active Number Translation table 8-15
Removing multiple number translation tables 8-16
Using number translations with terminals 8-19

Configuring MultiVoice Users 9-1

Adding user records 9-3
Understanding the user database records 9-5
Displaying and modifying user information 9-6
Selecting from a list of all users 9-7
Selecting a user using wildcard searches 9-10
Modifying user PINs 9-10
Removing user records 9-11
Removing multiple users 9-12

MultiVoice Administration 10-1

Setting Gateway-to-Gatekeeper registration policy 10-1
Identifying Gateways and Gatekeepers 10-2
Setting Gateway-to-Gatekeeper registration policy 10-2
Managing registration grace periods 10-3
Retrieving MultiVoice statuses 10-3
Gateway Status 10-4
Terminal status 10-7
Active call status 10-7
Testing call routes 10-9

Translator/router tool 10-9
Calling thru a Gateway 10-12
Calling from a Terminal 10-13
Viewing log files 10-14
Event log 10-15
Call log files 10-16
Displaying MVAM version 10-25
License Administration 10-26
Adding upgrade serial numbers 10-27
Displaying installed license(s) 10-29
Removing upgrade serial numbers 10-30
Supported Gateways and Terminals 10-33

Troubleshooting 11-1

Ensure the MultiVoice environment is set up correctly 11-1
Possible problems and solutions 11-3
The Web browser wants to download mvam_cgi.exe 11-3
MVAM is started, but nothing appears in the interface 11-3
MVAM doesn't create an event log 11-4
Callers dial destination correctly, but nothing happens 11-5
Callers dial destination, hear tick-tock sound, but nothing happens .. 11-6
Callers hear a fast busy tone after dialing, using single-stage dialing 11-6
MVAM does not register a correctly configured gateway 11-7
You cannot connect to the MVAM from the Web browser 11-8
Error messages 11-8
Couldn't read license. 11-8
The Gatekeeper application is not running 11-9
There are no registered gateways 11-9
There are no active calls 11-10
No calls have been made 11-10
There isn't a gateway covering the specified number 11-10
"Gateway Name" is not unique 11-10
The specified gateway is not administered 11-11
The specified user is unknown 11-11
"User Alias" is not unique 11-11
Additional troubleshooting resources 11-11
Event logs 11-11
Troubleshooting MultiVoice Gateway registration 11-13
Troubleshooting call establishment 11-14

MVAM interface screen 11-24
Viewing real-time information 11-24

MVAM Initialization File A-1

MVAM Licenses B-1

Per-port licensing B-1
MultiVoice Access Manager serial numbers B-1
License Packs/Upgrade serial numbers B-2
Window NT license installation B-3
Solaris and HP-UX license installation B-4
Gatekeeper-to-gatekeeper communications and MVAM licenses B-5

Legal Notices C-1

End User License Agreement C-1
Lucent Technologies InterNetworking Systems Global Warranty C-6

Index Index-1

Figures

Figure 1-1 Example of call routing over circuit-switched PSTN 1-2
Figure 1-2 MultiVoice packet format 1-3
Figure 1-3 Example of a MultiVoice network 1-6
Figure 1-4 Example of a MultiVoice network with a secondary gatekeeper 1-8
Figure 1-5 Redundant gatekeepers 1-9
Figure 1-6 Reciprocal secondary gatekeepers 1-10
Figure 1-7 Global secondary gatekeeper 1-11
Figure 1-8 Example of a MultiVoice network with overlapping coverage areas 1-14
Figure 1-9 Example of a MultiVoice network supporting multizone call routing 1-18
Figure 1-10 Example of a MultiVoice network using gatekeeper virtual zones 1-21
Figure 1-11 Example of an ISP offering data and voice services 1-23
Figure 1-12 Traditional 800 environment 1-24
Figure 1-13 Using MultiVoice and local 800 service 1-25
Figure 1-14 Connecting two sites by MultiVoice and a leased connection 1-26
Figure 1-15 Alternative voice-traffic paths between sites 1-27
Figure 1-16 Virtual private network using PC telephony 1-28
Figure 2-1 MultiVoice Access Manager Welcome message 2-7
Figure 2-2 Software License Agreement screen 2-8
Figure 2-3 Initial pre-installation instructions screen 2-8
Figure 2-4 Subsequent pre-installation instructions screen (second) 2-9
Figure 2-5 Subsequent pre-installation instructions screen (last) 2-9
Figure 2-6 Destination Location screen 2-10
Figure 2-7 Setup Type screen 2-11
Figure 2-8 Start Copying Files screen 2-13
Figure 2-9 License Installer dialog box 2-13
Figure 2-10 Successful Installation of MVAM message 2-14

Figure 3-1 Access Manager main screen (default) 3-3
Figure 3-2 Access Manager virtual zone main screen 3-4
Figure 3-3 MultiVoice Access Manager Options menu 3-6
Figure 3-4 MultiVoice Access Manager Security Options form 3-9
Figure 3-5 Event File Options screen 3-19
Figure 3-6 Registration Options form 3-20
Figure 3-7 Call Accounting Options form 3-25
Figure 3-8 Modify Dialing Prefixes form 3-26
Figure 3-9 Virtual zone main page 3-36
Figure 3-10 Virtual Zone Administration page 3-38
Figure 3-11 Select a Virtual Zone page 3-39
Figure 3-12 Virtual Zone Administration page for selected virtual zone .. 3-40
Figure 3-13 Add a Virtual Zone page 3-41
Figure 3-14 Successful addition of Virtual Zone 3-42
Figure 3-15 Display/Modify Virtual Zones page 3-43
Figure 3-16 Select a virtual zone to modify 3-44
Figure 3-17 Modify a Virtual Zone page 3-45
Figure 3-18 Remove a Virtual Zone page 3-46
Figure 3-19 Removal Confirmation of a virtual zone 3-46
Figure 3-20 Successful removal of a virtual zone 3-47
Figure 4-1 Gateway Administration page 4-2
Figure 4-2 Add a Gateway page 4-4
Figure 4-3 Adding multiple Gateways 4-5
Figure 4-4 Successful addition of Gateways 4-6
Figure 4-5 Display/Modify a Gateway's General Information page 4-7
Figure 4-6 Select a gateway to modify page 4-9
Figure 4-7 Modify a Gateway's General Information page 4-10
Figure 4-8 Modified Gateway page 4-11
Figure 4-9 Display/Modify a Gateway's Number Translations page 4-13
Figure 4-10 Modify a Gateway Number Translation Tables page 4-14
Figure 4-11 Display/Modify a Gateway's Number Translations page 4-16
Figure 4-12 Modified Number Translation confirmation page 4-17
Figure 4-13 Modify the Number Translation Table page 4-18
Figure 4-14 Display/Modify a Gateway's Coverage Area page 4-20
Figure 4-15 Modify Coverage Area for a Gateway page 4-21
Figure 4-16 Select a gateway to modify page 4-22
Figure 4-17 Modified Coverage Area confirmation page 4-23
Figure 4-18 Confirm removal of Inclusion Area 4-24
Figure 4-19 Successful removal of Inclusion Area 4-24

Figure 4-20 Remove a Gateway page 4-26
Figure 4-21 Removing multiple Gateways..... 4-27
Figure 4-22 Confirm removal of Gateways..... 4-28
Figure 4-23 Successful removal of Gateways 4-29
Figure 5-1 Logical Gateway Administration page 5-4
Figure 5-2 ADMA Rule Administration page..... 5-5
Figure 5-3 Add an ADMA Rule page 5-6
Figure 5-4 Display/Modify an ADMA Rule page..... 5-10
Figure 5-5 Select an ADMA Rule to modify page..... 5-11
Figure 5-6 Modify an ADMA Rule page 5-12
Figure 5-7 Modified ADMA Rules page..... 5-13
Figure 5-8 Remove an ADMA Rule page..... 5-14
Figure 5-9 ADMA Rule Set Administration page..... 5-15
Figure 5-10 Add an ADMA Rule Set page 5-17
Figure 5-11 Display/Modify an ADMA Rule Sets page 5-19
Figure 5-12 Select an ADMA Rule Set to modify page..... 5-20
Figure 5-13 Modify an ADMA Rule Set page 5-21
Figure 5-14 Modified ADMA Rule Sets page 5-22
Figure 5-15 Remove an ADMA Rule Set page..... 5-23
Figure 5-16 ADMA Gateway/Trunk Rule Administration page..... 5-25
Figure 5-17 Addition of ADMA Gateway/Trunk Rule Confirmed..... 5-29
Figure 5-18 Display/Modify an ADMA Gateway/Trunk Rule page..... 5-30
Figure 5-19 Select an ADMA Gateway/Trunk Rule to modify page..... 5-32
Figure 5-20 Modify an ADMA Gateway/Trunk Rule page 5-33
Figure 5-21 Modified ADMA Gateway/Trunk Rules page 5-34
Figure 5-22 Remove an ADMA Gateway/Trunk Rule page..... 5-35
Figure 5-23 Verification to Remove an ADMA Gateway/Trunk Rule..... 5-37
Figure 5-24 Removal of ADMA Gateway/Trunk Rule Confirmed 5-38
Figure 6-1 Gatekeeper Administration page 6-3
Figure 6-2 Add a Gatekeeper page..... 6-5
Figure 6-3 Successful addition of Gatekeeper..... 6-6
Figure 6-4 Display/Modify a Gatekeeper's General Information page..... 6-9
Figure 6-5 Select a Gatekeeper to modify page 6-11
Figure 6-6 Modify a Gatekeeper's General Information page 6-12
Figure 6-7 Modified Gatekeeper page..... 6-13
Figure 6-8 Display/Modify a Gatekeeper's Coverage Area page 6-14
Figure 6-9 Select a Gatekeeper to modify page 6-15
Figure 6-10 Modify Coverage Area for a Gatekeeper page..... 6-16
Figure 6-11 Modified Coverage Area configuration page 6-17

Figure 6-12 Confirm removal of Inclusion Area 6-18
Figure 6-13 Successful removal of Inclusion Area 6-19
Figure 6-14 Remove a Gatekeeper page 6-20
Figure 6-15 Removing multiple gatekeepers 6-21
Figure 6-16 Verify removal of gatekeepers 6-22
Figure 6-17 Successful removal of gatekeepers 6-22
Figure 7-1 Terminal Administration Page 7-2
Figure 7-2 Add a Terminal page 7-4
Figure 7-3 Successful addition of Terminal 7-5
Figure 7-4 Display/Modify a Terminal's General Information page 7-7
Figure 7-5 Modify a Terminal's General Information page 7-9
Figure 7-6 Modified Terminal page 7-10
Figure 7-7 Remove a Terminal page 7-11
Figure 7-8 Removing multiple terminals 7-12
Figure 7-9 Verify removal of terminals 7-13
Figure 7-10 Successful removal of terminals 7-13
Figure 8-1 Number Translations Administration page 8-3
Figure 8-2 Add a Number Translation Table page 8-5
Figure 8-3 Adding multiple Number Translation tables 8-6
Figure 8-4 Successful addition of Number Translation tables 8-7
Figure 8-5 Modify a Number Translation Table selection screen 8-10
Figure 8-6 Modify the Number Translation Table screen 8-11
Figure 8-7 Select a number translation table to modify page 8-13
Figure 8-8 Modify the Number Translation Table confirmation page 8-14
Figure 8-9 Remove a Number Translation Table 8-15
Figure 8-10 Removing multiple Number Translation tables 8-17
Figure 8-11 Verify removal of Number Translation tables 8-18
Figure 8-12 Successful removal of Number Translation tables 8-19
Figure 8-13 Modify the Terminal Ingress Translation Table page 8-20
Figure 9-1 User Administration page 9-2
Figure 9-2 Add a User page 9-3
Figure 9-3 User Add confirmation page 9-4
Figure 9-4 Display/Modify a User page 9-7
Figure 9-5 Select a user to modify page 9-8
Figure 9-6 Modify a User page 9-9
Figure 9-7 Modified User page 9-10
Figure 9-8 Remove a User page 9-11
Figure 9-9 Removing multiple users 9-13
Figure 9-10 Verify removal of users 9-14

Figure 9-11 Successful removal of users..... 9-14
Figure 10-1 Gateway Status selection page..... 10-4
Figure 10-2 All gateways status report..... 10-6
Figure 10-3 Active call log..... 10-8
Figure 10-4 Number Translator/Call Router page..... 10-10
Figure 10-5 Calling thru a Gateway options 10-12
Figure 10-6 Calling from a Terminal options..... 10-14
Figure 10-7 MultiVoice Access Manager Event Log..... 10-15
Figure 10-8 Software Version Information page..... 10-25
Figure 10-9 License Administration page 10-26
Figure 10-10 Add an Upgrade Serial Number page..... 10-28
Figure 10-11 Upgrade serial number added 10-29
Figure 10-12 Display Installed License(s) page..... 10-30
Figure 10-13 Remove an Upgrade Serial Number page 10-31
Figure 10-14 Confirm removal of upgrade serial number..... 10-32
Figure 10-15 Upgrade serial number removed..... 10-32
Figure 11-1 Access Manager Event Log page 11-12
Figure 11-2 Access Manager Interface screen 11-24

Tables

Table A-1 MVAM initialization file parameters..... A-2

About This Guide

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

Note: Due to significant new features and enhancements in MVAM Release 3.0.0, this release is not compatible with Gateways running MultiVoice Release 7.0.0 or earlier. In order to properly utilize this latest release of the MVAM software, all MultiVoice Gateways must be updated to Release 7.2.3 or later, for the MAX 6000, MAX 2000, and MAX 1800, or to release 7.0V8 or later, for the MAX TNT. We recommend all Gateways are upgraded before running MVAM Release 3.0.0.

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 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, and security on the MVAM.
- Chapter 4, “Configuring Gateway Databases,”describes how to create and manage Gateway information for a MultiVoice network. This includes

creating, modifying, and deleting Gateways, their associated number translation tables, and coverage areas.

- Chapter 5, “Configuring Logical Gateways,”describes how to create and manage Logical Gateways in a MultiVoice network to allow each incoming call to a VoIP Gateway to have its own set of configuration parameters. This includes creating, modifying, and deleting ADMA Rules, Rule Sets, and Gateway/Trunk Rules.
- Chapter 6, “Peer Gatekeeper Administration,” describes how to create and manage peer Gatekeeper information on the current Gatekeeper. This includes creating, modifying, and deleting peer Gatekeepers and their associated coverage areas.
- Chapter 7, “Terminal Administration,”describes how to create and manage PC terminal information for a MultiVoice network. This includes creating, modifying, and deleting terminals and their associated number translation tables.
- Chapter 8, “Using Number Translations,” describes how to create and manage ingress (inbound) and egress (outbound) number translation tables used for call processing. This includes creating, modifying, and deleting tables and translation rules.
- Chapter 9, “Configuring MultiVoice Users,” describes how to create and manage user information for a MultiVoice network. This includes creating, modifying, and deleting user records, assigning and modifying personal identification numbers, aliases, and telephone information.
- Chapter 10, “MultiVoice Administration,” discusses monitoring and log information. This chapter also explains how to locate MultiVoice Gateways for callers, and how to display the MVAM version and license information.
- Chapter 11, “Troubleshooting,” presents common problems, error messages, and troubleshooting tips.
- Appendix A, “MVAM Initialization File,” lists the possible values, and default values, for each parameter in the MultiVoice Access Manager Initialization file.
- Appendix B, “MVAM Licenses,”describes how to install and upgrade an MVAM license.
- Appendix C, “Legal Notices,”discusses end user license information warranty information.

This 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.
Italics	Represent variable information. Do not enter the words themselves in the command. Enter the information they represent. In ordinary text, italics are used for titles of publications, for some terms that would otherwise be in quotation marks, and to show emphasis.
[ ]	Square brackets indicate an optional argument you might add to a command. To include such an argument, type only the information inside the brackets. Do not type the brackets unless they appear in bold type.
|	Separates command choices that are mutually exclusive.
>	Points to the next level in the path to a parameter or menu item. The item that follows the angle bracket is one of the options that appears when you select the item that precedes the angle bracket.

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

Related publications

This guide does not provide a detailed explanation of products, architectures, or standards developed by other companies or organizations. Following are some related publications, 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*, Lucent Technologies

The following MultiVoice Access Manager applications notes are available at http://www.ascend.com:

- *MultiVoice Access Manager Web server configuration Application Note*
- *MultiVoice Access Manager ODBC database configuration Application Note*
- *MultiVoice Access Manager-AllBill billing system integration Application Note*
- *MultiVoice Access Manager-MIND/cti billing system integration Application Note*

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. Lucent Technologies does not maintain the sites, and cannot guarantee their availability in the future.

Introducing MultiVoice Concepts

1

The Public Switched Telephone Network (PSTN). 1-1

The MultiVoice network. 1-2

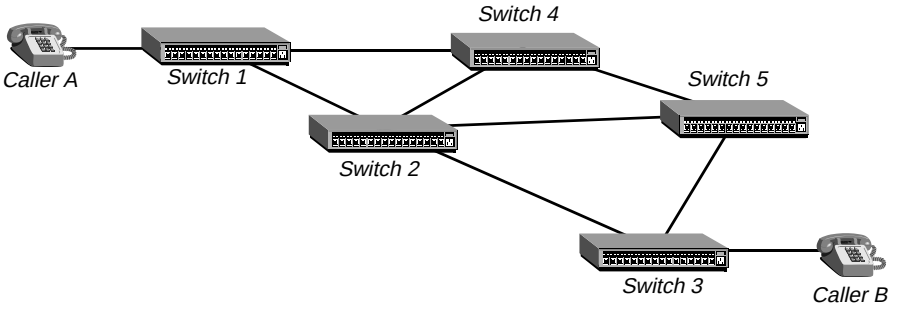
MultiVoice applications 1-21

The Public Switched Telephone Network (PSTN)

Traditionally, real-time voice information is sent over the Public Switched Telephone Network (PSTN). Circuit-switched technology provides every call with dedicated bandwidth, usually 64 Kbps. 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 that 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, voice traffic can be transmitted across IP networks.

The MultiVoice network

MultiVoice is compliant with International Telecommunications Union Telecommunication Standardization sector standard (ITU-T) H.323 for transmitting voice telephone calls across IP networks. The H.323 standard defines a framework for the transmission of real-time voice communications across IP networks. MultiVoice on the MultiVoice Gateway also supports integration with SS7 networks by means of IP Device Control (IPDC), a media

gateway control protocol, to provide call control for Voice over IP calls originating from SS7 networks.

MultiVoice Packet processing

MultiVoice voice and data are processed using User Datagram Protocol (UDP) packets. UDP is a protocol within the TCP/IP protocol suite that is used in place of TCP for processing real-time audio and video traffic. UDP is used with Real-time Transport Protocol (RTP) to provide a reliable delivery, packet sequence checking and error notification for MultiVoice call processing.

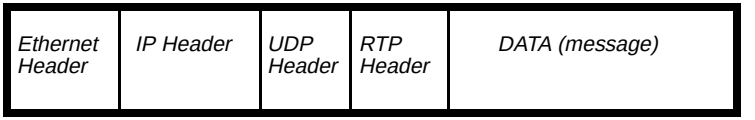
VoIP call data is compressed into frames assembled inside RTP packets. Each RTP packet rides on top of a UDP packet, and includes timestamping and synchronization information in its header for proper reassembly of the voice frames at the receiving end.

In a UDP/IP stack, the RTP header is created first and then the packet is moved down the stack to UDP and IP. UDP hands over these packets to the IP protocol layer along with the IP address of the destination node.

IP supplies the target address information of the default gateway to the Ethernet layer which establishes the data link between the two MultiVoice Gateways, which provides the connection between the packet network and the PSTN.

Figure 1-2 illustrates how each MultiVoice packet is formatted for transmission across the packet network.

Figure 1-2. MultiVoice packet format



Supported audio codecs

MultiVoice provides support for the following audio compression/decompression algorithms (codecs) as defined by the International Telecommunications Union

Telecommunications sector standards (Series G) for telephonic audio transmission:

Audio Codec	Description
G.711	This algorithm is designed to transmit and receive A Law and U Law pulse code modulation (PCM) voice at digital bits rates of 48, 56 and 64 Kbps. It is used for digital telephone sets on digital PBXs and ISDN channels. Support is required by the H.323 standard. MultiVoice supports both G.711 A Law and G.711 U Law.
G.723.1	This algorithm is designed to perform speech compression/decompression using a low bit rate, 5.3 Kbps or 6.5 Kbps output quality. This codec is designed specifically for voice/video transmission over low bit rate links (<56 Kbps). MultiVoice supports this codec at both bit rates.
G.728	This algorithm is designed to perform speech compression/decompression at 16 Kbps using low-delay code excited linear predictive methods, with a frame size of 2.5 milliseconds. MultiVoice implements this codec using a frame size of 5 milliseconds. It uses the same bitstream as outlined in the ITU-T standard, allowing speech processed by a MultiVoice Gateway to be processed by any other gateway that supports the G.728 standard.
G.729(A)	This is a Conjugate Structure, Algebraic Code Excited Linear Predictive (CS-ACELP) algorithm used for compression/decompression of speech at 8 Kbps, as defined by the ITU-T Standard G.729, with Annex A. This codec is supported by inter alia, AT&T, France Telecom and Japan's NTT.
RT-24	This is a Lucent Proprietary algorithm designed to compress speech samples from 64Kbps pulse code modulation (PCM) to 2.4Kbps, reducing the effective bandwidth required for transmission across the IP network. It uses a 22.5 millisecond audio frame, and encapsulates audio at 8 bytes per frame. The decoder produces 180 samples of audio from the 8-byte encoder output.

H.323 implementation

MultiVoice implements the H.323 standards defined for both gateways and gatekeepers. gateways connect the PSTN to the IP-based network. Callers dial a MultiVoice 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. The MultiVoice Access Manager (MVAM) performs the gatekeeper functions for a MultiVoice network.

Supporting the H.323 direct call model for Voice over IP networks, MultiVoice implementation includes:

- Integrating PSTN and packet networks to complete calls
- Using primary and secondary gatekeepers
- Using overlapping gateway coverage areas.

Integrating PSTN and packet networks

A MultiVoice network integrates both the PSTN and packet networks. Two gateways connect Caller A to Caller B. A computer running MVAM is the gatekeeper.

In Figure 1-3, when Caller A dials Caller B, the following events occur:

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

2 Gateway 1 establishes a session with the Gatekeeper.

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

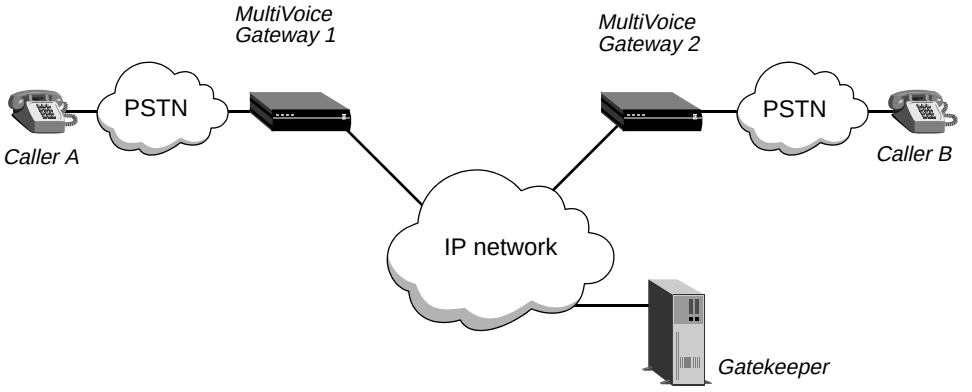
4 The Gatekeeper authenticates Caller A and, if successful, forwards the IP address of Gateway 2 to Gateway 1.

5 Gateway 1 establishes a session with Gateway 2.

6 Gateway 2 forwards the call request to Caller B.

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

Figure 1-3. Example of a MultiVoice network



If the callers in Figure 1-3 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 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. The coverage area consists of a group of telephone numbers that may dial and receive calls through a particular gateway. Coverage areas for each 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, to a database on the gatekeeper.

Inclusion areas

Individually, each of the telephone numbers and dial strings assigned to a coverage area represent individual *inclusion areas*. Together, these inclusion areas represent the coverage area for a MultiVoice Gateway. For example, an inclusion area could be specified by the partial telephone number *1732*. This

number is composed of a country code of *1* and area code of *732*. A gateway with this inclusion area would cover all telephone numbers within the 732 area code.

Using primary and secondary gatekeepers

Figure 1-4 shows an example of a MultiVoice network that uses primary and secondary gatekeepers to manage VoIP network operations. The VoIP network configuration in Figure 1-4 is designed to provide the MultiVoice network with redundant call-management capability.

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 gateway.

As illustrated in Figure 1-4, two MultiVoice gateways can connect Caller A to Caller B. Either of the systems running MultiVoice Access Manager can be the gatekeeper.

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

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

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

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

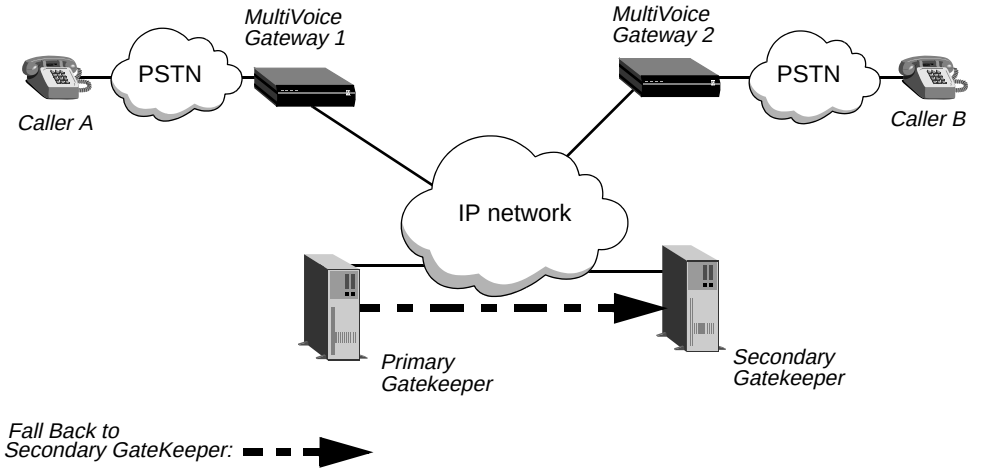
3 When registration is established with the Secondary Gatekeeper, Gateway 1 forwards the phone number and PIN authentication to the Secondary Gatekeeper.

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

5 Gateway 1 establishes a session with Gateway 2.

6 Gateway 2 forwards the call request to Caller B.

Figure 1-4. Example of a MultiVoice network with a secondary gatekeeper



The primary and secondary gatekeepers are separate computer systems, each with a unique network identity, each running its own copy of the MultiVoice Access Manager application, and functioning independently of each other. Each gatekeeper has unique gateway and user databases, and each maintains separate call and activity logs. To ensure coverage, the two gatekeepers must:

- Have duplicate gateway and user information
- Be administered using the same time
- Be synchronized using some third party clock synchronization mechanism (i.e., NTP).

The secondary gatekeeper does not report call activity to, nor share call records with the primary gatekeeper. Therefore, if a third-party billing system is used with MultiVoice, all the gatekeepers on the network must communicate with that billing system server.

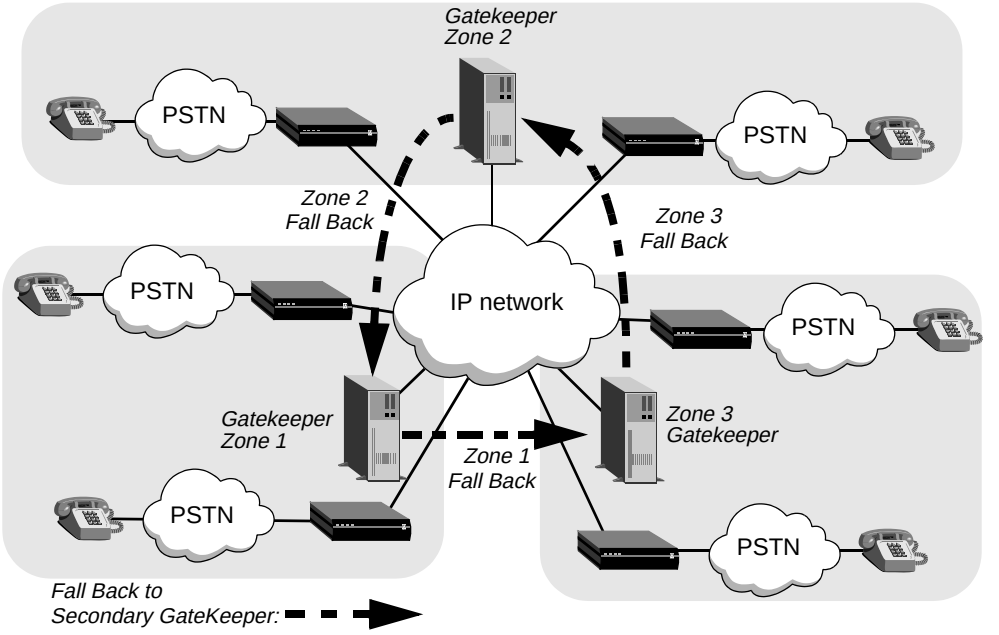
Increasing Gatekeeper reliability

The ITU-T H.323 standard defines a zone as a group of gateways that register with and are administered by a single gatekeeper. Calls may be routed by the gatekeeper directly between any pair of gateways in the same zone.

To maximize gatekeeper reliability, and reliability of a MultiVoice network, multiple MultiVoice Access Manager systems, each servicing its own H.323 zone, may be configured as redundant gatekeepers. This is called *sparing*.

Figure 1-5 illustrates a MultiVoice network where MVAM systems perform both primary and secondary gatekeeper functions. Each MVAM is the primary gatekeeper for its selected zone and also serves as the secondary gatekeeper for an adjoining zone. If the MultiVoice gateways in Zone 1 fail to register with the MVAM in that Zone 1, these gateways will attempt to register with the MVAM in Zone 3. Likewise, if the gateways in Zone 3 fail to register with their primary gatekeeper, those gateways attempt to register with the MVAM in Zone 2. In this configuration, each gatekeeper maintains duplicate gateway and user information for only one other gatekeeper's zone.

Figure 1-5. Redundant gatekeepers



In Figure 1-6, MVAM systems in a MultiVoice network are paired for use as reciprocal secondary gatekeepers. Each MVAM serves as both primary gatekeepers for their selected zones and as secondary gatekeepers for adjoining

zones. If a MultiVoice gateway in Zone 1 fails to register with the MVAM in that zone, that gateway attempts to register with its paired MVAM in Zone 2. Likewise, if a gateway in Zone 2 fails to register with its primary Gatekeeper, that gateway attempts to register with its paired MVAM in Zone 1. In this configuration, each gatekeeper maintains duplicate gateway and user information for the reciprocating gatekeeper's zone.

Figure 1-6. Reciprocal secondary gatekeepers

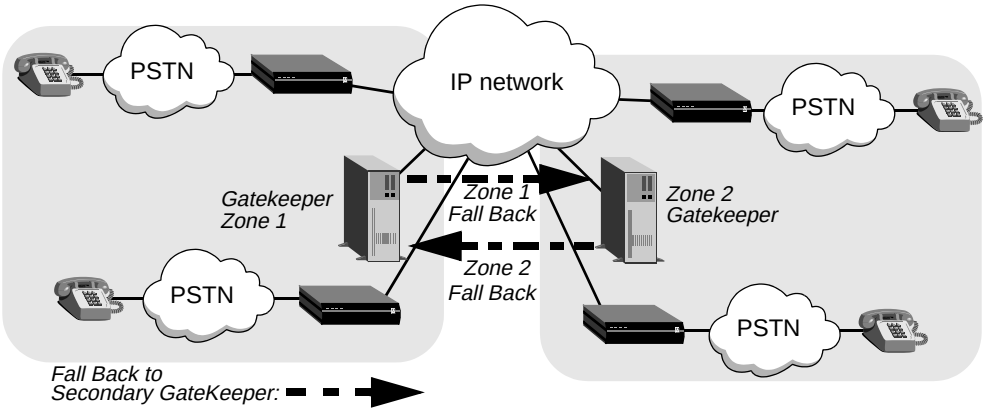
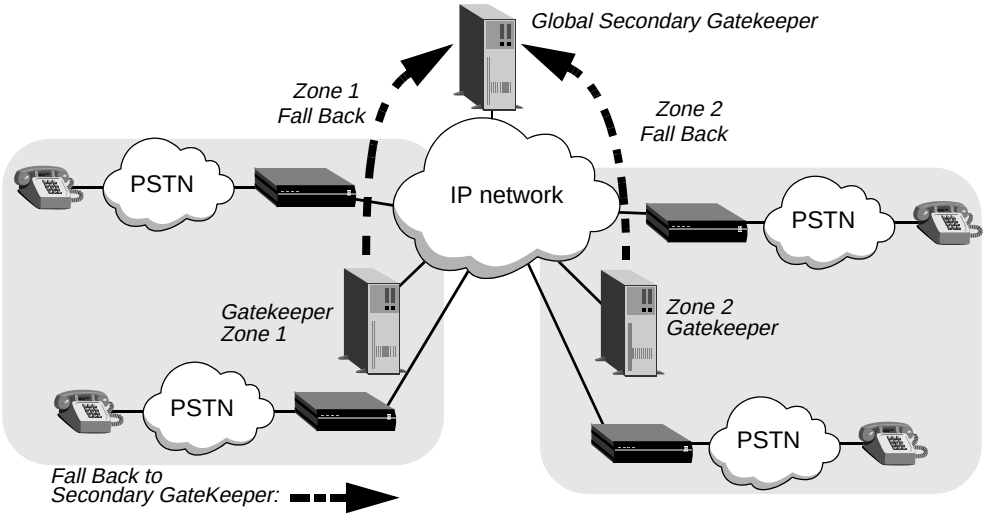


Figure 1-7 illustrates how a MultiVoice network may be configured to use a single MVAM as the secondary gatekeeper for the entire network. If any MultiVoice Gateway fails to register with its primary gatekeeper, the gateway attempts to register with the MVAM performing the global gatekeeper function. The MVAM which performs the global gatekeeper function maintains duplicate

gateway and user information for all other gatekeeper zones in the MultiVoice network.

Figure 1-7. Global secondary gatekeeper



Keep-alive registration

Once registered with a gatekeeper, a MultiVoice Gateway must periodically reregister. This is called *keep-alive registration*. Keep-alive registration is used to inform the gatekeeper that a gateway is available to accept calls. By default, a MultiVoice Gateway attempts keep-alive registration with its primary gatekeeper every 120 seconds. At registration time, the gateway will make up to five registration attempts, at 5-second intervals, until successfully contacting the gatekeeper.

When keep-alive registration fails, the MultiVoice Gateway does one of the following, if:

- A valid IP address (non-null) is configured for the Gatekeeper-Ip-Sec parameter, the gateway attempts to register with its secondary gatekeeper. Once registration is accomplished, the gateway implements the same keep-alive registration policy with the secondary gatekeeper as it did with its primary gatekeeper.

- No valid IP address is configured for the Gatekeeper-Ip-Sec parameter, the gateway goes into a *slow poll mode* with the primary gatekeeper. In this mode the gateway attempts to register with its primary gatekeeper at 30-second intervals, until successfully contacting the 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.

Reregistration with a primary gatekeeper

Once the MultiVoice Gateway registers with the secondary gatekeeper, the gateway periodically attempts to reregister with its primary gatekeeper. By default, the gateway makes one attempt to reregister with its primary gatekeeper after every five successful keep-alive registrations with the secondary gatekeeper. At that time, the gateway will make up to five registration attempts, at 5-second intervals, until successfully contacting its primary gatekeeper. If the MultiVoice Gateway cannot register with its primary gatekeeper, the gateway continues to perform keep-alive registration with its secondary gatekeeper.

Gatekeeper registration policy

Gatekeeper registration policy is set on both the MultiVoice Access Manager and MultiVoice Gateway. The MultiVoice Access Manager uses the registrationDuration parameter to set the interval at which a MultiVoice Gateway must perform keep-alive registration. This parameter defaults to 150 seconds, adding a 30-second buffer to the reregistration interval.

The MultiVoice Gateway uses the following parameters in the voip { 0 0 } profile to control gatekeeper registration:

Parameter	Description
Gatekeeper-Ip-Sec	The IP address of the gateway's secondary gatekeeper.
Gatekeeper-Keepalive	The time interval at which a gateway performs keep-alive registration with a gatekeeper.

Parameter	Description
Registration-Retries	The number of registration attempts a gateway performs during keep-alive registration, until successfully contacting the gatekeeper or failing.
Registration-Retry-Timer	The time interval between each registration attempt a gateway performs during keep-alive registration.
Primary-Retries	The interval at which a gateway attempts reregistration with its primary gatekeeper. This value represents a cycle of successful keep-alive registrations with the secondary gatekeeper.

Overlapping gateway coverage areas

In a MultiVoice network with overlapping gateway coverage areas, two or more gateways can process incoming calls to telephone numbers in the same coverage area. 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 gateways, creating overlapping coverage areas.

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 gateways.

Figure 1-8 illustrates a MultiVoice network with overlapping coverage areas. Two gateways provide coverage to area code 516. A system running MultiVoice Access Manager is the gatekeeper. 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 Gateway 1, and enters his or her PIN authentication (if required) and Caller D's phone number.

2 Gateway 1 establishes a session with the Gatekeeper.

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

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

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

6 Gateway 1 establishes a session with Gateway 2.

7 Gateway 2 forwards the call request to Caller D.

8 Now, Caller C dials Gateway 1, and enters his or her PIN authentication (if required) and Caller B's phone number.

9 Gateway 1 establishes a session with the Gatekeeper.

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

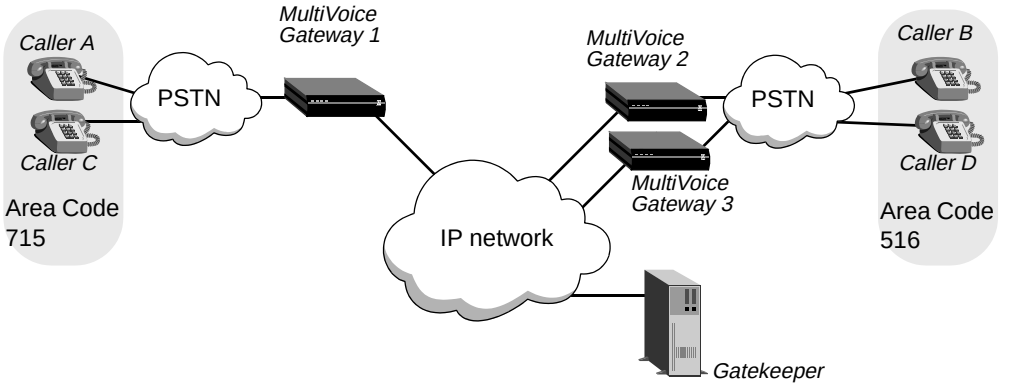
11 The Gatekeeper attempts to authenticate Caller C and, if successful, identifies the MultiVoice gateways that support the coverage area for Caller B's phone number.

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

13 Gateway 1 establishes a session with Gateway 3.

14 Gateway 3 forwards the call request to Caller B.

Figure 1-8. Example of a MultiVoice network with overlapping coverage areas



Since MultiVoice uses one port per call, the gatekeeper attempts to assign calls to each gateway based upon port availability, alternating call assignments between covering gateways.

In Figure 1-8, the Gatekeeper, having already routed a call from Caller A to Caller D through Gateway 2, determines that the call from Caller C to Caller B should be routed through Gateway 3 instead of Gateway 2 to keep the call volume balanced.

How calls are assigned to a MultiVoice gateway

When a call request is received from a gateway, the MVAM first identifies all the gateways which could be used to complete the call. The MVAM may connect calls by selecting a gateway based on the following:

- The available port capacity of each gateway,
- The current call volume of each gateway.

The selection method is controlled by parameters contained in the MVAM initialization file. See Appendix A, “MVAM Initialization File” for a detailed explanation of these parameters.

Assigning calls based on port capacity

The MultiVoice Access Manager assigns calls based on the available gateway port capacity when configured to do so. As call admission requests (ARQs) are received, the MVAM proceeds as follows:

1 Identifies all the gateways that could possibly connect the call.

2 Checks the ratio of ports-in-use to ports-available for each covering gateway.

3 Selects a gateway with the most available resources for connecting the call (such as, the smallest ratio of ports in use to ports available).

Using the ratio of the gateway’s ports-in-use to the gateway’s number of available ports provides better load balancing across gateways with overlapping coverage areas and maximizes the use of available network assets.

Using routing based on port capacity, when three MultiVoice Gateways have the same inclusion area (such as, 516-555-11), the gatekeeper assigns the call to the

MultiVoice Gateway having the most idle ports (ports available), based on the total port capacity of the gateway.

Assigning calls based on call volume

The MultiVoice Access Manager assigns calls based on current call volume of each gateway when configured to do so. As call admission requests (ARQs) are received, the MVAM proceeds as follows:

1 Checks the current call volume of each covering gateway.

2 Determines which gateway is connecting the fewest calls.

3 Assigns the call to the gateway currently connecting the fewest calls.

Calls routed based on call volume do not take into account the port capacity of the individual gateway, (a port being the combination of a digital signal level 0 (DS0) and digital signal processor (DSP)), how many ports are currently idle and available for connecting calls on a given gateway.

Using the call volume routing method, when three MultiVoice Gateways have the same inclusion area (such as, 516-555-11), the gatekeeper assigns the call to the MultiVoice Gateway with the fewest active calls (ports in use), disregarding the total port capacity of that gateway.

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

MultiVoice networks supporting multizone call routing

MultiVoice supports routing calls between gateways which are registered with different MultiVoice Access Managers (Gatekeepers). Calls originating at one gateway, registered to and administered by one gatekeeper, are connected using a different gateway which is registered to and administered by another gatekeeper.

The ITU-T H.323 standard defines a zone as a group of gateways that register with and are administered by a single gatekeeper. Calls may be routed by the gatekeeper directly between any pair of gateways in the same zone.

Routing across H.323 zones

When calls are routed between zones, the gatekeeper in the zone where the call originates contacts a gatekeeper in another zone to locate a gateway to connect the call. When routing between zones, two MultiVoice Access Managers reside on separate servers, each with their own unique set of registered gateways. The two Access Managers set up the call between two gateways residing in different zones.

Implementing call routing

MultiVoice Access Managers use the optional called endpoint signaling method of call routing, which allows an MVAM to route a call through another gatekeeper.

Each MVAM in a MultiVoice network system maintains a database of peer gatekeepers. Each entry in this database contains a gatekeeper's identifier (a unique name) and its IP address. Each MVAM in the system also has a database of peer gatekeeper inclusion areas.

These inclusion areas define the telephone numbers that a gatekeeper is responsible for covering. Overlapping coverage areas are also supported for gatekeepers.

Figure 1-9 shows an example of a MultiVoice call routed between two gateways in different zones. The gatekeeper MVAM_east requests a call routing for a call originating in New York City to a telephone number in Los Angeles from the gatekeeper MVAM_west, which cannot be connected through an East Coast Zone gateway.

When a MultiVoice Access Manager is asked by a gateway to route a call, it first determines if the call can be routed to a gateway within its own zone. If the call can not be routed within its zone:

1 The East Coast gatekeeper, MVAM_east, receives a request to send a call from the East Coast gatekeeper GW_NY1 to a destination telephone number in Los Angeles, CA.

2 MVAM_east checks its gateway database. It determines that this call cannot be completed through a gateway in the East Coast zone.

3 MVAM_east checks its known gatekeeper database to determine if the coverage area is supported in another zone and locates a coverage area supported by the West Coast gatekeeper, MVAM_west.

4 MVAM_east sends a Location Request message (LRQ) to MVAM_west.

5 MVAM_west checks its gateway database. It determines that its gateway, CA_GW1, can connect the call.

6 MVAM_west sends a Location Confirmed (LCF) message containing the IP address of gateway CA_GW1.

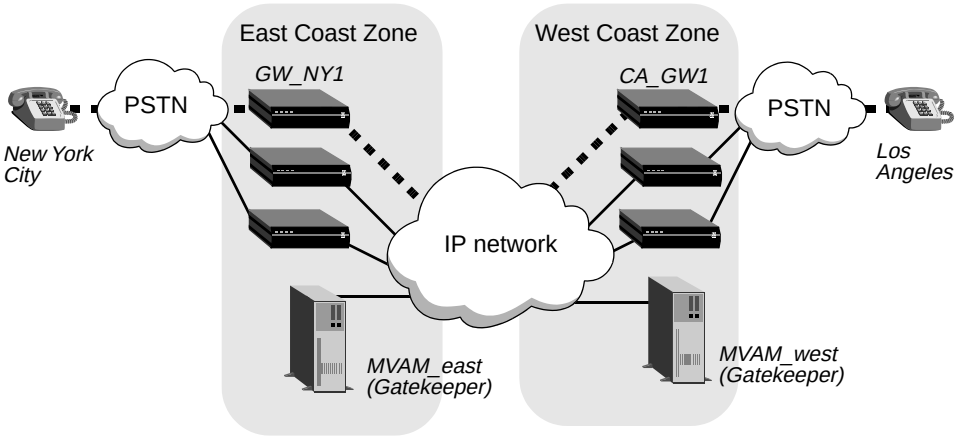
While waiting for a response, MVAM_east sends a Request-In-Progress (RIP) message to GW_NY1.

7 When MVAM_east receives the Location Confirmed (LCF) message from MVAM_west, an Admission Confirmed (ACF) message containing the conferenceId is sent to GW_NY1.

8 CA_GW1 completes the call.

If the covering gatekeeper decides it does not have a covering gateway, it returns a Location Reject (LRJ) message.

Figure 1-9. Example of a MultiVoice network supporting multizone call routing



While waiting for the covering gatekeeper to respond with gateway information, the MVAM generates pointers to a potential ACF message and the LRQ message in the Active Call Table, and returns without generating an ACF or an Admission

Reject (ARJ) message. The LRQ message has the conferenceIdentifier for the call in its nonStandardData parameter, and the covering gatekeeper returns this in the nonStandardData parameter of the LCF or LRJ message.

Gatekeeper virtual zones

The gatekeeper virtual zone feature allows a single MVAM to manage two or more groups of MultiVoice Gateways, each having its own unique configuration set. This includes distinct user, gateway, coverage areas, and call record databases, call administration settings, number translation tables, and call records and logs.

Definition of a gatekeeper virtual zones

A gatekeeper virtual zone is a subset of all MultiVoice Gateways that are administered and registered with a single MultiVoice Access Manager. Each virtual zone is managed by a virtual gatekeeper which exists on the same server as the MVAM. Each virtual gatekeeper has its own set of distinct gateway, gatekeeper, and user databases, which are separate and distinct from other databases maintained for the MVAM itself, or other virtual gatekeepers which also must exist on the same server.

Virtual zone call processing

When using gatekeeper virtual zones, calls are processed through a single MVAM as if it were different gatekeepers. Each virtual zone functions as an independent gatekeeper. A call received by gateways administered through a gatekeeper virtual zone are routed accordingly:

- The call is routed through another gateway within the same gatekeeper virtual zone
- The call is routed through a gateway within another gatekeeper virtual zone.

If the Access Manager is also setup to perform multizone operations (real gatekeeper-to-gatekeeper communications), a call received by gateways administered through one virtual zone are routed accordingly:

- The call is routed through another gateway within the same gatekeeper virtual zone
- The call is routed through a gateway within

- Another gatekeeper virtual zone on the same MVAM
- The zone administered by a remote MVAM
- Another gatekeeper virtual zone on a remote MVAM

Each gatekeeper virtual zone has a database of known peer gatekeepers. Each entry in this database contains a gatekeeper's identifier (a unique name) and its IP address. Each virtual zone on an MVAM also has a database of known gatekeeper inclusion areas.

These inclusion areas define which calls can be routed through a gatekeeper virtual zone. Overlapping coverage areas are also supported for virtual zones.

Figure 1-10 shows an example of a MultiVoice network using an MVAM with gatekeeper virtual zones. Each group of MultiVoice Gateways interacts with each gatekeeper virtual zone as if it was a single unique gatekeeper. In this instance, this MVAM has four gatekeeper virtual zones, in addition to the one "real" H.323 zone (GK_NJ) associated with the MVAM itself.

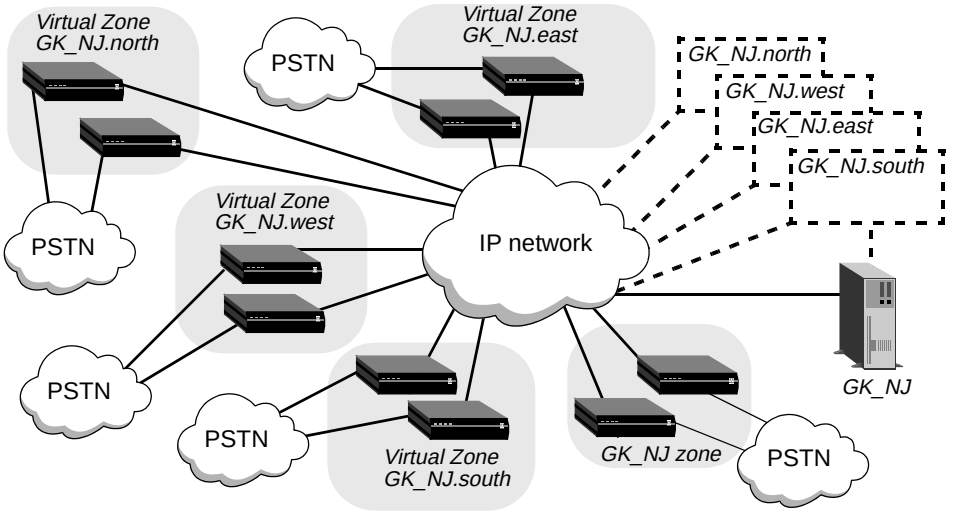
When a gateway in GK_NJ.north requests a call routing:

1. The call request is sent to the GK_NJ.north virtual zone on the GK_NJ Gatekeeper.
2. GK_NJ.north determines if the call can be routed to a gateway within its own zone. If the call can not be routed within its zone, the peer gatekeeper database is checked, to determine if the coverage area is supported by a remote gatekeeper or another virtual zone.
3. If a covering gatekeeper is located, a Location Request message (LRQ) is sent to the covering gatekeeper (such as, GK_NJ.south or a remote MVAM).
4. The covering gatekeeper determines if it has a covering gateway available to connect the call.
5. If a covering gateway is available, the covering gatekeeper responds with a Location Confirmed (LCF) message containing the IP address of the covering gateway.

   While waiting for the covering gatekeeper to respond, the gatekeeper virtual zone sends a Request-In-Progress (RIP) message to the originating gateway.
6. Once the Location Confirmed (LCF) message is received from the covering gatekeeper, an Admission Confirmed (ACF) message containing the conferenceId is sent to the calling endpoint.

7 The destination gateway completes the call.

Figure 1-10. Example of a MultiVoice network using gatekeeper virtual zones



If the covering gatekeeper decides it does not have a covering gateway, it returns a Location Reject (LRJ) message.

MultiVoice applications

MultiVoice supports a variety of applications, including:

- Basic public long-distance service
- Local 800 service
- Point-to-Point Private Branch Exchange (PBX) trunk extensions
- PBX trunk intraflow
- PC-to-phone over a virtual private network or an ISP's point of presence (PoP)

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

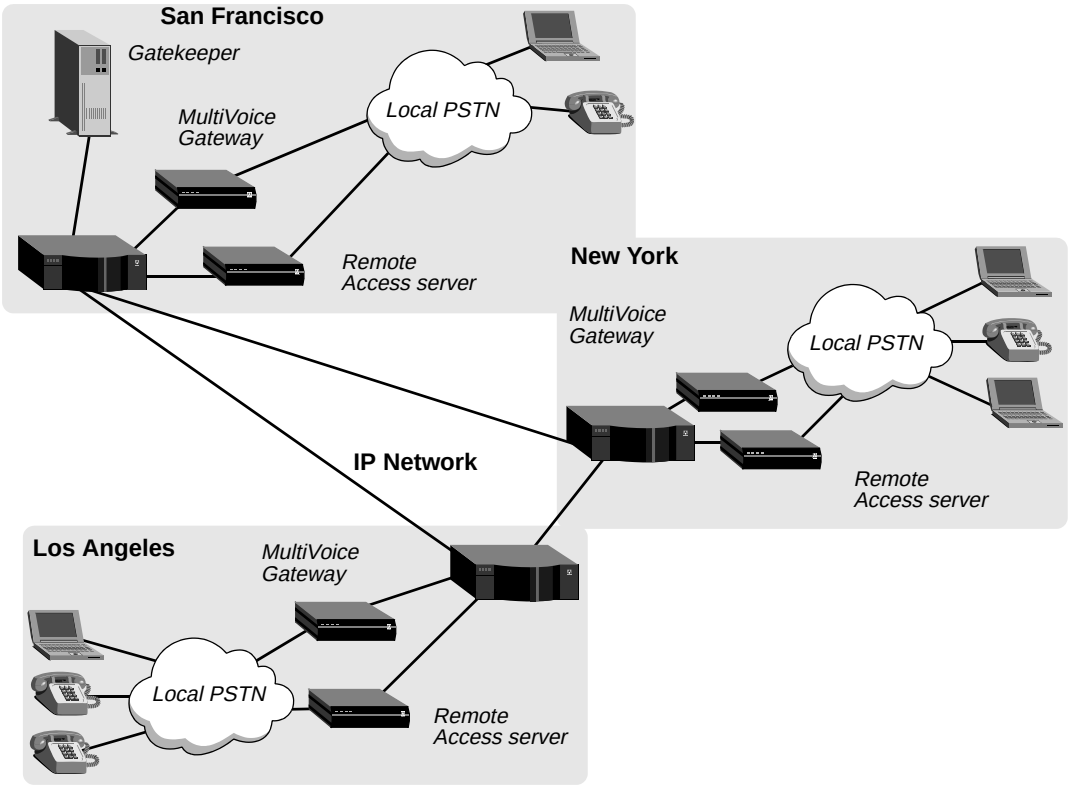
The IP network should be a managed infrastructure that maintains Quality of Service (QoS). Unmanaged IP networks have difficulty with consistent support for the real-time requirements of transporting voice and fax traffic. Whereas delays due to traffic congestion are usually only an inconvenience when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

For networks that support service precedence, MultiVoice provides options for configuring the Type of Service (ToS) byte. The MultiVoice administrator may change the Precedence bits (bit0, bit1, bit2) and the TOS bits (bit3, bit4, bit5, bit6) of the ToS byte contained in the UDP packet header. This changes the network priority for processing UDP packets by setting user defined values for delay, throughput and reliability.

Figure 1-11 shows an example of an ISP network implementing connectivity between New York, Los Angeles, and San Francisco. At each Point of Presence (PoP) in the figure, the ISP configures a MultiVoice Gateway dedicated to supporting voice traffic and a switch serving as a Remote Access server. Each MultiVoice Gateway and 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 Remote Access server. All customers send traffic over the same IP network.

Figure 1-11. Example of an ISP offering data and voice services



Local 800 service

Note: "800" refers to toll-free services which currently include the following exchanges: 800, 888, and 877.

Local 800 toll-free service can be much more cost-effective than traditional 800 service. Typically, leasing charges are less, and MultiVoice technology can eliminate long-distance phone charges.

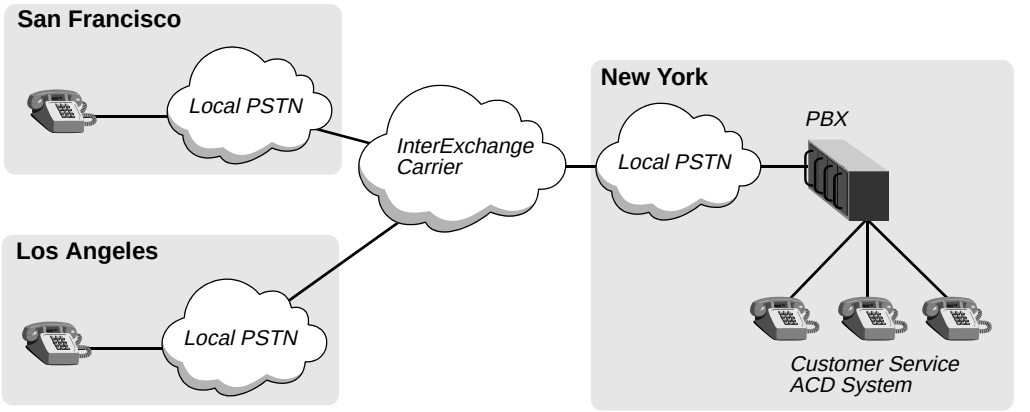
Traditional 800 service

Suppose a company maintains a customer service department, offering their customers a traditional 800 service phone number that they dial to receive assistance. Figure 1-12 shows an example of an environment without MultiVoice.

To reach a customer service representative, callers in San Francisco and Los Angeles dial an 800 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.

Figure 1-12. Traditional 800 environment

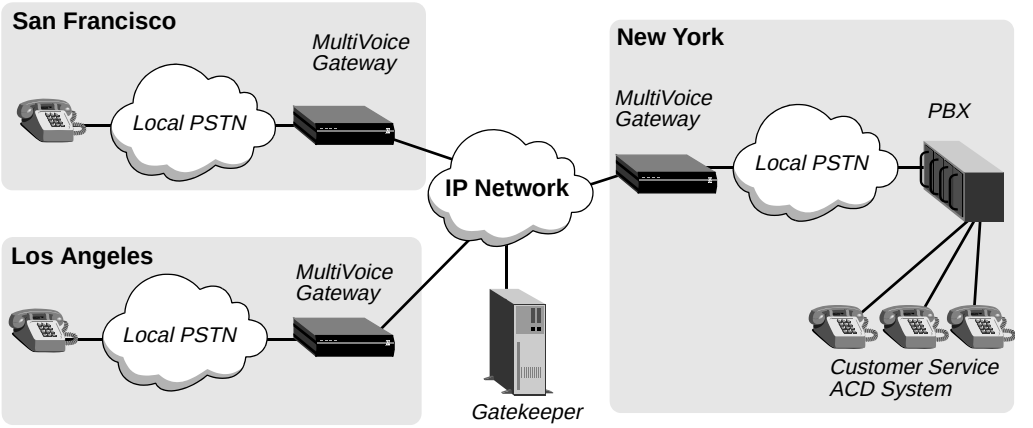


Using MultiVoice and local 800 service

Instead of leasing traditional 800 service, suppose the company in Figure 1-13 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. Figure 1-13 illustrates how a company can

use MultiVoice devices and local 800 service. Typically, leasing charges are less, and MultiVoice technology can eliminate long-distance phone charges.

Figure 1-13. Using MultiVoice and local 800 service

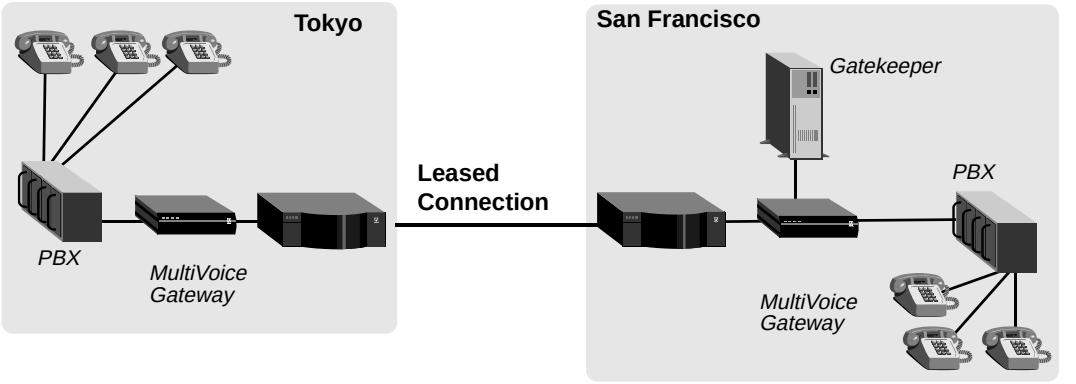


Point-to-point PBX trunk extension

Figure 1-14 shows an example of two locations connected by MultiVoice in a point-to-point configuration.

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.

Figure 1-14. Connecting two sites by MultiVoice and a leased connection

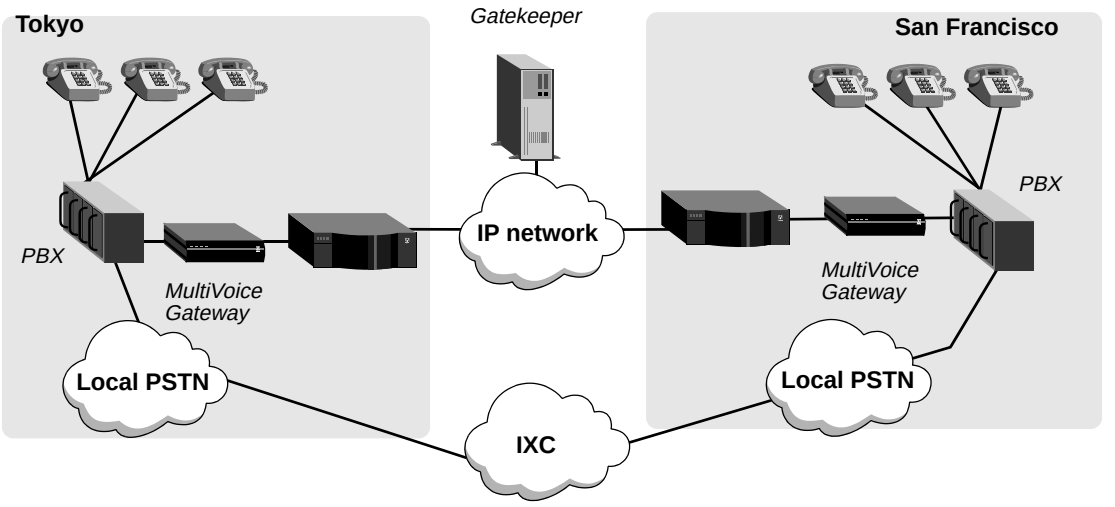


PBX trunk intraflow

Figure 1-15 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.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.

Figure 1-15. Alternative voice-traffic paths between sites



PC-to-Phone calls

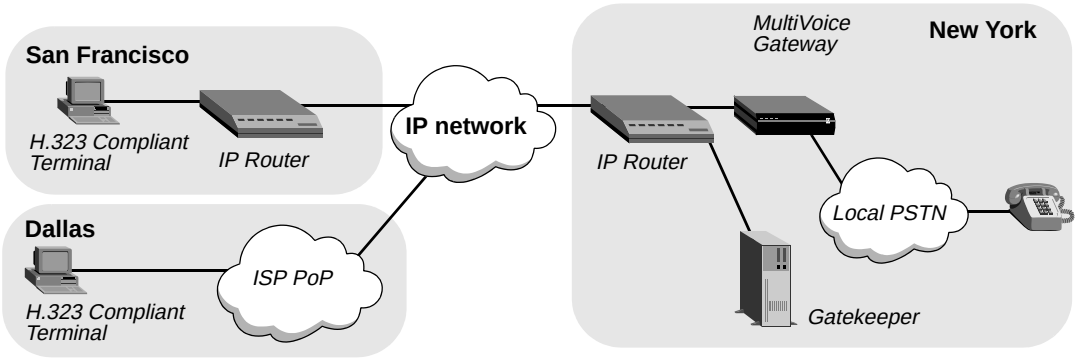
Calls initiated from PCs connected to a network are processed as if the PC was one of the MultiVoice Gateways. This requires that the PC be a fully *H.323-compliant terminal*. It must be able to register and communicate with the gatekeeper as if it were a gateway. It must also be able to communicate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

Figure 1-16 shows how to PC-to-Phone calls could be connected using either a *virtual private network* (VPN) or an ISP's PoP.

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 gateway.

Figure 1-16. Virtual private network using PC telephony



H.323 compliant terminals

H.323 compliant terminals are described in detail in the ITU-T Recommendation H.323. To work with MultiVoice, 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.

Gateway-to-client keep-alive registration

MultiVoice supports the use of a keep-alive protocol for gateway-to-clients (PCs) and/or gateway-to-gateway connections. This allows the gateway to detect terminated call connections when a remote endpoint becomes unreachable. The MultiVoice administrator may disable this feature or control the keep-alive time interval through the gateway interface. If the keep-alive timer expires during an active call, the call will be dropped by the gateway and reported to the MVAM with the disconnect reason "forcedDrop."

Setting Up MultiVoice Access Manager

2

Before you begin 2-1
Installing a Web server 2-5
Installing MultiVoice Access Manager 2-5
Starting MVAM 2-25
Stopping MVAM 2-32
Uninstalling MVAM 2-33

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 MultiVoice Access Manager serial number.
- This manual.

System requirements

The MultiVoice Access Manager can be installed on:

- a Windows NT 4.0 server or workstation
- a SPARC Solaris 2.5.1/2.6 system
- an HP-UX 10.20/11.00 system.

Minimum configuration for Windows NT systems

The minimum system configuration for installing MultiVoice Access Manager on a Windows NT 4.0 system is:

- Pentium 266 MHz CPU (faster than 266 MHz recommended)
- 64 Mb of system RAM (96 Mb or greater recommended)
- 4 GB hard disk (greater than 4 GB recommended)
- CD-ROM drive. This is required if you purchased and received the software on CD.
- a TCP/IP network interface card

Warning: Windows NT systems must be upgraded to Service Pack 4, or later, in order for Release 3.0.0 to function properly. Running this release of MVAM without Service Pack 4, or later, installed may corrupt the Windows NT system, the MVAM application, and MultiVoice network operations.

Minimum configuration for SPARC Solaris 2.5.1 systems

The minimum, and recommended, system configuration for installing the MultiVoice Access Manager on a SPARC Solaris 2.5.1 or 2.6 system are:

- 64 Mb of system RAM
- 250 Kb of hard disk space
- CD-ROM drive. This is required if you purchased and received the software on CD.
- a TCP/IP network interface card

Minimum configuration for HP-UX 10.20 systems

The minimum, and recommended, system configuration for installing the MultiVoice Access Manager on an HP-UX 10.20 or 11.00 system are:

- 64 Mb of system RAM
- 250 Kb of hard disk space
- CD-ROM drive. This is required if you purchased and received the software on CD.
- a TCP/IP network interface card

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

Windows NT 4.0, Solaris 2.5.1/2.6, and HP-UX 10.20/11.00 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; however, 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, included with the Windows NT 4.0 Server system.
- Imatix's Xitami Web server, version 1.3c or later, available from Imatix at `http://www.imatix.com`, for use with a Windows NT 4.0 Workstation.

On 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.

On HP-UX 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 Access Manager per-port licensing

The MultiVoice Access Manager provides per-port licensing implemented by serial numbers. A MultiVoice Access Manager serial number is included with MVAM Release 3.0.0 software and is required for installation. The serial number is located on the product packaging as well as on the Warranty Registration Card. The MultiVoice Access Manager software will not run without a valid serial number. See Appendix B, "MVAM Licenses" for more information.

Installation sequence

To simplify installation of the MultiVoice Access Manager, it is recommended you use the following installation sequence:

1 Install the Web server software on the system where you will run MVAM.

2 Install the MultiVoice Access Manager application.

3 Install any third-party billing application you will run with MVAM.

If you follow a different installation sequence, it may be necessary to manually perform additional configuration of each of the software packages.

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 consists of:

- Setting the location of the MVAM HTML files. On a Windows NT system, the HTML files are located, by default, in the webpages subdirectory of the MVAM installation directory. On a Solaris system or an HP-UX system, the location of the HTML files are specified by the user during installation.
- Setting the location of the CGI directory. On a Windows NT system, `mvam_cgi.exe` is located, by default, in the cgi-bin subdirectory of the MVAM installation directory. On a Solaris system or an HP-UX system, the location of `mvam_cgi.exe` is specified by the user during installation.

When configuring the path information, use the directory names for the MVAM HTML and CGI directories specified during installation of the MultiVoice Access Manager software.

Restart your Web server to ensure the new values are set before you launch MVAM. See vendor-specific instructions for your Web server, for details on configuring the default HTML and CGI directories.

Installing MultiVoice Access Manager

Procedures for installing and launching MVAM depend on the platform (Window NT, Solaris, or HP-UX) you intend to use.

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 installing the MultiVoice Access Manager to Release 3.0.0:

- Back up the files in the subdirectories `db` and `calls`, including the calls/current/ directory.
- Locate the MultiVoice Access Manager serial number for your MultiVoice Access Manager software, you will need this to install the software.

  Your serial number is located on the Warranty Registration card included with your purchase of the software.

Installation on a Windows NT 4.0 system

Before you begin with the installation of the MultiVoice Access Manager (MVAM) Release 3.0, we recommend that you:

1. Locate and note your MVAM Release 3.0.0 serial number.
2. Exit all programs, including MVAM if it is installed and currently running.
3. If you are upgrading an existing MVAM installation, make a backup copy of your existing MVAM installation directory (typically the c:\mvam directory) as well as the mvam.ini residing under your Windows NT installation directory.

Note: During installation, it is recommended that you accept the default installation information.

Installation procedure

To install the MultiVoice Access Manager:

1. Start Windows NT.
2. Insert the MVAM Installation CD into the CD-ROM drive.

   If the installation program does not start automatically:

– Click the Start menu. Select Run and type `d:\Setup.exe` in the entry field (substitute the appropriate letter if your CD-ROM drive is not drive `d:`), then click OK, or

– In Windows NT Explorer, open the directory window for your CD-ROM drive and double click `Setup.exe`.

Setup displays the MultiVoice Access Manager Welcome message, as illustrated in Figure 2-1:

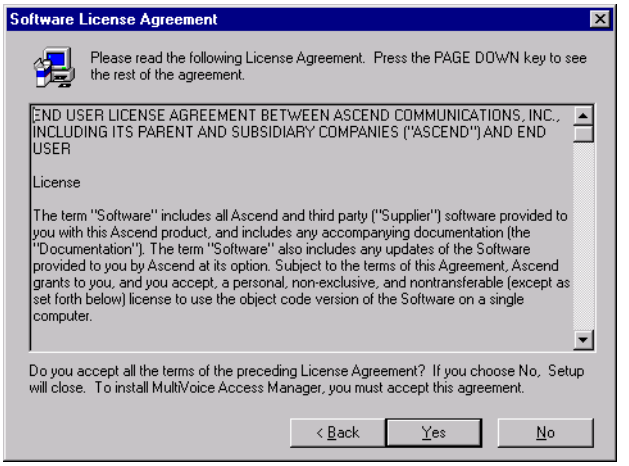
Figure 2-1. MultiVoice Access Manager Welcome message



3 Click the Next button to continue installation.

4 The next screen displays the Software License Agreement, as illustrated in Figure 2-2. In order to continue, you must click the Yes button, acknowledging that you accept the terms of the Lucent End User Agreement. Clicking the No button will abort MVAM installation.

Figure 2-2. Software License Agreement screen



The next sequence of screens contain a set of instructional messages, as illustrated by Figure 2-3, Figure 2-4, and Figure 2-5, which explain the installation process and direct you to collect and backup files from your current MVAM installation before continuing.

Figure 2-3. Initial pre-installation instructions screen

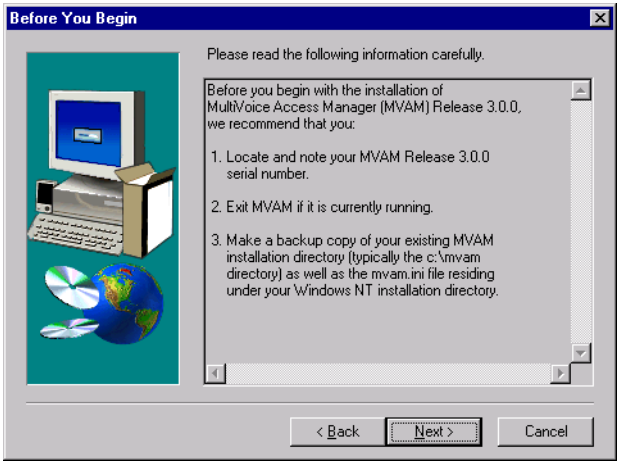


Figure 2-4. Subsequent pre-installation instructions screen (second)

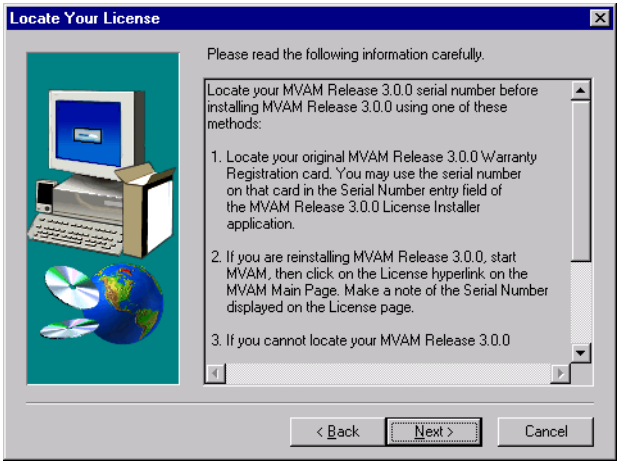
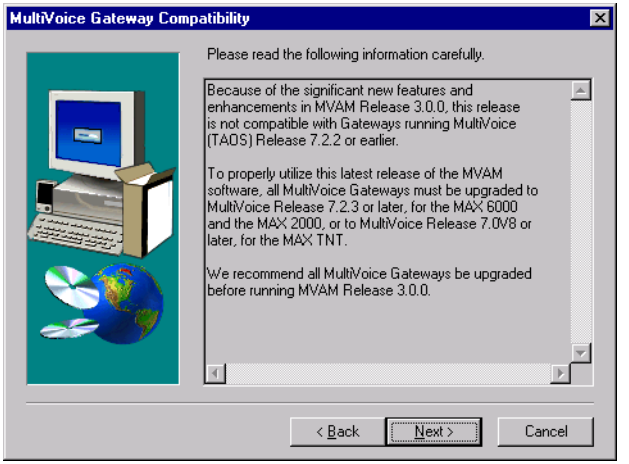


Figure 2-5. Subsequent pre-installation instructions screen (last)



5 Click the Next buttons to page through these screens.

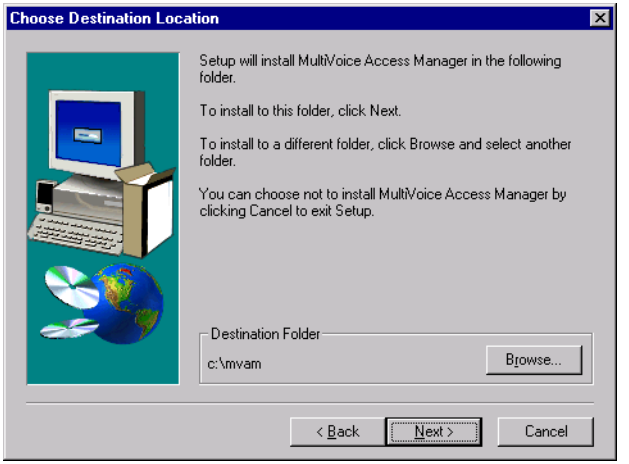
Once you have paged through and read these screens, Setup displays the Destination Location screen, as illustrated in Figure 2-6. This screen is used to identify the installation directory for MVAM.

6 Select the Next button to accept the default installation directory `c:\mvam`. You may click the Browse button to designate a different Destination Folder.

Note: It is recommended that you accept the default destination.

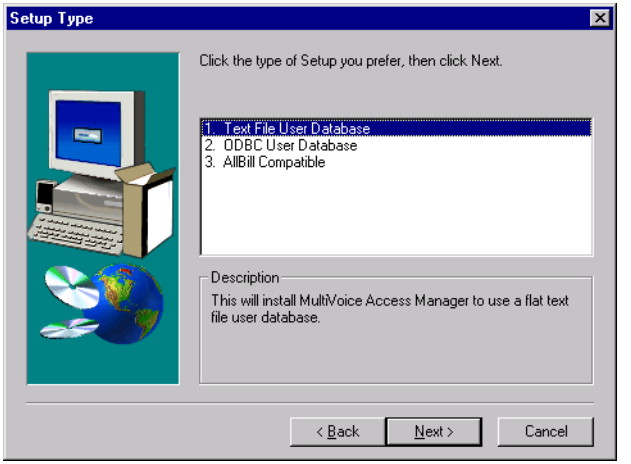
Note: If you are performing an upgrade installation for an earlier release of MVAM and it is not installed in `c:\mvam`, change the destination folder to the same folder in which the currently installed MVAM resides.

Figure 2-6. Destination Location screen



After selecting the installation location, Setup displays the Setup Type screen, as illustrated by Figure 2-7. This defines the data format of the User database.

Figure 2-7. Setup Type screen



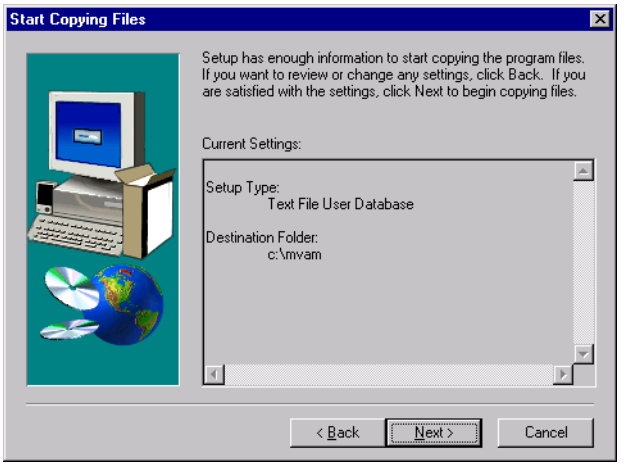
7 Select one of the following database formats for MVAM user records by selecting an entry in the selection window:

Database Format	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), and many third-party billing systems.
AllBill Compatible	Select this method if you use the AllBill billing application to store your information.

Note: If you select the ODBC User Database option you must install the appropriate ODBC drivers from the Microsoft Data Access Components (MDAC) 2.1 software package. These drivers are available from Microsoft Support at its Universal Data Access download site. The appropriate ODBC drivers must be installed before you start MVAM.

After selecting the user database format, the installation program displays the Start Copying Files screen as illustrated in Figure 2-8.

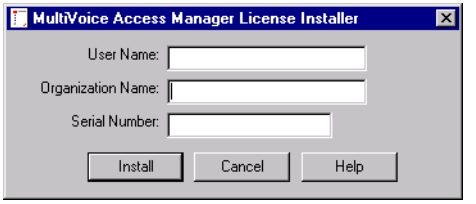
Figure 2-8. Start Copying Files screen



8 This displays a summary of your installation settings. If this information is correct, click the Next button to continue. If you need to change any of this information click the Back button until you return to the appropriate screen, then make any desired changes.

Once you have verified your installation options, Setup displays the MultiVoice Access Manager License Installer dialog box, as illustrated in Figure 2-9.

Figure 2-9. License Installer dialog box



9 In this MultiVoice Access Manager License Installer dialog box:

– Enter your name or the name of the person in the User Name field who will use the program. Example: John Smith

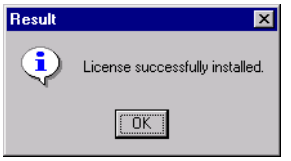
– Enter the name of your organization in the Organization Name field. Example: Lucent Technologies

– Enter the MultiVoice Access Manager serial number that is printed on the Warranty Registration card that was included in the MVAM 3.0.0 installation package. Example: MVAM-300-AN-00000000

Note: If you enter an incorrect serial number, the Installer does not install the license, and MVAM will not run.

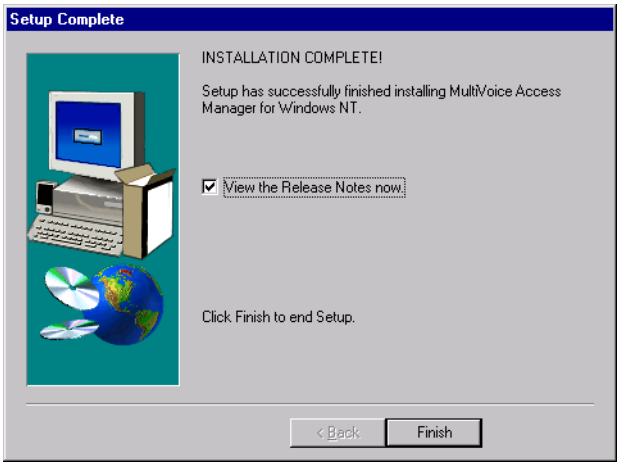
– Click the Install button. The message "`Please Wait...`" appears on the screen.

Once you have entered a valid MultiVoice Access Manager serial number, Setup displays the following message:



10 Click the OK button. Setup displays a message that the MultiVoice Access Manager was installed successfully, as shown in Figure 2-10.

Figure 2-10. Successful Installation of MVAM message



Configuring system software

To properly configure MVAM Release 3.0.0 for Windows NT, perform the following steps:

1. Update your newly installed mvam.ini file under your Windows NT installation directory with any custom settings that cannot be set via MVAM's Web browser-based administration interface with the settings from your previous mvam.ini file, if any. See Appendix A, "MVAM Initialization File" for more information.

   Note: If you had a previous release installed, your previous mvam.ini file was copied to `mvam.ini.BAK` under your Windows directory (for example, c:\Windows or c:\Winnt).

2. Configure the Web server to use the directory names for the MVAM HTML and CGI directories specified during installation of the MVAM software.

   For example, specify `c:\mvam\cgi-bin` as the CGI directory and `c:\mvam\webpages` as the HTML directory, if you accepted the default installation directory, `c:\mvam`, when you installed MVAM.

   If you want to enable and use the Virtual Zones feature, set the Web server's default HTML page to `frame.htm` instead of `index.htm`.

3. Start MVAM and verify that the MVAM release number 3.0.0 is displayed.

4. Configure MVAM via a Web browser. We do not recommend manually editing the \mvam\db data files to restore your settings unless you are familiar with the (updated) formats for these files. Configure the gateway(s) and coverage areas required. Verify/set the appropriate security options (such as PIN or ANI) under Options/Security or configure ADMA rules for authentication. Configure the other MVAM options as desired.

5. Configure the gateway(s) to be used with the gatekeeper address. Configure the VPN mode setting (No=gateway PIN prompting is enabled), and the voice announcements TFTP settings on the gateway, if the MLG parameter is not enabled.

   If the MLG parameter is enabled on the gateway, configure ADMA rules to control dial mode and determine the voice announcements directory to use.

6. Verify that the gateway(s) have successfully registered with MVAM.

7. Make a call, answer it, and then hang up. If the call was successfully placed, then MVAM has been installed and configured correctly and its configuration is now complete.

Installation on a Solaris system

To install MultiVoice Access Manager (MVAM) on a Solaris workstation or server, use the UNIX pkgadd command. You must perform the installation as the root user. During the installation, you are asked to define the MVAM user and the installed location(s) for the MVAM software.

Before you begin with the installation of the MultiVoice Access Manager (MVAM) Release 3.0, we recommend that you:

1 Locate and note your MVAM Release 3.0.0 serial number.

2 Exit MVAM if it is installed and currently running.

3 If you are upgrading an existing MVAM installation, make a backup copy of your existing MVAM installation directory (typically the /opt/mvam/ directory) as well as the mvam.ini or .mvam.ini file residing in /opt/mvam/ or your $HOME directory.

During installation you will be prompted to:

- enter your valid MultiVoice Access Manager serial number (printed on the Warranty Registration card that was included in the MVAM 3.0.0 installation package).
- enter the valid user and group IDs for the MVAM user (verify them by looking in the /etc/group file; do not enter a non-system user ID that is less than 100),
- enter the MVAM installation directory,
- enter the directories where your Web server stores its HTML pages and its CGI scripts.

Note: You should install your Web server before you install MVAM.

Note: You must be logged in as `root` to install MVAM; you need not be logged in as `root` to run MVAM. Run MVAM as the user you designate as MVAM user during your installation.

Installation for boot-up operation

During MultiVoice Access Manager installation, the user is prompted to install the application at system boot-up:

```
Do you want MVAM to start at system boot-up [no]?
```

When "y" is entered for this prompt, the Access Manager is installed to startup when the Solaris system boots up. The appropriate commands are written to the Solaris boot files, which will start the Access Manager in the background, without opening the MultiVoice Access Manager Integrated Window.

When "n", the default, is entered for this prompt, the Access Manager is installed to run as a foreground application.

Installation procedure

To install the MultiVoice Access Manager:

1. Install and configure a supported Web server, such as the Apache Web server. Be sure to note the Web server's HTML page and CGI bin directories where MVAM will install its Web pages and CGI adapter executable as you'll be prompted for them.
2. Load the MVAM CD-ROM into the Solaris system, making sure that it is mounted on `/cdrom`.
3. Execute `pkgadd` to install MVAM by typing the following command:

   ```
   pkgadd -d /cdrom/lumvam LUmvam
   ```
4. Follow the instructions that appear on your screen. Below is a script of a sample MVAM Release 3.0.0 installation on a Solaris system.

Note: Default IDs, filenames, and directories are provided (in parentheses) during installation. It is recommended that you use these defaults, unless a filename or directory is specified. These defaults are determined by the attributes associated with the current login ID of the user performing the installation, for example, `root`. You *must* have write permissions to the directories you specify or accept as the default for MVAM to install properly.

Sample Solaris installation script for upgrading from Release 2.2.0 to MVAM Release 3.0.0

Note: The sample script below may differ slightly from your installation script.

```
# pkgadd -d /cdrom/lumvam LUmvam

Processing package instance <LUmvam> from </cdrom/lumvam>
```

```
MultiVoice Access Manager
(sparc) 3.0.0
MultiVoice Access Manager
Copyright (c) 1997-1999 Ascend Communications, Inc., a subsidiary
of Lucent Technologies Inc. All rights reserved.
Copyright (c) 2000 Lucent Technologies Inc. All rights reserved.
MVAM 2.2.0 (package ASNDmvam.2) detected.
Do you want to upgrade MVAM 2.2.0 to 3.0? (y)
```

Note: Several messages recommending actions to perform prior to installation, as well as software compatibility messages will display.

```
Do you want MVAM to start at system boot-up? (no)

User name: MultiVoice administrator
Organization name: VoIP networks operations
Serial number: MVAM-300-AS-99999999
Please wait...

Using </> as the package base directory.
## Processing package information.
## Processing system information.
   12 package pathnames are already properly installed.
## Verifying disk space requirements.
## Checking for conflicts with packages already installed.

The following files are already installed on the system and are being
used by another package:
  /opt/mvam/README
...
  /usr/local/apache/htdocs/xlatrouteh.htm

Do you want to install these conflicting files [y,n,?,q] y
## 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 <LUmvam> [y,n,?] y

Installing MultiVoice Access Manager as <LUmvam>

## Executing preinstall script.
## Installing part 1 of 1.
/opt/mvam/README
...
/usr/local/apache/htdocs/xlatrouteh.htm
[ verifying class <none> ]
## Executing postinstall script.
Please wait...
MVAM license installed successfully.
Please 'pkgrm ASNDmvam.2' to uninstall MVAM 2.x.

Installation of <LUmvam> was successful.
```

Sample Solaris installation script for MVAM Release 3.0.0

Note: The sample script below may differ slightly from your installation script.

```
# pkgadd -d /cdrom/lumvam LUmvam

Processing package instance <LUmvam> from </cdrom/lumvam>

MultiVoice Access Manager
(sparc) 3.0.0
MultiVoice Access Manager
Copyright (c) 1997-1999 Ascend Communications Inc., a subsidiary of Lucent Technol-
ogies Inc. All rights reserved.
Copyright (c) 2000 Lucent Technologies Inc. All rights reserved.
```

Note: Several messages recommending actions to perform prior to installation, as well as software compatibility messages will display.

```
MVAM user [?,q] mvammgr
Please wait...
MVAM group (software) [?,q]
MVAM top level directory (/opt/mvam) [?,q]
/opt/mvam does not exist; create it?  (n) y
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]
Do you want MVAM to start at system boot-up? (no)

User name: MultiVoice administrator
Organization name: VoIP networks operations
Serial number: MVAM-300-AS-99999999
Please wait...

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 <LUmvam> [y,n,?] y

Installing MultiVoice Access Manager as <LUmvam>

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

```
/opt/mvam/README
    .
    .
    .
/usr/local/apache/htdocs/xlatrouteh.htm
[ verifying class <none> ]
## Executing postinstall script.
Please wait...
MVAM license installed successfully.

Installation of <LUmvam> was successful.
```

Configuring system software

To properly configure MVAM Release 3.0.0 for Solaris, do the following:

1. Update your mvam.ini file under the HOME directory specified at install time with any custom settings that cannot be set via MVAM's Web browser-based administration interface with the settings from your previous mvam.ini file, if any.
2. If you installed MVAM's HTML content and CGI scripts under `/opt/mvam/` (in `/opt/mvam/htdocs/` and `/opt/mvam/cgi-bin/`, respectively), configure your Web server to use these directories. If you want to enable and use the Virtual Zones feature, also set the Web server's default HTML page to `frame.htm` instead of `index.htm`.
3. Start MVAM and verify that the MVAM version number 3.0.0 is displayed.
4. Configure MVAM via a Web browser. We do not recommend manually editing the /opt/mvam/db/ data files to restore your settings unless you are familiar with the (updated) formats for these files. Configure the gateway(s) and coverage areas required. Verify/set the appropriate security options (such as PIN or ANI) under Options/Security or configure ADMA rules for authentication. Configure the other MVAM options as desired.
5. Configure the gateway(s) to be used with the gatekeeper address. Configure the VPN mode setting (No=gateway PIN prompting is enabled), and the

voice announcements TFTP settings on the gateway, if the MLG parameter is not enabled.

If the MLG parameter is enabled on the gateway, configure ADMA rules to control dial mode and determine the voice announcements directory to use.

6 Verify that the gateway(s) have successfully registered with MVAM.

7 Make a call, answer it, and then hang up. If the call was successfully placed, then MVAM has been installed and configured correctly and its configuration is now complete.

Installation on an HP-UX system

To install MVAM Release 3.0.0 on an HP-UX system, you must be logged in as a user with permission to write to the Web server's document root and CGI bin directories. If you attempt to install MVAM Release 3.0.0 in a directory in which you do not have write permissions, the installation will fail.

Before you begin with the installation of the MultiVoice Access Manager (MVAM) Release 3.0, we recommend that you:

1 Locate and note your MVAM Release 3.0.0 serial number.

2 Exit MVAM if it is installed and currently running.

3 If you are upgrading an existing MVAM installation, make a backup copy of your existing MVAM installation directory (typically the /opt/mvam/ directory) as well as the mvam.ini or .mvam.ini file residing in /opt/mvam/ or your $HOME directory.

During installation you will be prompted to:

- enter your valid MultiVoice Access Manager serial number (printed on the Warranty Registration card that was included in the MVAM 3.0.0 installation package).
- enter the valid user and group IDs for the MVAM user (verify them by looking in the /etc/group file; do not enter a non-system user ID that is less than 100),
- enter the MVAM installation directory,

- enter the directories where your Web server stores its HTML pages and its CGI scripts.

Note: You should install your Web server before you install MVAM.

Installation procedure

To install the MultiVoice Access Manager:

1. Install and configure a supported Web server, such as the Apache Web server. Be sure to note the Web server's HTML page and CGI bin directories where MVAM will install its Web pages and CGI adapter executable as you'll be prompted for them.
2. Load the MVAM CD-ROM into the HP-UX system, making sure that it is mounted on `/SD_CDROM`.

   Note: The CD-ROM must not be installed via HP's System Administration Manager (SAM). The CD-ROM must be mounted (by `root`) similar to the following:

   ```
   mount -F cdfs -o cdcase /dev/dsk/c1t22d0/SD_CDROM
   ```

   where `/dev/dsk/c1t2d0` is the CD-ROM drive and /SD_CDROM is the directory where the CD-ROM will be mounted.

   Note: If the CD-ROM appears to have an HPUX/ directory, and its files and directories are upper case, the CD-ROM was not mounted properly. Refer to step 2 to properly mount the CD-ROM.
3. Change to the `/SD_CDROM/hpux` directory.
4. As `root`, or as the user who will be running MVAM, type the following command:

   ```
   ./install
   ```
5. Follow the instructions that appear on your screen. Below is a script of a sample MVAM Release 3.0.0 installation on an HP-UX system.

Note: Default IDs, filenames, and directories are provided (in parentheses) during installation. It is recommended that you use these defaults, unless a filename or directory is specified. You *must* have write permissions to the directories you specify or accept as the default for MVAM to install properly.

Sample HP-UX installation script for MVAM Release 3.0.0

Note: The sample script below may differ slightly from your installation script.

```
$ ./install

MultiVoice Access Manager
(hp-ux) 3.0.0
MultiVoice Access Manager
Copyright (c) 1997-1999 Ascend Communications Inc., a subsidiary of Lucent Technol-
ogies Inc. All rights reserved.
Copyright (c) 2000 Lucent Technologies Inc. All rights reserved.
```

Note: Several messages recommending actions to perform prior to installation, as well as software compatibility messages will display.

```
MVAM user [?,q] mvammgr
Please wait...
MVAM group (software) [?,q]
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]
User name: MultiVoice administrator
Organization name: VoIP networks operations
Serial number: MVAM-300-AH-99999999
Please wait...
MVAM license installed successfully.
```

Configuring system software

To properly configure MVAM Release 3.0.0 for HP-UX, do the following:

1. Update your mvam.ini file under the HOME directory specified at installation with any custom settings that cannot be set via MVAM's Web browser-based administration interface.
2. If you installed MVAM's HTML content and CGI scripts under `/opt/mvam/` (in `/opt/mvam/htdocs/` and `/opt/mvam/cgi-bin/`, respectively), configure your Web server to use these directories. If you want to enable and use the Virtual Zones feature, also set the Web server's default HTML page to `frame.htm` instead of `index.htm`.
3. Start MVAM and verify that the MVAM version number 3.0.0 is displayed.
4. Configure MVAM via a Web browser. We do not recommend manually editing the /opt/mvam/db/ data files to restore your settings unless you are familiar with the (updated) formats for these files. Configure the gateway(s) and coverage areas required. Verify/set the appropriate security options (such as PIN or ANI) under Options/Security or configure ADMA rules for authentication. Configure the other MVAM options as desired.
5. Configure the gateway(s) to be used with the gatekeeper address. Configure the VPN mode setting (No=gateway PIN prompting is enabled), and the voice announcements TFTP settings on the gateway, if the MLG parameter is not enabled.

   If the MLG parameter is enabled on the gateway, configure ADMA rules to control dial mode and determine the voice announcements directory to use.
6. Verify that the gateway(s) have successfully registered with MVAM.
7. Make a call, answer it, and then hang up. If the call was successfully placed, then MVAM has been installed and configured correctly and its configuration is now complete.

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 Solaris system, as well as on an HP-UX 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 Solaris and HP-UX systems, the location of this subdirectory is set by the user during installation.
`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, HP-UX))	Contains all the HTML files. **Note:** For Solaris and HP-UX systems, the location of this subdirectory is set by the user during installation.

MVAM configuration and control files

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

File	Description	File Location on Solaris & HP-UX	File Location on Windows NT
MVAM Initialization file	This file contains all values set when MVAM is started. If this file is missing, nothing is displayed when MVAM is started. (For details, see Appendix A, "MVAM Initialization File.")	`$HOME/mvam.ini`	`\Winnt\mvam.ini`
Application Data file	Created during MVAM installation. If this file is missing or corrupted, the MVAM will not run. It is stored in the MVAM installation directory.	`$HOME/mvam.dat`	`\Winnt\mvam.dat`
API configuration file	This file is installed by default and used to configure MVAM and API applications for using the API.	`/opt/mvam/bin/amv_gk_table`	`c:\mvam\bin amv_gk_table`

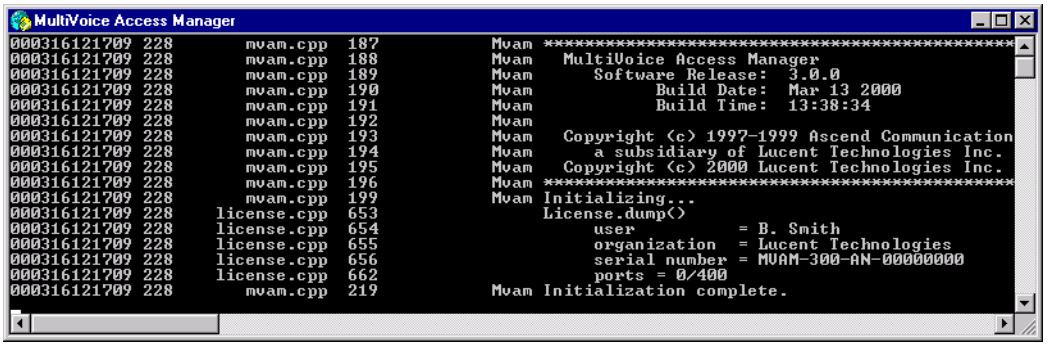
Launching MVAM on a Windows NT system

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 a few key items of information:

- The version of the MVAM that you loaded
  `Software Release: 3.0.0`
- The total numbers of ports in use and the total supported port capacity of this Access Manager
  `ports = 0/400`
- Verification that MVAM loaded successfully
  `Mvam Initialization complete`

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.

Changing window properties

The text in the window may be difficult to read due to the property settings of the window. To change the windows properties.

1 Right click the globe icon and select Properties.

2 You may change the properties by selecting any of the tabs displayed: Options, Font, Layout, and Colors.

- Options: You can make changes to the cursor size, command history, QuickEdit Mode, Insert Mode, and display options
- Fonts: You can choose to display different fonts and font sizes for character-based windows (consoles) and command prompt windows.

– Layout: You can specify where console windows are set up on the screen, the size of the window, and the amount of information the screen buffer contains. For example: By adjusting the screen buffer size in both directions (width and height), you can add scroll bars to the window, and by adjusting the window size you can make the window larger across the monitor screen.

– Color: You can specify the color of the text and background of all character-based windows (consoles) and command prompt windows.

Note: Each property tab has a help feature. For more information on each property tab, click the Help button in the lower-right corner of the tab selected.

3 Select the OK button.

4 The properties will remain in effect until you close the window if you select "Apply properties to current window only".

If you select "Modify the shortcut that started this window", the properties will remain in effect every time you open this window.

Launching the MVAM on a SPARC Solaris system

Note: We do not recommend MVAM be run as `root`, or any other privileged user (numeric user ID less than 100). MVAM has no known security vulnerabilities; however, good practices call for software to be installed with the least possible privileges. MVAM needs no special privileges; it can, and should be run as an ordinary non-privileged UNIX system user.

To launch MVAM on a SPARC Solaris system:

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 option, `--home`, followed by the name of the working directory used by the MultiVoice Access Manager (`/opt/mvam`).

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

After you launch the MVAM, the following window appears:



The display includes a few key items of information:

- The version of the MVAM that you loaded
  `Software Release: 3.0.0`
- The total numbers of ports in use and the total supported port capacity of this Access Manager
  `ports = 0/3000`
- Verification that MVAM loaded successfully
  `Mvam Initialization complete`

After checking the MVAM window, minimize it.

Launching the MVAM on an HP-UX system

Note: We do not recommend MVAM be run as `root`, or any other privileged user (numeric user ID less than 100). MVAM has no known security vulnerabilities; however, good practices call for software to be installed with the least possible privileges. MVAM needs no special privileges; it can, and should be run as an ordinary non-privileged UNIX system user.

To launch MVAM on an HP-UX system:

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 option, `--home`, followed by the name of the working directory used by the MultiVoice Access Manager (`/opt/mvam`).

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

After you launch the MVAM, the following window appears:



The window displays a few key items of information:

- The version of the MVAM that you loaded
  `Software Release: 3.0.0`
- The total numbers of ports in use and the total supported port capacity of this Access Manager
  `ports = 0/3000`
- Verification that MVAM loaded successfully
  `MVAM Initialization complete`

After checking the MVAM window, minimize it.

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 host 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 host name.

Stopping MVAM

The MultiVoice Access Manager may need to be stopped for various reasons, such as: performing installation, applying changes made to the initialization file, etc. MVAM will shut down cleanly when the system is shut down or rebooted.

Stopping MVAM on a Windows NT system

Close the window in which MVAM is running by either:

- Selecting the icon in the upper-left corner of the window and selecting Close, or
- Selecting the close box (the right-most of the three boxes) in the upper-right corner of the window.

Stopping MVAM on a Solaris or HP-UX system

MVAM running on a Solaris or HP-UX system, may be stopped in several ways:

- If MVAM is running in the foreground, hit the “interrupt” key (usually Ctrl+C).

- If MVAM is running in a window, close the window (unless it was started with the “nohup” command).
- If you know MVAM’s process ID, execute the kill command as follows:

  `kill 10247`

  where *10247* is MVAM’s process ID (found by executing the ps command).

  Note: As for all Unix systems, it is **not** recommended to use “`kill -9`” or “`kill -KILL`”. If you are unfamiliar with the kill command, do not use this command with any options.

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 subdirectories `db` and `calls`, including the file, `calls/current/calls.txt`.

Uninstalling MVAM from a Windows NT system

MVAM may be uninstalled from Windows NT in two ways: from the Start menu or from the Add/Remove Software utility on the Control Panel.

To uninstall MVAM from the Start menu:

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 Programs > MultiVoice Access Manager > Uninstall MVAM.
3. You will be prompted to confirm the deletion of all files. Select Yes to uninstall MVAM, select No to abort the uninstallation.

To uninstall MVAM from the Add/Remove Software utility:

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.
4. Select the MultiVoice Access Manager entry.
5. Click the Add/Remove button to automatically uninstall MVAM.

Uninstalling MVAM from a Solaris system

To uninstall MVAM from a Solaris 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: You must perform this procedure when upgrading MVAM. It is recommended that you backup the files in the db directory first. 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 LUmvam`**

   The following prompt appears:

   ```
   The following package is currently installed:
   LUmvam  MultiVoice Access Manager
    (sparc) 3.0.0

   Do you want to remove this package?
   ```

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

   During this process, `pkgrm` will prompt you to confirm the removal of MVAM files.

Uninstalling MVAM from an HP-UX system

The process of uninstalling MVAM 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.

Proceed as follows:

1. Make sure that MVAM is not running.
2. Run the following script for the bin directory under the MVAM top level directory, for example, `/opt/mvam/` if MVAM was installed in this directory:

   ```
   /opt/mvam/bin/uninstall
   ```

3. The following appears:

   ```
   The following package is currently installed:
   LUmvam  MultiVoice Access Manager
    (hp-ux) 3.0.0

   Do you want to remove this package?
   ```

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

Configuring the Access Manager 3

Connecting to MVAM 3-1

Configuring MVAM options 3-5

Configuring Gatekeeper virtual zones 3-28

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 to a local MVAM installation

To access MVAM from the same computer where you installed it, enter any of the following URLs in your Web browser's Address field:

- `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.

To access an MVAM configured for Gatekeeper virtual zones, enter any of the following URLs in your Web browser's Address field:

- `http://localhost/frame.htm`
- `http://name/frame.htm`
- `http://127.n.n.n/frame.htm`
- `http://n.n.n.n/frame.htm`

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 contact the MVAM application, you may need to specify `localhost/index.htm`.

Connecting to a remote MVAM installation

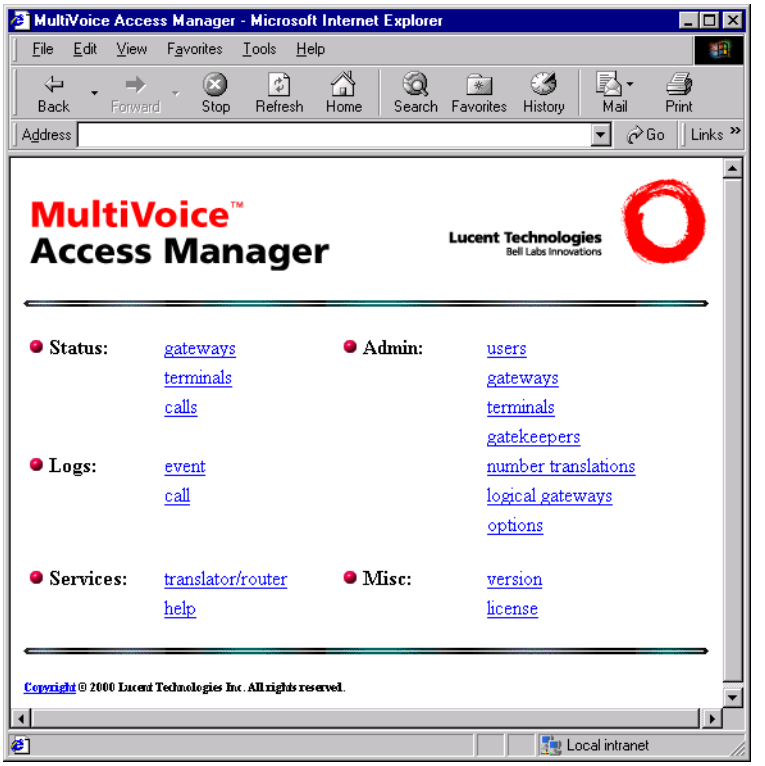
To access MVAM from a different computer, enter the hostname or IP address of the computer where MVAM is running in your Web browser's Address field. For example:

`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 main screen appears as illustrated in Figure 3-1:

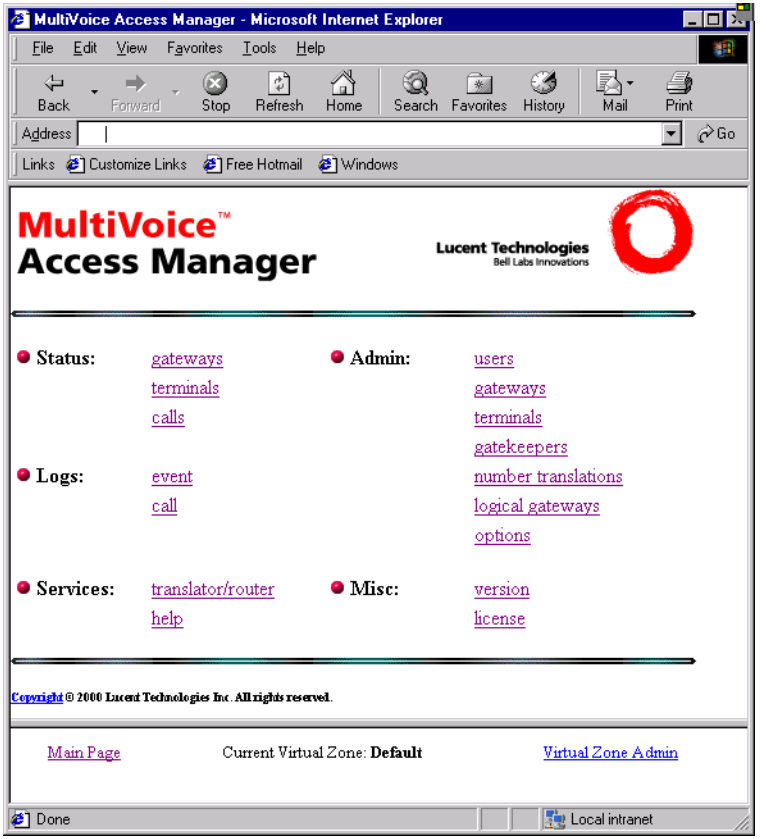
Figure 3-1. Access Manager main screen (default)



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

When your MVAM is configured to support Gatekeeper virtual zones, you may use the virtual zone main screen, as illustrated by Figure 3-2:

Figure 3-2. Access Manager virtual zone main screen



From this screen, you may administer and configure Gatekeeper options for the current virtual zone. You also access the Virtual Zone Admin menus from this screen. Those menus are used to configure and select the current virtual zone.

About on-line help

On-line help displays information about screens and their fields.

- Click a Help button (if present) to have MVAM display information about the current screen.

- Click an underlined field name to have MVAM display information about that option/entry.

To access the complete help system, click either:

- `Serivces: Help` on the MVAM main page
- The underlined text `Help Topics Index` on any on-line help screen

Control buttons

MultiVoice Access Manager forms, used for retrieving and editing database information, usually include a set of control buttons in the bottom left corner. When a form includes these buttons, they perform the following functions:



This button commits the information entered on the screen, writing it to the appropriate MultiVoice Access Manager database. On forms where existing information is modified, pressing this button will overwrite any existing database records with the modified information.



and



These buttons reset all the entries displayed on the screen to their original values. If fields were initially blank, the field is emptied of user-entered information. For all other fields, the original entries are displayed. These buttons will not undo changes already submitted to the Access Manager databases.



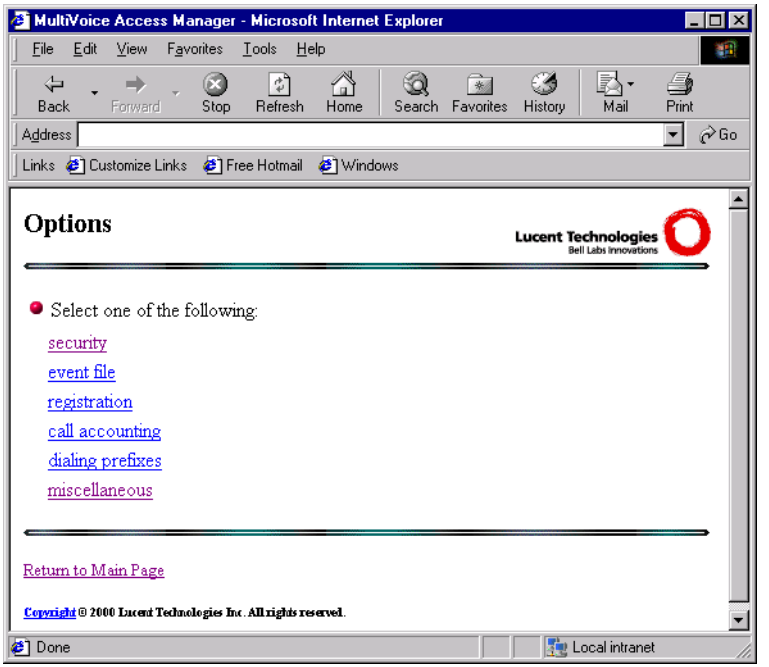
This button opens the help file for the current MultiVoice Access Manager form.

Configuring MVAM options

The Options form is used to set various MultiVoice Access Manager performance features. These options control how the Access Manager handles security, event

file creation frequency, registration, call accounting, dialing prefixes, and registration capacity for terminals, as illustrated in Figure 3-3:

Figure 3-3. MultiVoice Access Manager Options menu



Note: This menu is used to change values contained in the MultiVoice Access Manager initialization file. Changes made from these screens do not take effect until MVAM is stopped and re-started. See “Starting MVAM” on page 2-25, and “Stopping MVAM” on page 2-32.

These options include:

Option	Description
security	The Security Options form is used to select a method of caller authentication for the MultiVoice network, and controls admission of calls from H.323-compliant terminals. By default, MultiVoice does not require callers to authenticate themselves, and will connect calls from PCs to telephones.
event file	The Event File Options form is used to modify the frequency with which the MultiVoice Access Manager creates event files. MultiVoice Access Manager writes event records logging all system activity to a text file which may be created daily, weekly, or monthly.
registration	The Registration Options form is used to control MultiVoice Gateway and H.323 terminal registration. This includes enabling/disabling H.323 terminal registration and keep-alive registration, and both terminal and Gateway keep-alive registration time intervals.
call accounting	The Call Accounting Options form is used to modify the frequency with which the MultiVoice Access Manager creates call record files. Call records are written to text files which may be created daily, weekly, or monthly. Alternatively, call records may be kept in a single text file which is created only once.
dialing prefixes	The Modify Dialing Prefixes form is used to set the dialing prefixes for pass-through and alias dialing. These prefixes are used by the MultiVoice Access Manager to identify a dial string as a telephone alias or as a fully qualified telephone number. Alias dialing is not supported in a MultiVoice network.

Option	Description
miscellaneous	The Miscellaneous Options form is used to specify the Gatekeeper Identifier. The Gatekeeper Identifier field sets the basename of the Access Manager, which is used for Gatekeeper to Gatekeeper communications.

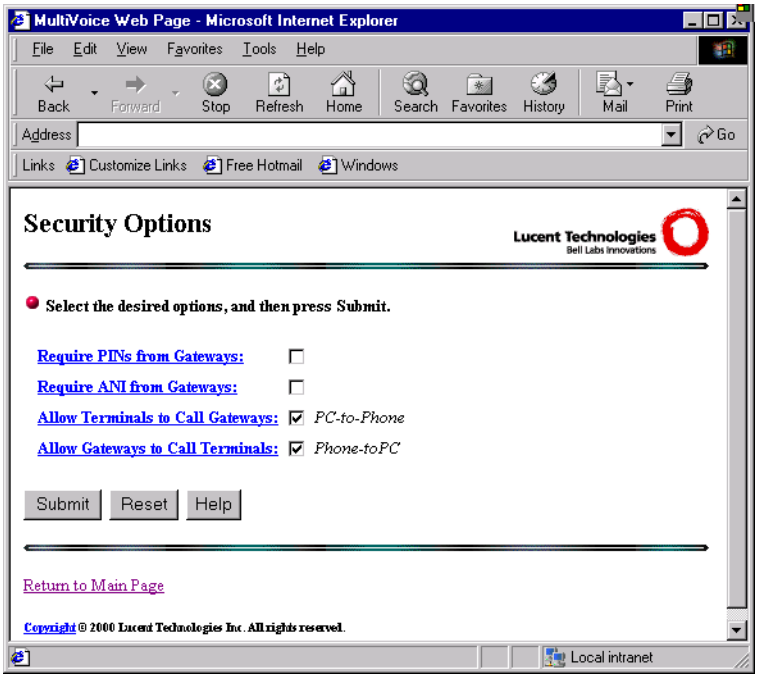
Configuring security

The Security Options form is used to control caller access to the MultiVoice network. By default, MultiVoice allows unauthenticated access for voice calls originating from the PSTN.

Using this form, illustrated in Figure 3-4, you may modify caller access by electing to enable or disable the PIN authentication, ANI authentication, PC-to-phone communication, and phone-to-PC communication.

By default, all Security Options are disabled. Click the checkbox next to the option you wish to enable/disable. In Figure 3-4, the Allow Terminals to Call Gateways option, and the Allow Gateways to Call Terminals options are enabled.

Figure 3-4. MultiVoice Access Manager Security Options form



Enabling the options on the Security Options form will:

Option	Description
Require PINs from Gateways[a]	Requires callers dialing in from the PSTN to authenticate by entering a Personal Identification Number (PIN) before the call is connected.
Require ANI from Gateways[a]	Requires the Access Manager to authenticate callers dialing in from the PSTN using the calling telephone's Automatic Number Identification (ANI) string before connecting the call.

Option	Description
Allow Terminals to Call Gateways	Allows the Access Manager to admit calls originating from H.323-compliant terminals, PCs, connected to the IP network. This allows PC-to-phone calls to be connected across the MultiVoice network.
Allow Gateways to Call Terminals	Allows the Access Manager to route calls originating from the PSTN to H.323-compliant terminals, PCs, connected to the IP network. This allows Phone-to-PC calls to be connected across the MultiVoice network.

[a.] You may configure PIN authentication, ANI authentication, or both.

You must re-start the Access Manager in order to apply changes made to these parameters. See “Starting MVAM” on page 2-25.

Configuring PIN authentication

Enabling PIN authentication requires callers to dial into a MultiVoice Gateway, then, after presenting callers with either a dial tone or prompts indicating that MVAM requires PIN authentication, they must enter a system-generated Personal Identification Number before allowing the call to be connected. (For more information, see “Call processing using PIN authentication” on page 3-12.)

To configure PIN authentication, proceed as follows:

1 From the MVAM main page, click `Admin: options` > `security`, to display the Security Options screen.

2 Click the `Require PINs from Gateways` check box.

3 Click the Submit button to save this setting.

Configuring ANI authentication

ANI authentication, when enabled, 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 the MultiVoice Access Manager. If the ANI matches the information in the user

database, MVAM continues with call setup. (For more information, see "Call processing using ANI authentication" on page 3-13.)

To require ANI authentication, proceed as follows:

1. From the MultiVoice Access Manager main page, click `Admin: options` > `security`, to display the Security Options screen.
2. Click the `Require ANI from Gateways` check box.
3. Click the Submit button to save this setting.

Note: If you are planning to use ANI authentication, the User Alias field in a user's record 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.

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

Call processing without using authentication

If you do not use call authentication, MVAM processes calls from the PSTN 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. MVAM 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.
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 MVAM. By default, this may take up 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.

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

Call processing using PIN authentication

If you configure PIN authentication, MVAM processes calls from the PSTN 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 MVAM 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. Once created, you may modify a user's PIN, if desired.

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 MVAM. By default, this may take up 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.

Call processing using 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 MVAM and passes the ANI and destination phone number to it.

6 MVAM compares the ANI to the User Alias information in the user database.

If the ANI does not match a User Alias, MVAM disconnects the caller.

7 If the ANI matches a User Alias, MVAM 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.

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.

To detect DNIS/ANI on Gateways using two stage dialing, set the values of Sig Mode and Collect DNIS/ANI in the Gateway's T1 profile as follows:

```
Net/T1
 Line Config
  <line>
   <line #>
    Sig Mode=Inband
    Rob Ctl=wink-inc-200 or wink-inc-400
    Collect DNIS/ANI=No
```

To detect DNIS/ANI on Gateways using single stage dialing, set the values of Sig Mode and Collect DNIS/ANI in the Gateway's T1 profile as follows:

```
Net/T1
 Line Config
  <line>
   <line #>
    Sig Mode=Inband
    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.

To detect DNIS/ANI on Gateways using R2 signaling, set the following values in the Gateway's E1 profile:

```
10-1** Factory
 Line 1...
 >Sig Mode=R2
  Switch Type=CAS
  Framing Mode=2DS
  # Complete=end-of-pulsing
  Grp B Answer Signal=B-6
  Grp B Busy Signal=B-3
  Grp B No Match Signal=B-7
  Grp II Signal=II-2
  Answer Delay=200
  Caller Id=N/A
  L3 End=N/A
  L2 End=N/A
  NL Value=N/A
```

```
LoopAvoidance=N/A
Clock Source=Yes
```

To detect DNIS/ANI on Gateways using E1/PRI signaling, set the following values in the Gateway's E1 profile:

```
10-1** Factory
 Line 1...
 >Sig Mode=ISDN
  Switch Type=Net5
  Framing Mode=2DS
  # Complete=N/A
  Grp B Answer Signal=N/A
  Grp B Busy Signal=N/A
  Grp B No Match Signal=N/A
  Grp II Signal=N/A
  Answer Delay=N/A
  Caller Id=N/A
  L3 End=N/A
  L2 End=N/A
  NL Value=N/A
  LoopAvoidance=N/A
  Clock Source=Yes
```

To detect DNIS/ANI on Gateways using E1/PRI signaling, set the following values in the Gateway's E1 profile:

```
Net/T1
 Line Config
  <line>
   <line #>
    Sig Mode=ISDN
```



Caution: If you elect to use both ANI and PIN authentication, both values must match a caller's user information. If either value is invalid, the call will be rejected.



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

Enabling PC-to-phone operations

An Access Manager may be configured to admit calls from networked PCs to dialed telephone numbers on the PSTN. This requires that terminals be allowed to initiate calls.

To enable this feature for a MultiVoice network, proceed as follows:

1 From the MVAM main page, click `Admin: options` > `security`, to display the Security Options screen.

2 Click the `Allow Terminals to call Gateways` checkbox.

3 Click the Submit button to save this setting.

Additional Configuration for PC-to-phone operations

In addition, you must also configure the following options on the Access Manager:

- Both PIN and ANI authentication must be disabled.
- You must enable the `Allow Terminals to Register` option on the Registration Options form. Calling terminals can register with Access Manager upon submission of an Admission Request (ARQ).
- You should disable the `Age Terminal Registration` option on the Registration Options form. This eliminates the need to have the PC perform keep-alive registration with MVAM. Once MVAM acknowledges the call request, the PC remains registered.

These other parameters which control PC-to-phone operations are changed by editing the initialization file, `mvam.ini`. Changes to these parameters are applied by stopping and restarting MVAM. See “Starting MVAM” on page 2-25, and “Stopping MVAM” on page 2-32.

- 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 (ACF) 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 (ACF) message sent to the MultiVoice Gateway that connects the call.

- `ignoreTerminalDrqs` and `ignoreTerminalBrqs` should be enabled, the default setting for these parameters. When set, MVAM ignores Drop Request messages (DRQs) and Bandwidth Request messages (BRQs) received from H.323 compliant terminals.

Enabling PC-to-phone operations

An Access Manager will eventually support call routing from telephones on the PSTN to networked PCs, over a MultiVoice Network. Currently, this feature is not supported.

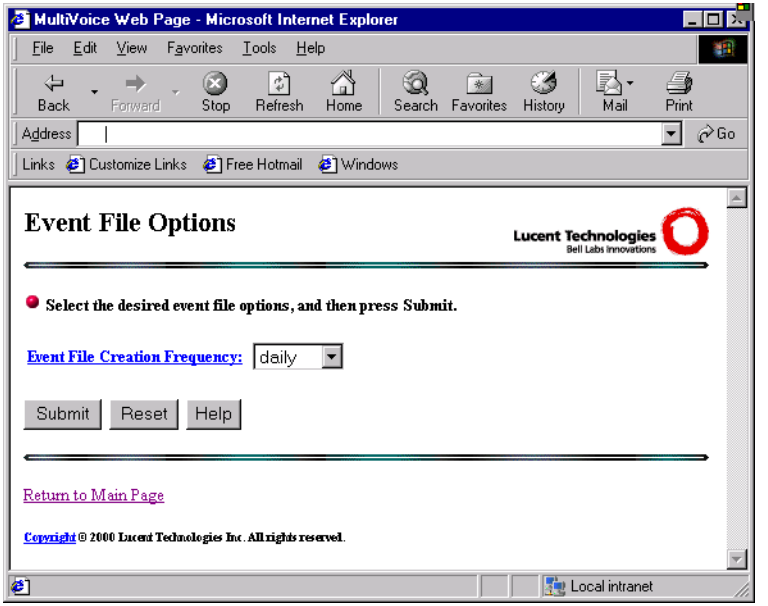
Configuring event log generation

MultiVoice Access Manager writes event records to a text file which may be created on daily, weekly, or monthly basis. Alternatively, event records may be kept in a single text file which is created once.

MVAM maintains an event log and call logs. The event log contains a running list of processes performed by the Access Manager. Call logs are text files, containing start, stop, and incomplete records for each call, which you can retrieve to generate customer billings.

Event log creation, or “rollover” is set from the Event File Options screen, as illustrated by Figure 3-5:

Figure 3-5. Event File Options screen



You set the log file creation frequency by selecting the desired time interval from the pull-down list for `Event File Creation Frequency`. Daily is the default frequency.

To set the log file creation interval, proceed as follows:

1 From the MVAM main page, click `Admin: options` > `security`, to display the Security Options screen.

2 Click the arrow to open the pull-down list for the `Event File Creation Frequency` field, and click a file generation interval.

The following conventions apply:

– A new day starts at midnight.

– A new week starts on Sunday.

– A new month starts on the first day of month.

3 Click the Submit button to save this setting.

Configuring Registration

The Registration Options form, as illustrated by Figure 3-6, is used to set registration policy for MultiVoice Gateways and PC terminals. This includes setting registration permissions for PC terminals, keep-alive registration intervals, and registration response margins. By default, MVAM supports registration, initial and keep-alive, with both Gateways and PC terminals.

Figure 3-6. Registration Options form



MultiVoice allows you to modify registration policy by setting the following:

Option	Description
Allow Terminals to Register	When selected (default), the Gatekeeper will allow H.323-compliant terminals to register when it initiates a PC-to-phone call.
Age Terminal Registration	When selected (default), the initial registration between the Gatekeeper and an H.323-compliant terminal will expire after a preset time limit.
Terminal Registration Period	This sets the time interval, in seconds, at which an H.323-compliant terminal must perform keep-alive registration with the Gatekeeper, following its initial registration. Default value is 120 seconds.
Gateway Registration Period	This sets the time interval, in seconds, at which a MultiVoice Gateway must perform keep-alive registration with the Gatekeeper, following its initial registration. Default value is 120 seconds.
Registration Period Margin	This sets a buffer, in seconds, which the Gatekeeper waits for a Gateway or PC terminal to complete a keep-alive registration attempt. This is designed to reduce the frequency of expired registrations. Default value is 30 seconds.

Enable terminal registration

To process VoIP calls originating from H.323-compliant terminals (PCs), MVAM must allow PCs to register with the Gatekeeper. Since the Access Manager does not maintain databases with PC endpoints, registration cannot occur before a call request is received.

Enabling the `Allow Terminals to Register` option, PCs may register with the Gatekeeper when they submit a call admission request (ARQ). When

enabled, a PC terminal will register with the Gatekeeper, signalling that it is "alive" when it initiates a call request. It then will periodically re-register, if the `Age Terminal Registration` option is also enabled, until the call disconnects.

To enable terminal registration, proceed as follows:

1. From the MVAM main page, click `Admin: options` > `registration`, to display the Registration Options screen.
2. Click the `Allow Terminal Registration` checkbox. If the check mark appears in the box, this feature is enabled.
3. Click the Submit button to save this setting.

Aging terminal registration

Registered H.323-compliant terminals (PCs) may be required to perform keep alive registration with the Gatekeeper. Since the Access Manager does not maintain databases with PC endpoints, registration cannot occur before a call request is received.

The `Allow Terminals to Register` option lets PCs register with a Gatekeeper when they submit a call admission request (ARQ). When enabled, a PC terminal will register with the Gatekeeper, signalling that it is "alive" when it initiates a call request. It then will periodically re-register, if the `Age Terminal Registration` option is also enabled, until the call disconnects.

To enable terminal registration, proceed as follows:

1. From the MVAM main page, click `Admin: options` > `registration`, to display the Registration Options screen.
2. Click the `Allow Terminal Registration` checkbox. If the check mark appears in the box, this feature is enabled.
3. Click the Submit button to save this setting.

Setting keep alive registration time intervals

Keep alive registration is a way of communicating to MVAM that a Gateway or PC is still "alive", that is, working and available to connect calls. The keep alive registration time interval is the time MVAM waits for a Gateway or PC to send

subsequent registration messages after initial registration. This establishes a re-registration schedule which:

- For Gateways, continues from the time of initial registration until that Gateway can no longer communicate with a Gatekeeper,
- For terminals (PCs), continues from the time of initial registration until the active call connection for that PC is terminated.

Setting the terminal registration period

To connect VoIP calls, H.323-compliant terminals (PCs) must register themselves with a Gatekeeper when submitting a call request. If you checked the box for the `Age Terminal Registration` option, active PCs must also send the Gatekeeper registration requests at regular intervals, for the duration of the VoIP call. This keep alive registration time interval must be set at the Gateway and sent as part of the call setup instructions to the PC.

This keep alive registration time interval for PCs is set on the Gatekeeper from the Registration Options screen, by changing the value entered in the `Terminal Registration Period` field.

To change the keep alive registration time interval for registered terminals, proceed as follows:

1 From the MVAM main page, click `Admin: options` > `registration`, to display the Registration Options screen.

2 Highlight the entry for the `Terminal Registration Period` field, and enter the time interval, in seconds, the Gatekeeper will wait between terminal keep alive registrations.

3 Click the Submit button to save this setting.

Setting the Gateway registration period

To be available to connect VoIP calls, MultiVoice Gateways must register themselves with a Gatekeeper, and periodically re-register at regular intervals. Active MultiVoice Gateways keep in constant contact with the MVAM by sending registration requests at regular intervals. This keep alive registration time interval must be set on both the Gateway and the Gatekeeper.

To change the keep alive registration time interval on a MultiVoice Gateway, edit the Ethernet > Mod Config > VOIP Options > Keepalive Timer parameter, specifying the time, in seconds, to wait between registration requests.

The keep alive registration time interval is set on the Gatekeeper using the Registration Options screen, by changing the value entered in the `Gateway Registration Period` field.

To change the keep alive registration time interval on a Gatekeeper, proceed as follows:

1. From the MVAM main page, click `Admin: options` > `registration`, to display the Registration Options screen.
2. Highlight the entry for the `Gateway Registration Period` field, and enter the time interval, in seconds, the Gatekeeper will wait between Gateway keep alive registrations.
3. Click the Submit button to save this setting.

Setting the registration grace period

To reduce the likelihood of a Gateway or terminal becoming unregistered, MVAM allows you to establish a re-registration grace period, adding time to the interval between registrations. This grace period is intended to reduce the frequency with which a Gateway or terminal become unregistered as a result of delays caused by network traffic, packet loss or collisions, etc., by allowing a extra time for endpoints to complete registration.

This registration grace period is set on the Gatekeeper using the Registration Options screen, by changing the value entered in the `Registration Period Margin` field.

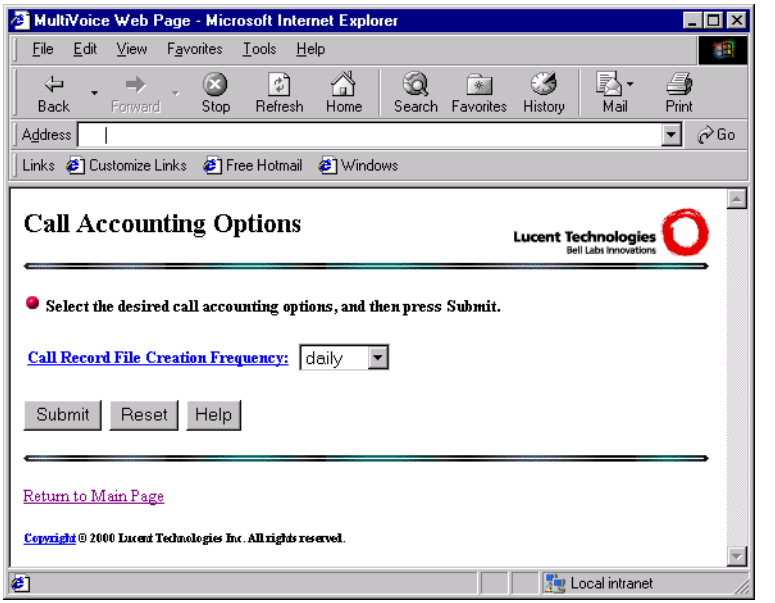
To adjust this registration grace period on a Gatekeeper, proceed as follows:

1. From the MVAM main page, click `Admin: options` > `registration`, to display the Registration Options screen.
2. Highlight the entry for the `Registration Period Margin` field, and enter the time interval, in seconds, the Gatekeeper will wait between Gateway keep alive registrations.
3. Click the Submit button to save this setting.

Setting call accounting options

Call logs are text files containing start, stop, and incomplete records for each call. Use the Call Accounting Options form to specify whether the MVAM maintains a continuous call log or creates call logs on a daily, weekly, or monthly basis. The data in the call logs is comma delimited; you can parse it to produce billing records.

Figure 3-7. Call Accounting Options form



To set call-log frequency:

1. From the MVAM main page, click `Admin: options` > `call accounting`, to display the Registration Options screen.
2. On the right side of the `call record file creation frequency` field, click the Down arrow to display available selections.
3. Select a value.

4 Click the Submit button to save this setting.

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

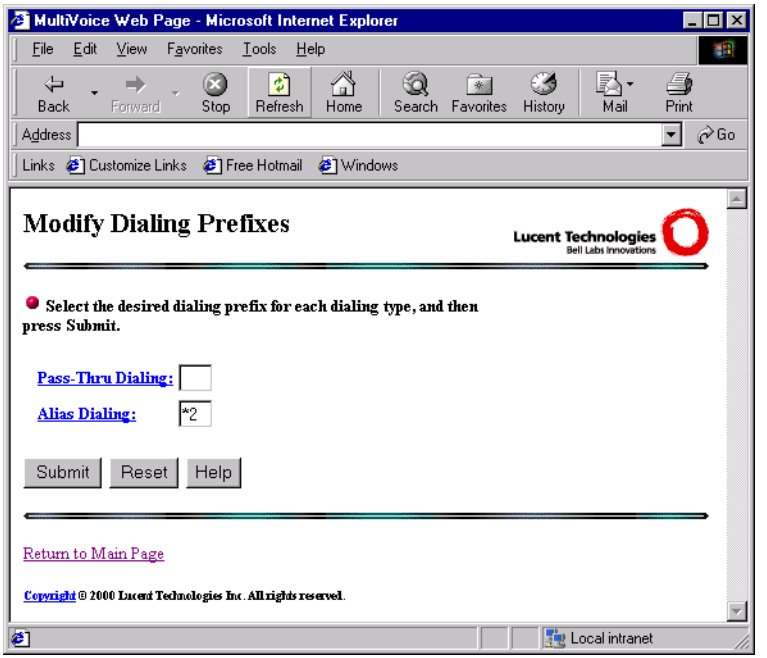
Modifying dialing prefixes

Note: Alias dialing is not supported in a MultiVoice network.

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

Use the Modify Dialing Prefixes form, illustrated in Figure 3-8, to assign dialing prefixes that MVAM uses to differentiate between dialed telephone aliases and actual dialed telephone numbers.

Figure 3-8. Modify Dialing Prefixes form



Modify the dialing prefixes used by the Gatekeeper by setting the following:

Option	Description
Pass-Thru Dialing	The Pass-Thru Dialing prefix is a two-digit code which tells the MultiVoice Access Manager that the dialed string which follows is a complete telephone number, requiring no alias number translation prior to connecting the call. This may be a two-character string consisting of an asterisk (*) followed by any number from 1 to 9. By default, this parameter has no assigned value.
Alias Dialing	The Alias Dialing prefix is a two-digit code which tells the MultiVoice Access Manager that the dialed string which follows is a telephone alias, which must be converted to a complete telephone number prior to connecting the call. This may be a two-character string consisting of an asterisk (*) followed by any number from 1 to 9. By default, this parameter has an assigned value of `*2`.

Configuring dialing prefixes

To configure a dialing prefix:

1. From the MVAM main page, click `Admin: options > dialing prefixes` to display the Modifying Dialing Prefixes screen.
2. Set Pass-Thru Dialing to the dialing prefix that callers use to indicate to MVAM that it should dial the phone number as entered (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. Click the Submit button to save this setting.

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.

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.

Configuring Gatekeeper virtual zones

This feature allows a single Access Manager to manage multiple, separate H.323 zones. This feature is referred to as Virtual Zones, or Gatekeeper virtual zones. For example, a single Access Manager may have individual zones for Ford, GM, and Chrysler. Data for each Gatekeeper virtual zone, such as user, gateway, coverage areas, and call record databases, are separate and distinct.

Definition of an Access Manager (Gatekeeper) virtual zone

A Gatekeeper virtual zone is a subset of all MultiVoice Gateways which are administered and registered with a single MultiVoice Access Manager. Each virtual zone is managed by a virtual Gatekeeper which exists on the same server as the Access Manager. Each virtual Gatekeeper has its own set of distinct Gateway, Gatekeeper, and user databases, which are separate and distinct from other databases maintained for the Access Manager itself, or other virtual Gatekeepers which exist on the same server.

Call routing using virtual zones

When using Gatekeeper virtual zones, calls are processed through a single Access Manager as if it were different Gatekeepers. Each virtual zone functions as an independent Gatekeeper. A call received by Gateways administered through one virtual zone are routed accordingly:

- The call is routed through another Gateway within the same virtual zone.
- The call is routed through a Gateway within another virtual zone.

If the Access Manager is also setup to perform multi-zone operations (real Gatekeeper-to-Gatekeeper communications), a call received by Gateways administered through one virtual zone are routed accordingly:

- The call is routed through another Gateway within the same virtual zone.
- The call is routed through a Gateway within:
  - another Gatekeeper virtual zone on the same server.
  - a zone administered by a remote Access Manager.
  - another Gatekeeper virtual zone on a remote Access Manager.

Each Gatekeeper virtual zone has a database of known peer Gatekeepers. Each entry in this database contains a Gatekeeper's identifier (that is, a unique name) and its IP address.

Each virtual zone on an Access Manager also has a database of known Gatekeeper inclusion areas. These inclusion areas define the telephone numbers that a virtual zone is responsible for covering. Overlapping coverage areas are also supported for virtual zones.

VIrtual zone call processing

When a Gateway requests call routing, the Gatekeeper virtual zone first determines if the call can be routed to a Gateway within its own zone. If the call can not be routed within its zone:

1 The known Gatekeeper database is checked, to determine if the coverage area is supported by a remote Gatekeeper or another virtual zone.

2 If a covering Gatekeeper is located, a Location Request (LRQ) message is sent to the covering Gatekeeper (i.e., virtual zone or remote Access Manager).

3 The covering Gatekeeper determines if it has a covering Gateway.

4 If a covering Gateway is available, the covering Gatekeeper responds with a Location Confirmed (LCF) message containing the IP address of the covering Gateway.

While waiting for the covering Gatekeeper to respond, the Gatekeeper virtual zone sends a Request-In-Progress (RIP) message to the originating Gateway.

5 Once the Location Confirmed (LCF) message is received from the covering Gatekeeper, an Admission Confirmed (ACF) message containing the conferenceId is sent to the calling endpoint.

6 The destination Gateway completes the call.

If the covering Gatekeeper determines it does not have a covering Gateway, it returns a Location Reject (LRJ) message.

While waiting for the covering Gatekeeper to respond with Gateway information, the Gatekeeper virtual zone generates pointers to a potential ACF message, and the LRQ message in the Active Call Table, and returns without generating an ACF or an ARJ. The LRQ message has the conferenceIdentifier for the call in its nonStandardData parameter, and the covering Gatekeeper returns this in the nonStandardData parameter of the LCF or LRJ message.

Virtual zone support files

A Gatekeeper virtual zone database list, `zone.txt`, is located in the Access Manager database directory (i.e., c:\mvam\db or /opt/mvam/db). This file, which is read at startup, points to configuration information for all virtual zones. For example: `NJ_Newark,/opt/mvam/allzones/NJ_Newark`. It will always have, minimally, one record of the form "`,c:\mvam`"—representing the default Gatekeeper virtual zone, the Access Manager itself.

This file contains records that are made up from two comma-separated fields:

Parameter	**Description**
zone name (i.e., NJ_Newark)	This is the name/Gatekeeper ID assigned to a virtual zone.
zone directory (i.e., /opt/mvam/allzones/NJ_Newark)	This is the directory which contains all the zone-specific database and configuration files (i.e., Gateway and user databases, Gateway coverage areas, current call logs, etc.).

Following example are sample entries found in the zone.txt file:

```
,c:\mvam
NJ_Newark,c:mvam\allzones\NJ_Newark
```

In this example, the user created virtual zone named `NJ_Newark` on the Access Manager, and stored this virtual zone configuration in `c:\mvam\allzones\NJ_Newark`. The zone.txt file will always include the entry `c:\mvam`. This identifies the default virtual zone.

Virtual zone configuration files and parameters

As virtual zones are added to an Access Manager, new directories and files are created that hold the zones' data. These are stored under the /opt/mvam/allzone or c:\mvam\allzones directories. For example: the directory `c:\mvam\allzones\Chrysler` will contain a zone specific `mvam.ini`, a \db subdirectory, a \calls directory and an \nxts directory.

Gatekeeper databases

For virtual zone call routing to work, each Gatekeeper virtual zone must know about the other real and logical Gatekeepers on the network, and their respective coverage areas. This information is stored in the Gatekeeper table and Gatekeeper coverage table.

The Gatekeeper table (`gk.txt`) stores the Gatekeeper identifier, usually a combination of the network name of the Access Manager server and the virtual zone identifier, and the IP addresses of peer Gatekeepers. The parameters used to identify Gatekeepers in this file must meet the following criteria:

Parameter	Type	Unique	Mandatory
Gatekeeper Identifier	NAME	yes	yes
Gatekeeper IP Address	IP	no[a]	yes

a. The same IP address may be used for more than one Gatekeeper Identifier, if the Access Manager at that IP address is configured to support virtual-zone call routing. Then more than one virtual Gatekeeper would be associated with an IP address.

A Gatekeeper Identifier may be either of the following:

Value	Description
gkID	This is the name by which the Access Manager is known to the MultiVoice network. This is usually the same as the network name of the system where the Access Manager is installed.
gkID.zone	This identifies a Gatekeeper virtual zone. This consists of the Access Manager name and a zone name which exists on that Access Manager.

The Gatekeeper coverage table, `gkc.txt`, stores the coverage information for the known Gatekeepers. The parameters used in this file must meet the following criteria:

Parameter	Type	Unique	Mandatory
Gatekeeper Identifier	NAME	yes	yes
Coverage Area	STRING(s)	yes[a]	no

a. The same rules concerning the size and formatting of Gateway coverage areas are applied to these Gatekeeper coverage areas.

The database files, `gk.txt` and `gkc.txt`, may be populated on one Access Manager/virtual zone and then manually copied to other virtual zones.

Mvam.ini

Each zone has its own mvam.ini file, which contains certain zone specific [Sections]/Parameters that override values within the main mvam.ini file. They are as follows:

Parameter	Description
[Gwt]file	This parameter points to the virtual zone-specific Gateway database, `zone/db/gw.txt`

Parameter	Description
[Gwct]file	This parameter points to the virtual zone-specific Gateway coverage area database, `zone/db/gwc.txt`
[Gkt]file	This parameter points to the virtual zone-specific known Gatekeeper database, `zone/db/gk.txt`
[Gkct]file	This parameter points to the virtual zone-specific Gatekeeper coverage area database, `zone/db/gkc.txt`
[UtText]file	This parameter points to the virtual zone-specific user database, `zone/db/user.txt`
[Act]frequency	This parameter sets rollover, or refresh interval, for the virtual zone specific call log (defaults to daily).
[Act]filePath	This parameter points to the virtual zone-specific call log directory, `zone/calls/`
[Sec]proxyPinRequired	This parameter enables/disables PIN authentication for calls initiated through this virtual zone (defaults to 0).
[Sec]aniRequired	This parameter enables/disables ANI authentication for calls initiated through this virtual zone (defaults to 0).
[Sec]allowPcToPhone	This parameter enables/disables this virtual zone to accept calls originating from PC terminals (defaults to 1).
[Sec]allowPhoneToPc	This parameter enables/disables this virtual zone to accept calls placed to PC terminals (defaults to 0).
[Prefixer]passThruPrefix	This parameter is a two-place pass-through dialing prefix for calls initiated through this virtual zone. By default this parameter has no assigned value.

Parameter	Description
[Prefixer]aliasPrefix	This parameter is a two-place alias dialing prefix for calls initiated through this virtual zone (defaults to *2). **Note:** Alias dialing is not supported in a MultiVoice network.
[Nxtl]file	This parameter points to the virtual zone-specific number translation table list, `zone/db/nxtl.txt`
[Nxtl]nxtPath	This parameter points to the virtual zone-specific number translation table directory, `zone/db/nxts/`
[Tt]nxtIn	This parameter points to the virtual zone-specific inbound number translation table, `zone/db/nxts/gw_in.txt`. By default this parameter has no assigned value.

Virtual zone database files and directories

The /db directory will contain zone-specific copies of the following Access Manager database files. This structure mimics the base Access Manager directory structure, with the exception of the zone-specific overrides coming from the named zone's own `mvam.ini` file:

Database	Description
`user.txt`	This is the user database file for the named virtual zone.
`gw.txt`	This is the Gateway database file for the named virtual zone.
`gwc.txt`	This is the Gateway coverage area database file for the named virtual zone.
`nxtl.txt`	This is the list of number translation tables for the named virtual zone.

Database	Description
`gk.txt`	This is the Gatekeeper database file for the named virtual zone.
`gkc.txt`	This is the Gatekeeper coverage area database file for the named virtual zone.
`/nxts` (directory)	This directory contains the number translation tables (files) for the named virtual zone.
`/calls` (directory)	This directory contains the subdirectory `/current`, where the current call log is maintained for this named virtual zone.

Using virtual zones

The Access Manager's Web-based interface allows users to choose whether the Gatekeeper will operate in either virtual- or single-zone mode. This is accomplished through the use of HTML frames. Customers wishing to use virtual zones can configure their http server to provide the `frame.htm` page as the default MultiVoice Access Manager page. Alternatively, the user may specify the URL which points directly to `frame.htm` on the Access Manager server, `http://222.22.22.22/frame.htm`, to enable this feature.

Customers wishing to perform single H.323 zone administration should configure `index.htm`, the traditional MultiVoice Access Manager page, as the default.

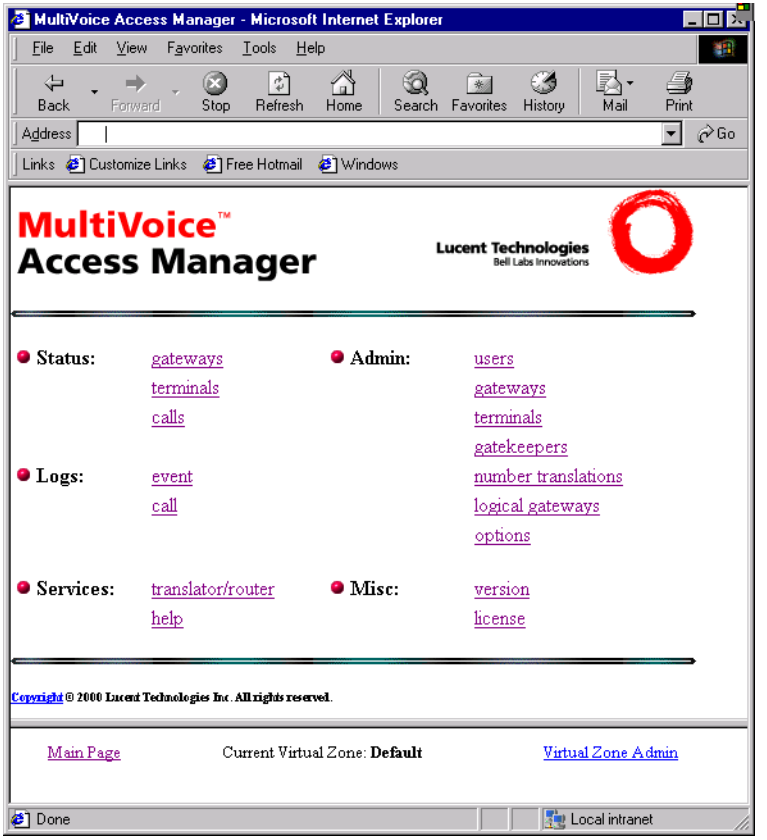
Virtual zone main page (frame.htm)

The Access Manager's virtual zone main page is divided into two frames:

- An administration frame
- A virtual zone management frame.

Figure 3-9 is an example of a typical virtual zone main page.

Figure 3-9. Virtual zone main page



The upper frame, the larger of these frames, is the MultiVoice Access Manager administration frame. It is large enough to hold the traditional MultiVoice Access Manager main page, with all the links to the Access Manager's administration HTML pages. All pre-existing MultiVoice Access Manager navigation and data manipulation is performed in the upper frame for the selected zone.

The lower frame is the virtual zone management frame. Hyperlinks in this frame are used to create and select virtual zones on the Access Manager. These include:

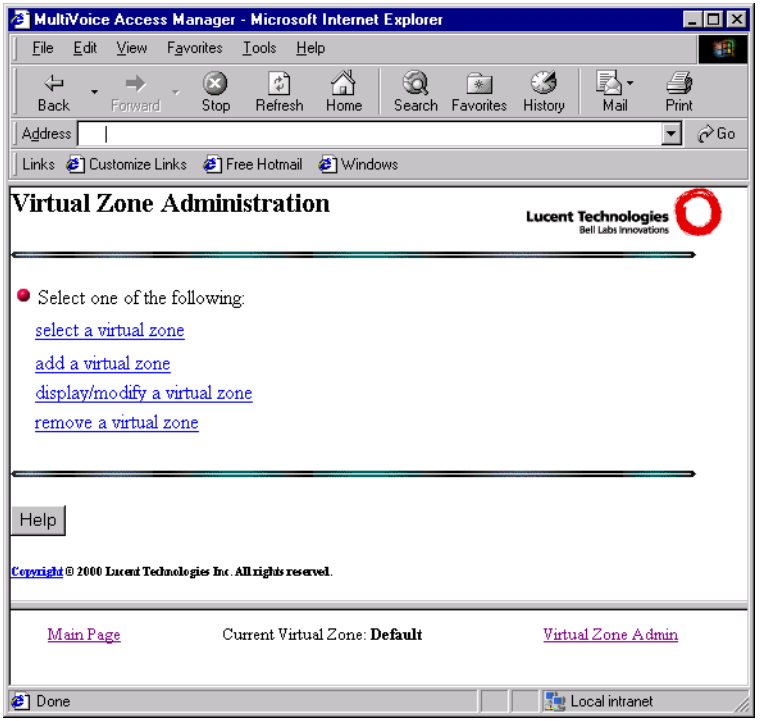
Option	Description
Main Page	This link takes a user back to the top of the MultiVoice Access Manager menu hierarchy from any MultiVoice administration page.
Current Virtual Zone	This displays the name of the current virtual zone. In Figure 3-9, the current virtual zone is Default, indicating that all administration that will be performed is for the Access Manager itself.
Virtual Zone Admin	Selecting this link opens the Virtual Zone Administration page, which contains links for selecting, creating, modifying, displaying, and removing zones.

Virtual zone administration

With the addition of this feature, we now have the Virtual Zone Administration page, which is shown in Figure 3-10. This page is accessed by selecting the Virtual Zone Admin link in the lower frame. On this page, you will find the following new links:

- select a virtual zone
- add a virtual zone
- display/modify a virtual zone
- remove a virtual zone

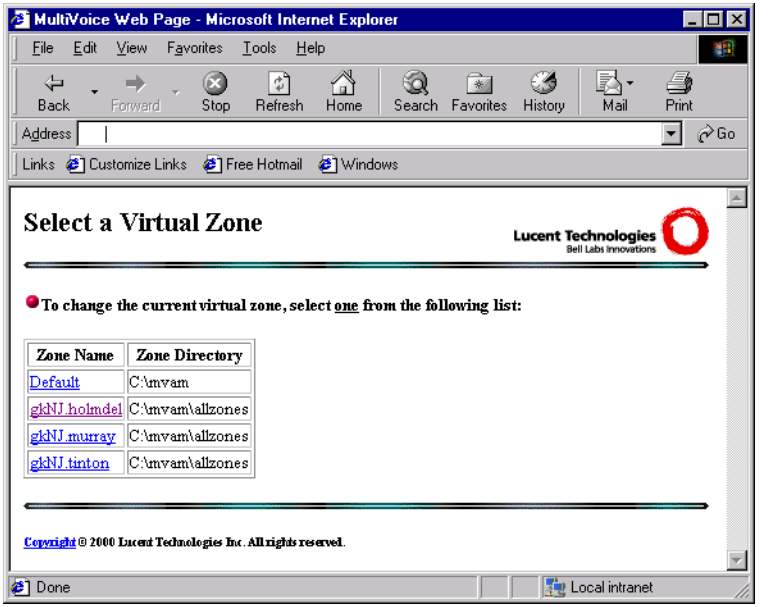
Figure 3-10. Virtual Zone Administration page



Select a virtual zone

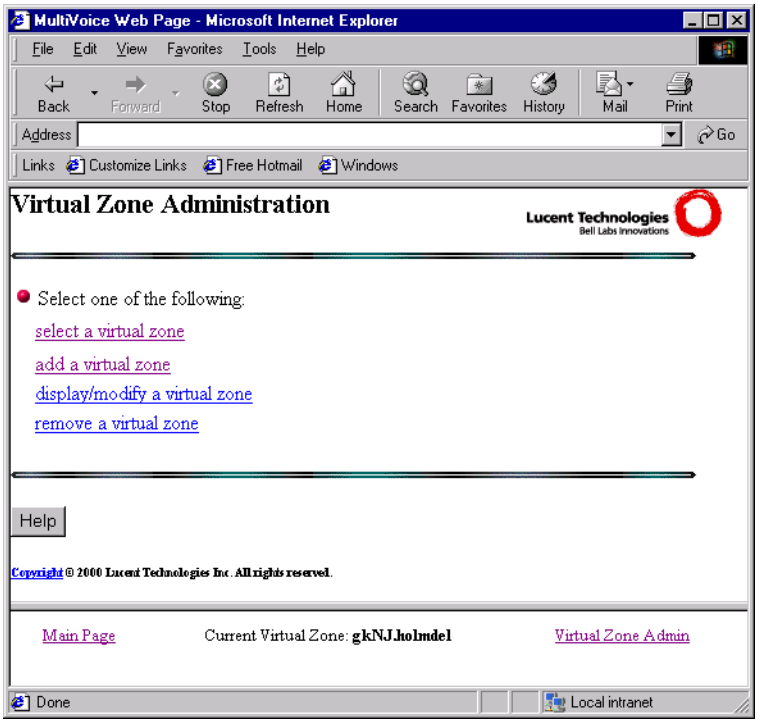
When selected, the Select a Virtual Zone link, displays a table of all the administered virtual zones, as shown in Figure 3-11. Within that table, each virtual zone name is a link which allows the MultiVoice administrator to select that virtual zone.

Figure 3-11. Select a Virtual Zone page



Once a virtual zone is selected, the Access Manager returns to the top of the MultiVoice Access Manager menu hierarchy. All subsequent Gatekeeper administration activity is applied to the selected zone. This name of the current virtual zone is displayed in the lower frame, as illustrated in Figure 3-12:

Figure 3-12. Virtual Zone Administration page for selected virtual zone



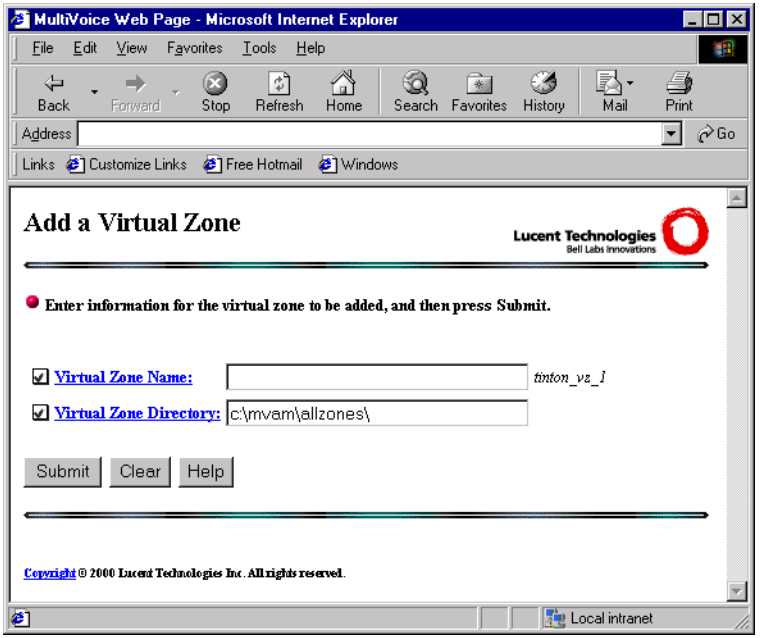
When a virtual zone is changed, all subsequent edits to users, Gateways, Gateway coverage areas, etc. will occur within and for that zone.

Note: ADMA rules (Rules, RuleSets, Gateway/Trunk Rules) are configured at the MVAM level and and are seen in every virtual zone.

Add a virtual zone

When selected, the Add a Virtual Zone link displays a form where the MultiVoice administrator may create new virtual zones, as shown in Figure 3-13.

Figure 3-13. Add a Virtual Zone page

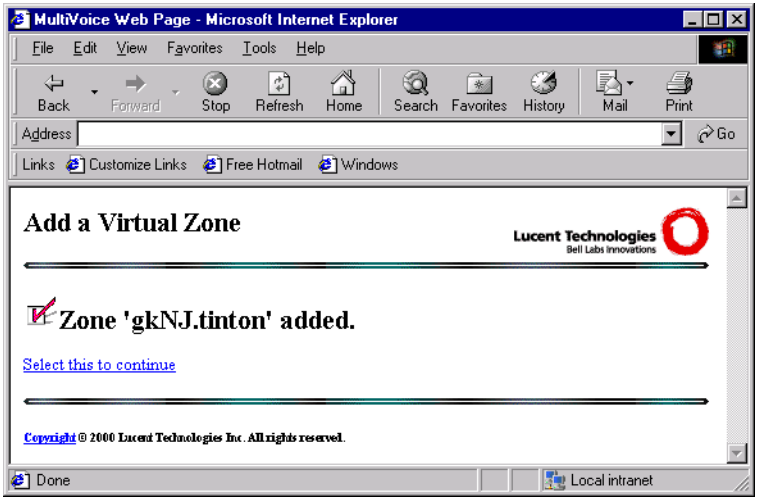


To create a virtual zone, enter the following information on this form:

Parameter	Description
Virtual Zone Name	This is an alpha-numeric string which is the Gatekeeper Identifier for this virtual zone. By default, this field is blank. The virtual zone name consists of the Access Manager name and a zone name which exists on that Access Manager.
Virtual Zone Directory	This field displays the default root directory for all new zones. All the zone-specific database and configuration files are stored in this location. The default value for this field is defined in the system mvam.ini file, `[Zt]:rootForZones`.

Click the Submit button to create the new virtual zone. After the Gateways are added to the Gateways database, a confirmation message displays, as shown in Figure 3-14.

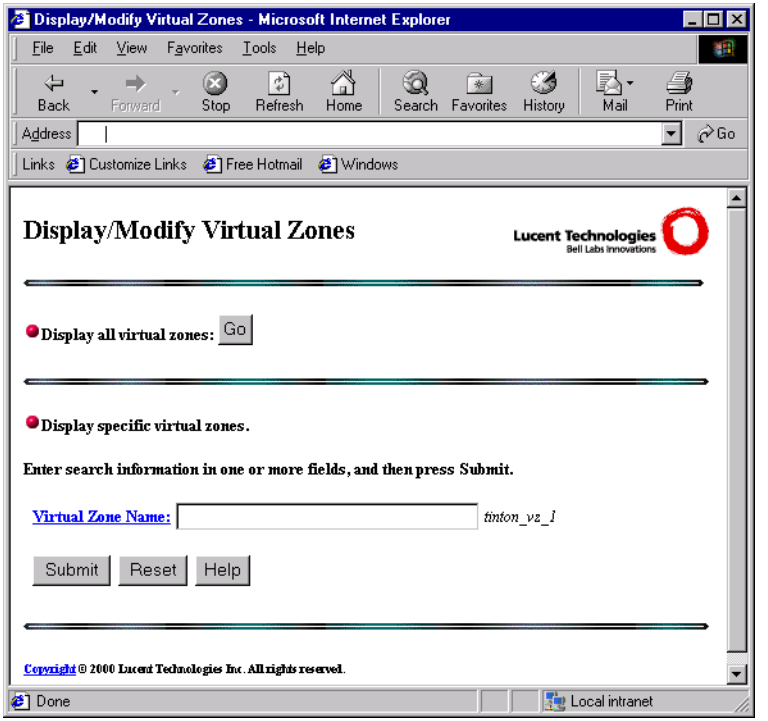
Figure 3-14. Successful addition of Virtual Zone



Display/modify virtual zones

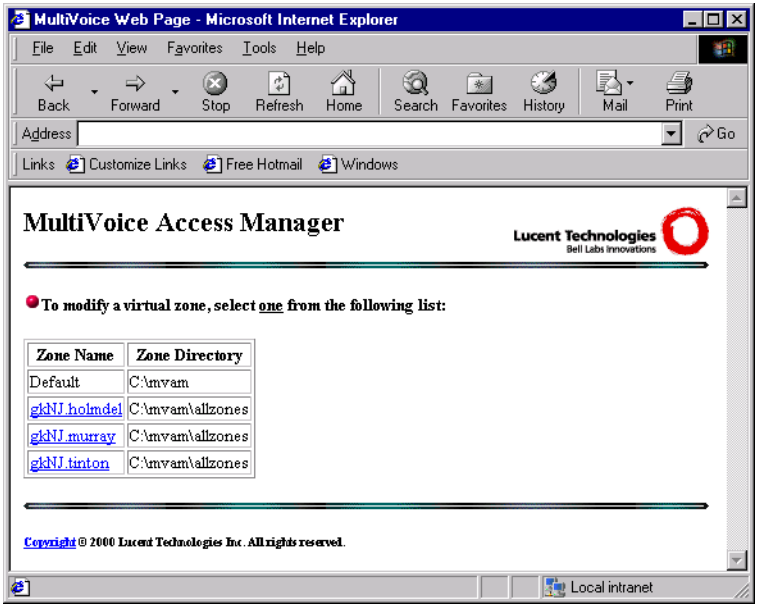
When selected, the Display/Modify A Virtual Zone link displays a virtual zone selection page as in Figure 3-15 below. From here the MultiVoice administrator enters a virtual zone name or displays a table of virtual zones configured for this Access Manager. When selecting from the table, the MultiVoice administrator clicks a name within that table, displaying information about the virtual zone on the Modify a Virtual Zone page.

Figure 3-15. Display/Modify Virtual Zones page



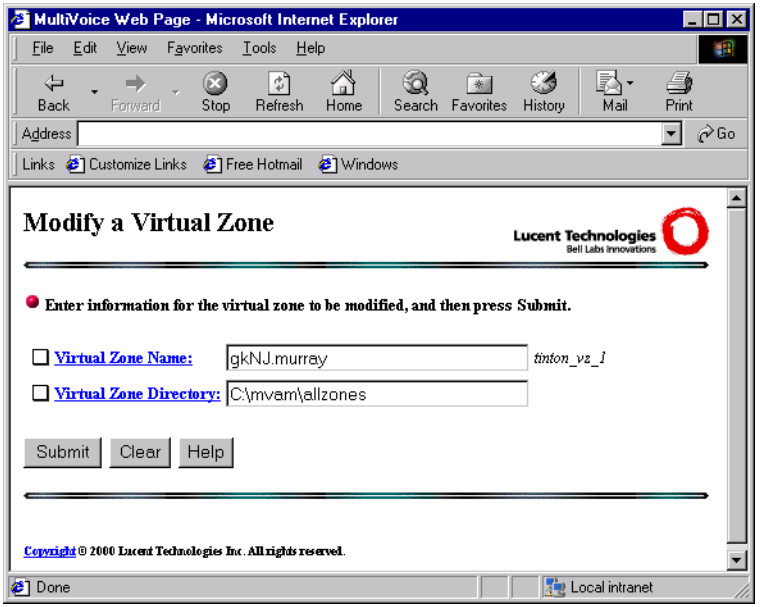
Enter the virtual zone name and click the Submit button to display information for a specific virtual zone; or click the Go button to display a list of all virtual zones configured on the Access Manager, as illustrated in Figure 3-16:

Figure 3-16. Select a virtual zone to modify



Once a virtual zone is selected, a virtual zone modification page, similar to Figure 3-17 appears.

Figure 3-17. Modify a Virtual Zone page

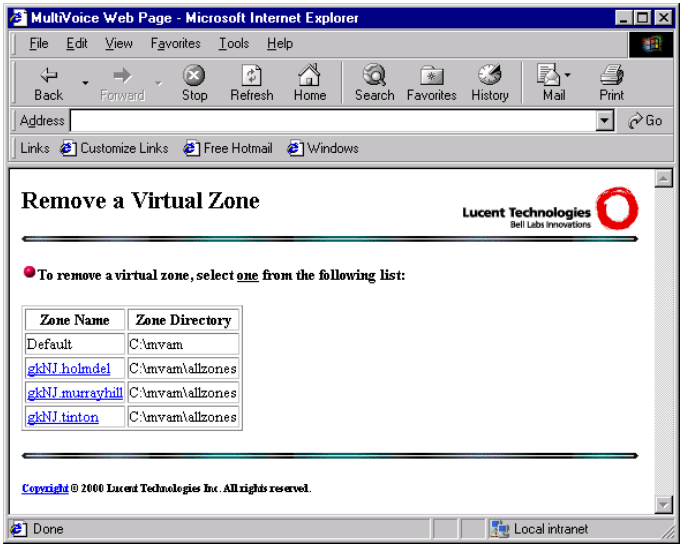


Enter changes for the virtual zone on this page then click the Submit button. A confirmation message will display the changes made.

Remove a virtual zone

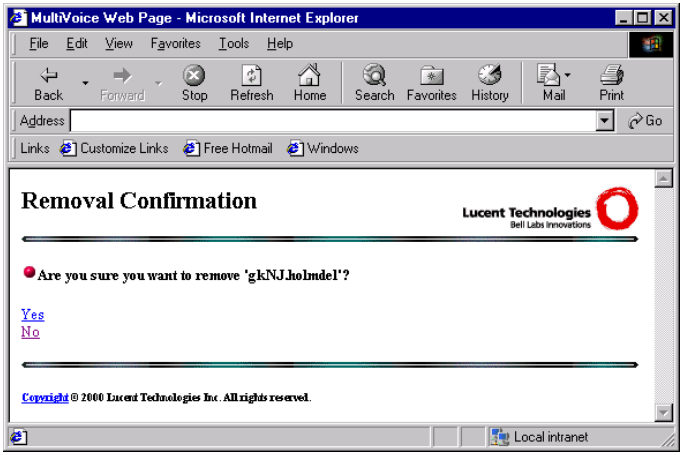
When selected, the Remove a Virtual Zone link displays a table containing all the administered virtual zones. Within that table, each zone name is a link which, when selected, allows the MultiVoice administrator to remove the selected virtual zone.

Figure 3-18. Remove a Virtual Zone page



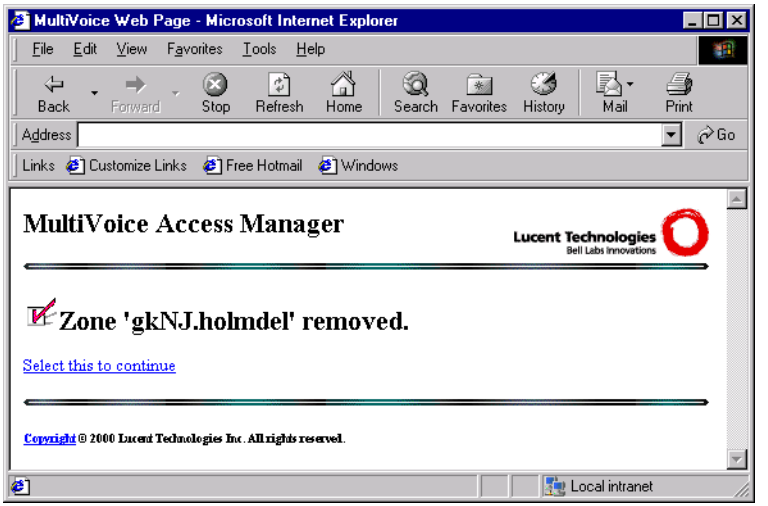
Once a virtual zone is selected, the Access Manager prompts for confirmation of the removal request, as illustrated in Figure 3-19:

Figure 3-19. Removal Confirmation of a virtual zone



When the request is confirmed, a message similar to Figure 3-20 is displayed and all information pertaining to the selected virtual zone is purged from the system.

Figure 3-20. Successful removal of a virtual zone



Note: All zones can be removed except the “Default” zone. The Default zone contains the base MultiVoice Access Manager configuration and databases, which were created when the application was installed.

Changes to the Integrated Event Log:

When the MultiVoice Access Manager is initialized, it displays a real-time event log in the MultiVoice Access Manager Interface screen. This event log displays each event as it occurs. System components and events that are zone specific are displayed with their respective virtual zone names as a suffix to that entry (for example, `Event(Zone)`). For example, the real-time event log would display components and events associated with the Chrysler zone, as follows:

```
Act(Chrysler)
Gwct(Chrysler)
Gwt(Chrysler)
Locator(Chrysler)
UtText(Chrysler)
```

Configuring Gateway Databases

4

Adding Gateway records 4-4

Displaying and modifying a Gateway's general information. 4-6

Displaying and modifying Gateway number translation tables 4-12

Displaying and modifying coverage areas 4-18

Removing a Gateway 4-26

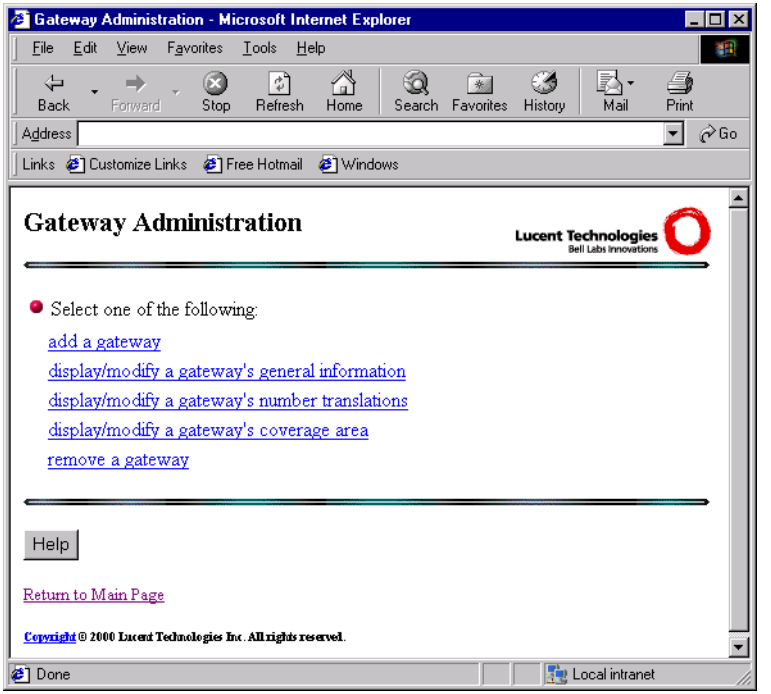
From the MVAM, you can:

- Add Gateways to the MultiVoice network
- Display and modify Gateway information
- Display and modify Gateway number translations
- Display and modify Gateway coverage areas
- Remove Gateways from the MultiVoice network

Note: When you add, modify, or delete Gateways on an Access Manager, the Gateway Name denotes the physical MultiVoice Gateways in your network. The Gateway Name must match the value assigned to the System > Sys Config > Name parameter set on the Gateway itself.

In the Administration section of the Access Manager main screen, click `gateways`. The Gateway Administration page, as illustrated in Figure 4-1, appears:

Figure 4-1. Gateway Administration page



From this page, you may perform the following Gateway administration tasks:

Option	Description
add a gateway	This option is used to add one or more new Gateways to the Gateway database.
display/modify a gateway's general information	This option is used to display and modify Gateway information retrieved from the Gateway database.
display/modify a gateway's number translations	This option is used to map number translation tables to Gateways, and for modifying the translation rules of the selected translation tables.
display/modify a gateway's coverage area	This option is used to display and modify Gateway coverage areas Gateways retrieved from the Gateway database.
remove a gateway	This option is used to remove one or more existing Gateways from the Gateway database.

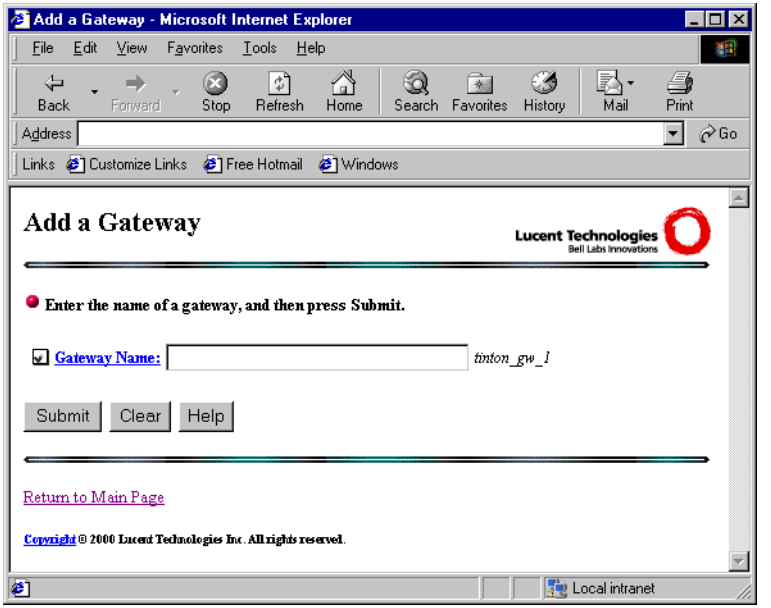
Note: You can get on-line help for any screen by clicking the Help button, or for specific fields by clicking any underlined field name.

Most Access Manager screens display 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.

Adding Gateway records

To add one or more Gateways to the MultiVoice network, click the Add a Gateway link on the Gateway Administration screen. The Add a Gateway screen, as illustrated in Figure 4-2, appears:

Figure 4-2. Add a Gateway page



To create a new Gateway record, enter the following information on this page:

Parameter	Description
Gateway Name	This is an alpha-numeric string which uniquely identifies a Gateway. It must match the value assigned to the System > Sys Config > Name parameter set on the Gateway.

Once you have entered this information, click the Submit button to save it in the Gateway database.

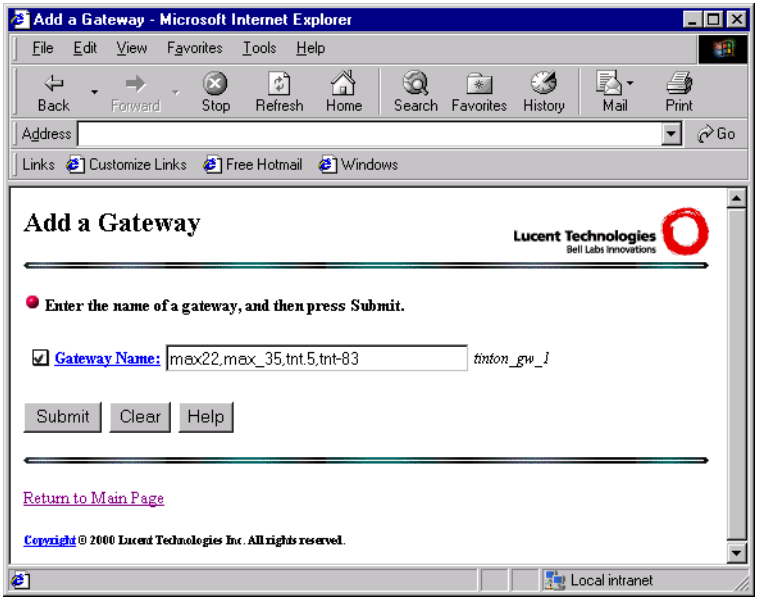
Adding multiple gateways

The Add a Gateway page allows you to add multiple Gateways in one operation by entering the Gateway Name of the Gateways you wish to add, separating each with a comma, and clicking the Submit button.

Note: A comma is the only delimiter. Entering a comma and a space will cause MVAM to display a message stating that leading and trailing spaces are not allowed.

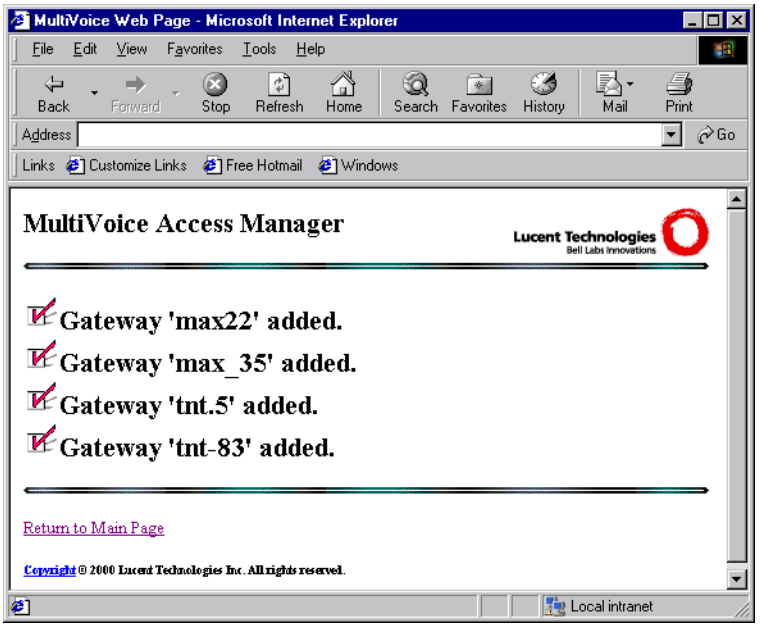
Figure 4-3 shows four Gateways (max22, max_35, tnt.5, and tnt-83) in the Gateway Name field to be added to the Gateways database.

Figure 4-3. Adding multiple Gateways



After the Gateways are added to the Gateways database, a confirmation message displays, as shown in Figure 4-4.

Figure 4-4. Successful addition of Gateways



Displaying and modifying a Gateway's general information

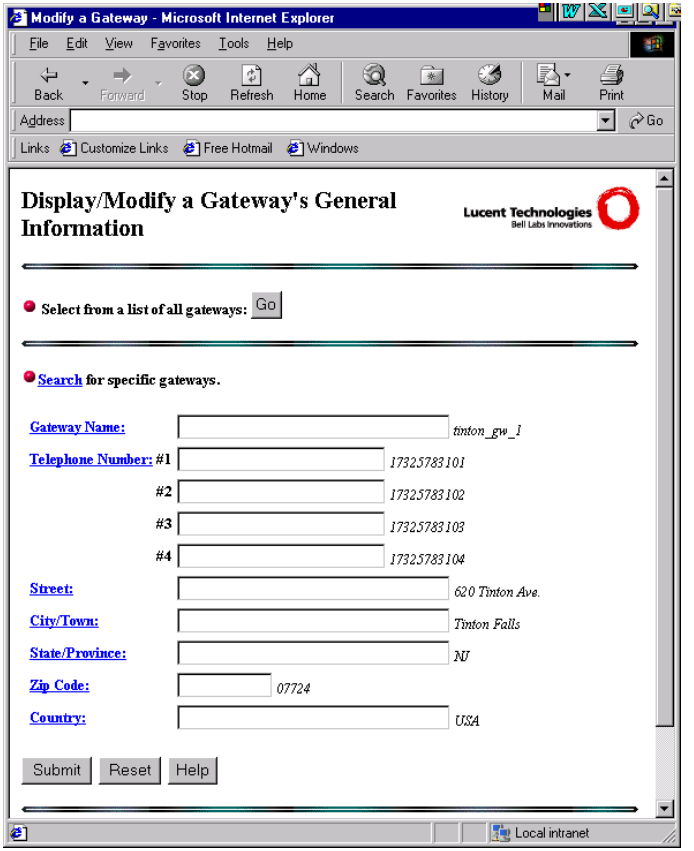
To update a Gateways's database record, click the `display/modify a gateway's general information` on the Gateway Administration screen. This option is used to:

- Select and display specific MultiVoice Gateway information from the Gateway database,
- Modify the information displayed in that database record.

Upon selection of this option, the Display/Modify a Gateway's General Information page, illustrated in Figure 4-5, appears. This page is used to select a MultiVoice Gateway. Selection may be done by:

- Clicking the Go button to display a list of all MultiVoice Gateways; then clicking a hyperlink to open a specific Gateway record.
- Entering a wildcard entry for Gateway name, or some combination of location and telephone number information on this screen; then clicking the Submit button to:
  - Retrieve all matching Gateway records,
  - Then clicking a hyperlink to open a specific Gateway record.
- Entering a specific Gateway name, telephone number, or address information.

Figure 4-5. Display/Modify a Gateway's General Information page



Understanding the Gateway database records

This page, and all the related pages for this Gateway administration option, use the data fields which make up the Gateway database record. This includes values for the following fields:

Parameter	Description
Gateway Name	This is an alpha-numeric string which uniquely identifies a Gateway. It must match the value assigned to the System > Sys Config > Name parameter set on the Gateway.
Telephone Numbers (1-4)	These are the telephone numbers that callers dial to reach the Gateway. 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.
Street	This is the premises or street address where the MultiVoice Gateway is installed.
City/Town	This is the city, town, or village where the MultiVoice Gateway is installed.
State/Province	This is the state, province, or region where the MultiVoice Gateway is installed.
Zip Code	This is the United States Post Office zip code, or local postal code for the location where the MultiVoice Gateway is installed.
Country	This the country where the MultiVoice Gateway is installed.

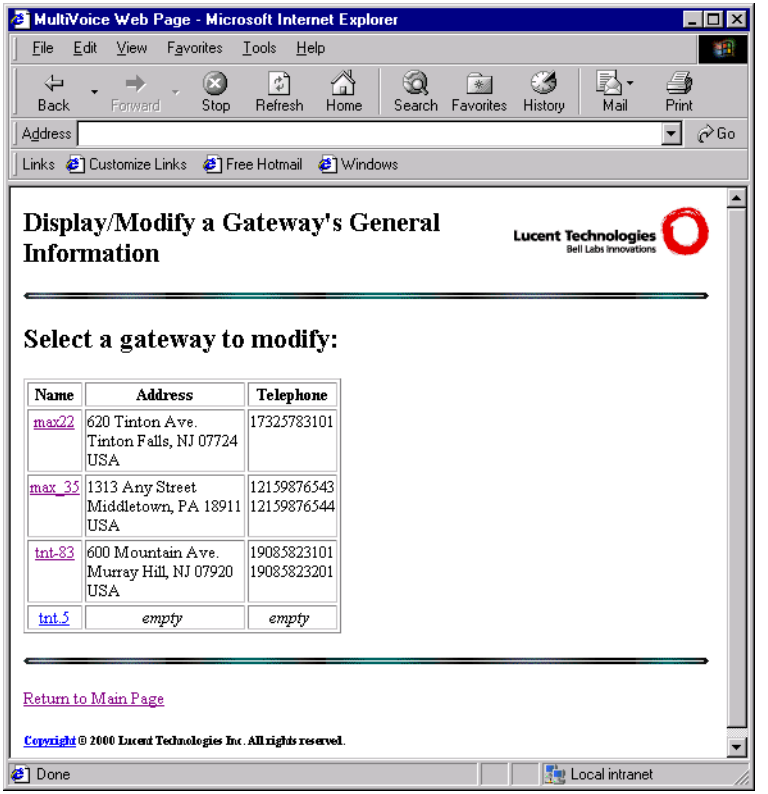
For complete information about each field, see the MVAM on-line help.

Selecting from a list of all gateways

To select a Gateway record from a list of all MultiVoice Gateways:

1 From the Display/Modify a Gateway's General Information page, click the Go button. A list of all Gateways appears, as illustrated in Figure 4-6:

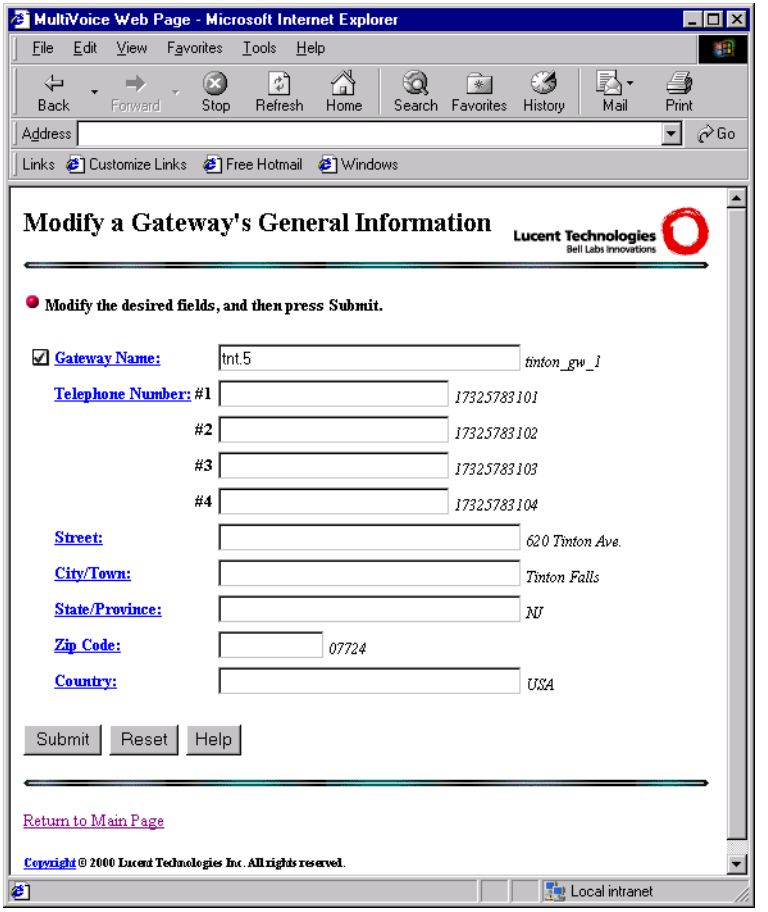
Figure 4-6. Select a gateway to modify page



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

The Access Manager displays the selected Gateway record on the Modify a Gateway's General Information page, as illustrated in Figure 4-7:

Figure 4-7. Modify a Gateway's General Information page

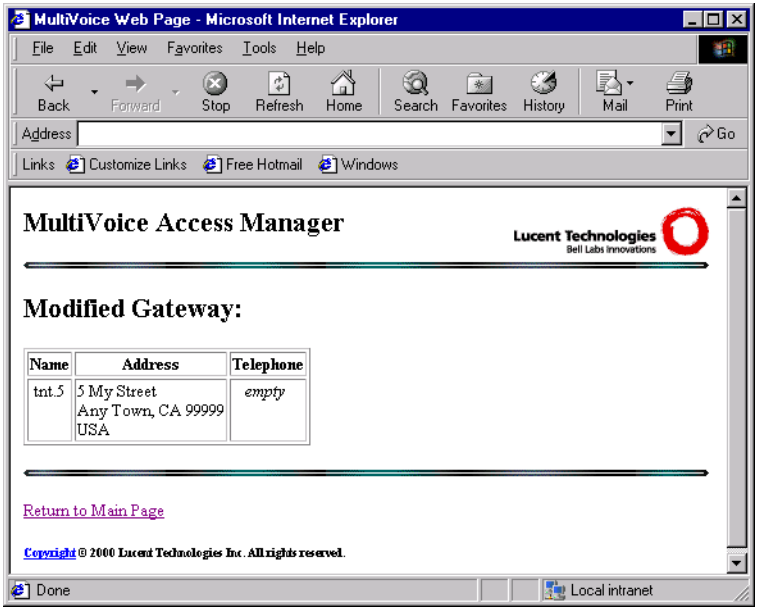


3 Modify any field by typing in the new information.

4 Click the Submit button to save the settings.

The Access Manager confirms the saved changes by displaying the Modified Gateway information page, as illustrated by Figure 4-8:

Figure 4-8. Modified Gateway page



Selecting a gateway using wildcard searches

The wildcard character "%" is supported in all fields of the Gateway, Gatekeeper, Terminal, ADMA, and User search forms. For example, entering "d%" in the Gateway Name field on a search form will cause all gateways whose names begin with "d" to be displayed.

The wildcard character may appear at either the beginning or the end of an entry. Once all your search criteria is entered on the screen, click the Submit button to display any matches for your search criteria.

Modifying and saving Gateway data

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 increase the number of ports your MVAM supports by purchasing a License Pack and entering valid upgrade serial numbers to your current MVAM installation. For details about upgrading the MVAM license, contact an authorized Lucent Technologies representative. See Appendix B, “MVAM Licenses,” for more information on License Packs.

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 Gateway Name field in the MVAM Gateway record must match the value assigned to the System > Sys Config > Name parameter set on the Gateway itself.

Displaying and modifying Gateway number translation tables

The display/modify a gateway’s number translation table option is used to:

- Select number translation tables assigned to specific MultiVoice Gateways,
- Modify the rules for number translations for these assigned tables.

Number translation tables are used by the Access Manager to convert a telephone number dialed by a caller into the actual telephone number a MultiVoice Gateway needs to complete a call. For more information on using number translations see Chapter 8, “Using Number Translations.”

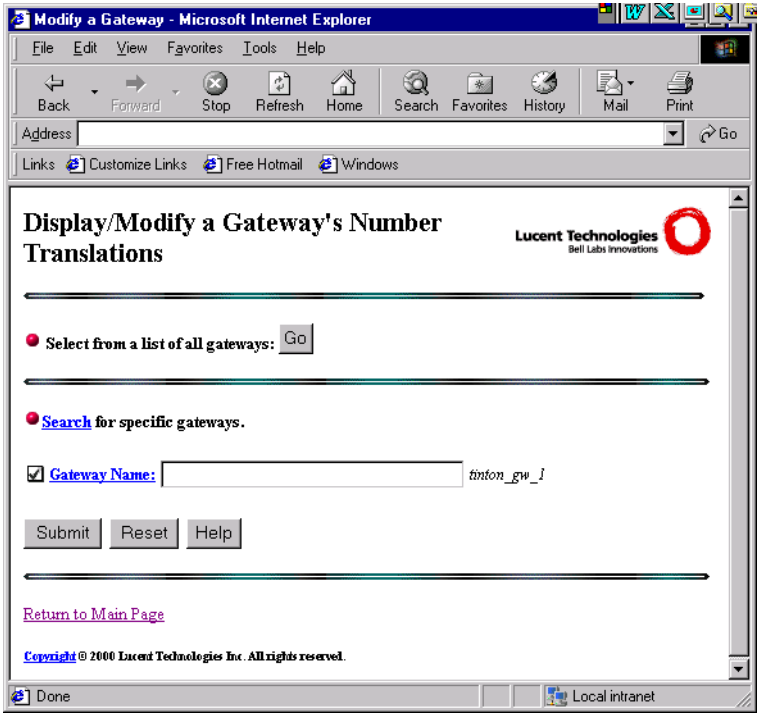
The Display/Modify a Gateway’s Number Translations page, illustrated in Figure 4-9, is used to select the number translation tables assigned to a MultiVoice Gateway. Selection may be done by either:

- Clicking the Go button to display a list of all MultiVoice Gateways and their associated number translation tables; then clicking a hyperlink for one of the following:
  - a Gateway to change the assigned ingress or egress number translation table,
  - an ingress translation table to edit the translations rules for that table,

  – an egress translation table to edit the translation rules for that table.

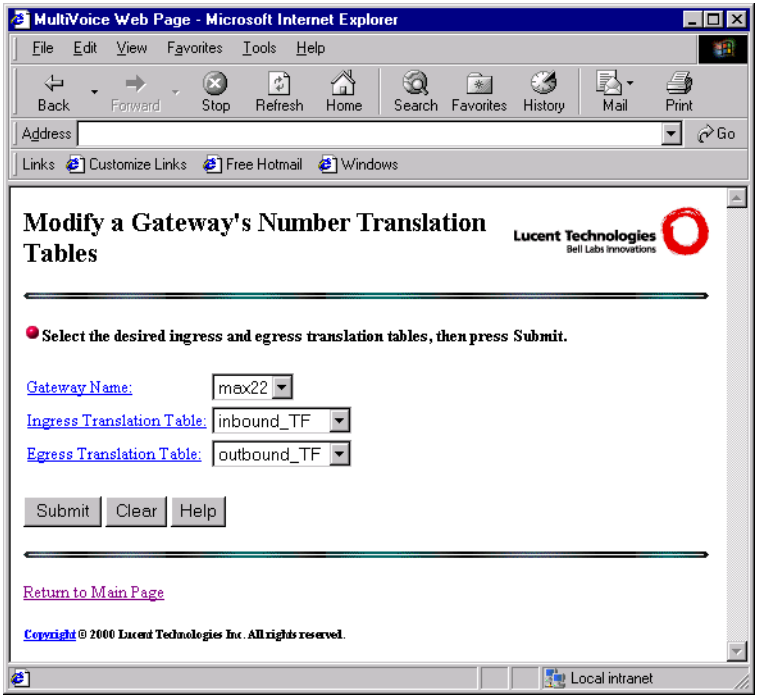
- Entering a Gateway Name in the Gateway Name field; then clicking the Submit button.

Figure 4-9. Display/Modify a Gateway's Number Translations page



When a Gateway is selected, the Access Manager will display the Modify a Gateway Number Translation Tables page, as illustrated in Figure 4-10, displaying the Gateway name and its assigned ingress and egress tables.

Figure 4-10. Modify a Gateway Number Translation Tables page



To modify the ingress and egress table assignments, select the following values on this page:

Parameter	Description
Gateway Name	This is an alpha-numeric string which uniquely identifies a Gateway. It must match the value assigned to the System > Sys Config > Name parameter set on the Gateway.

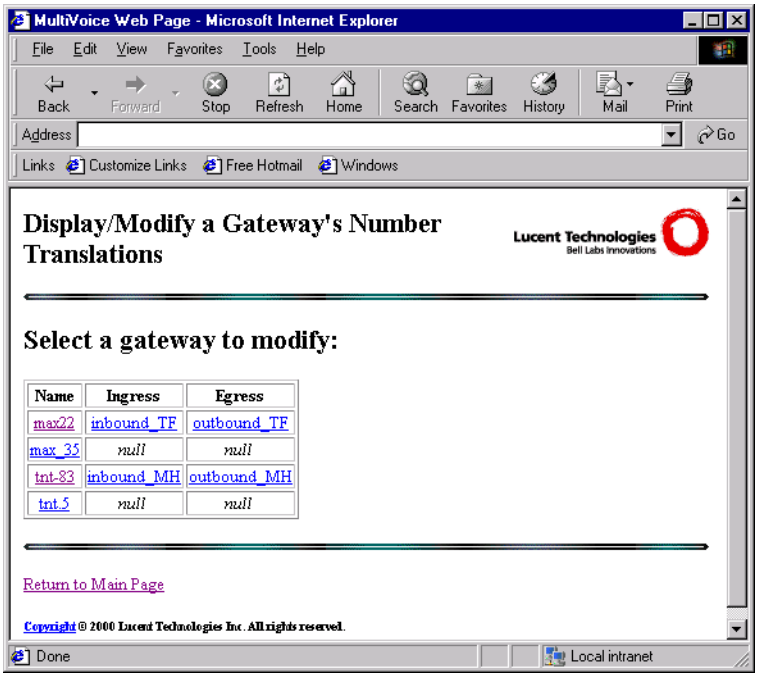
Parameter	Description
Ingress Translation Table	This identifies the number translation table this Gateway uses for processing inbound calls received from the PSTN. This table contains the translation rules the Gateway will apply to dialed telephone numbers, to generate the canonical form of the destination telephone number; which is used for Gateway or Gatekeeper routing.
Egress Translation Table	This identifies the number translation table this Gateway uses for processing outbound calls to the PSTN. This table contains the translation rules the Gateway will apply to the canonical form of the destination telephone number, to generate the localized dialing string; which is used to connect the call to its final destination.

Once you have selected the values on this page, click the Submit button to save your changes.

Selecting from a list of all gateways with number translation tables

From the Display/Modify a Gateway's Number Translations page, click the Go button. A list of all Gateways with assigned translation tables appears, as illustrated in Figure 4-11:

Figure 4-11. Display/Modify a Gateway's Number Translations page



Modifying assigned number translation tables

To modify the number translation tables assigned to a Gateway:

1 Click the hyperlink for a displayed Gateway.

The Access Manager displays the selected Gateway record on the Modify a Gateway's Number Translation Tables page, as illustrated in Figure 4-10:

2 Modify assigned number translation tables by:

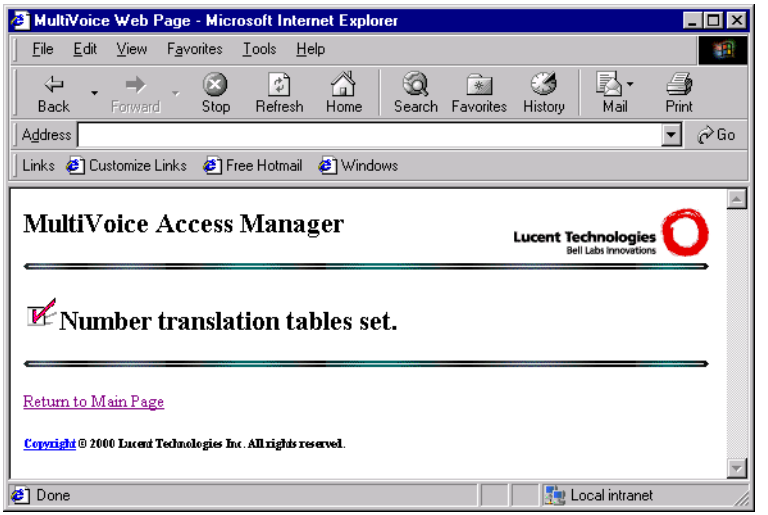
– Typing in the name of a number translation table for either the ingress or egress translation tables,

– Clicking an entry from the pull-down lists for either the ingress or egress translation tables.

3 Clicking the Submit button to save your settings.

The Access Manager confirms the saved changes by displaying a confirmation message, as illustrated by Figure 4-12:

Figure 4-12. Modified Number Translation confirmation page



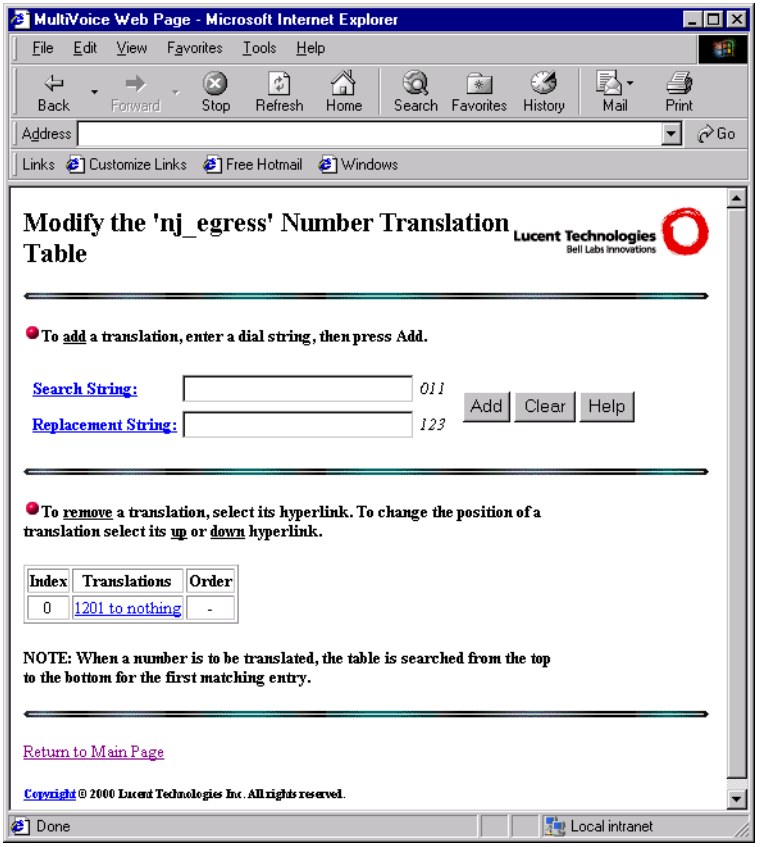
Modifying number translation rules

You may modify the rules contained in number translation tables assigned to a Gateway by:

1 Clicking the hyperlink for an ingress or egress number translation table from the list of all Gateways, as illustrated in Figure 4-11.

The Access Manager displays the selected number translation table on the Modify the Number Translation Table page, as illustrated in Figure 4-13:

Figure 4-13. Modify the Number Translation Table page



See Chapter 8, “Using Number Translations” for information on using this page.

2 Once you have finished making modifications to this number translation table, click the Submit button.

Displaying and modifying 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 that 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 numbers 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.

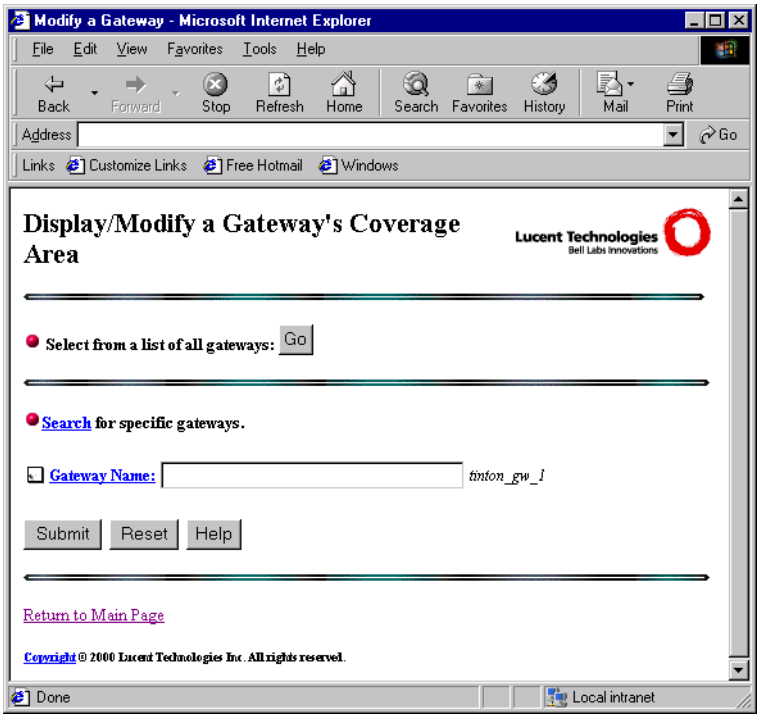
Modifying a coverage area

The Display/Modify a Gateway's Coverage Area option is used to assign coverage areas to specific MultiVoice Gateways administered by the Access Manager.

The Display/Modify a Gateway's Coverage Area page, illustrated in Figure 4-14, is used to select a MultiVoice Gateway coverage area. Selection may be done by either:

- Clicking the Go button to display a list of all administered MultiVoice Gateways and their associated coverage areas; then clicking a hyperlink of a Gateway to add, remove, or edit associated Inclusion Areas,
- Entering a Gateway name in the Gateway Name edit field; then clicking the Submit button.

Figure 4-14. Display/Modify a Gateway's Coverage Area page

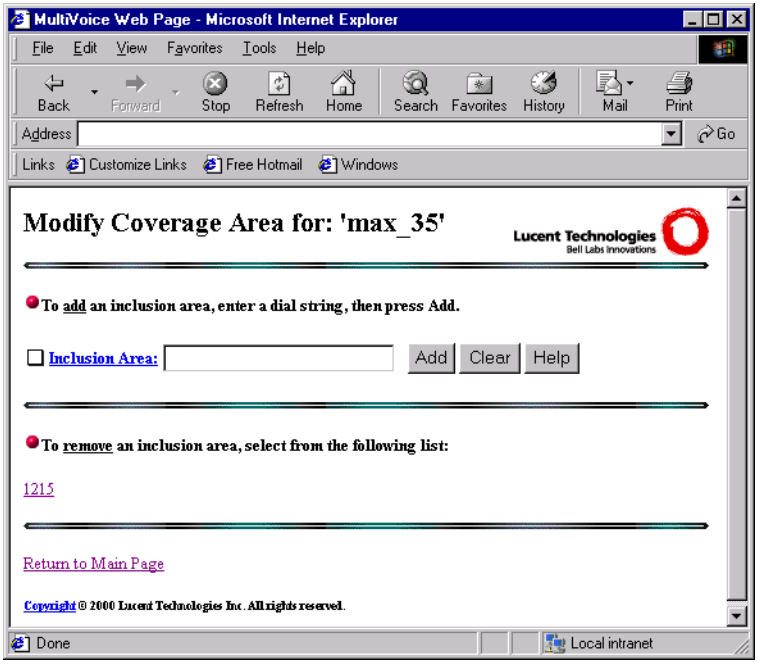


When a Gateway is selected, the Access Manager displays the Modify Coverage Area for a Gateway page, as illustrated in Figure 4-15.

Note: The add and remove sections are displayed if the gateway has been assigned one or more Inclusion Areas. If the gateway has not been assigned an Inclusion Area, the section allowing you to add an Inclusion area will be the only section displayed.

The name of the Gateway selected displays in the title of the screen, for example, `Modify Coverage Area for: 'max_35'`

Figure 4-15. Modify Coverage Area for a Gateway page



To add a new inclusion area, enter the following information on this page:

Parameter	Description
Inclusion Area	This is a numeric string which uniquely identifies the destination telephone numbers which are connected through the selected Gateway. It is specified by a Complete or Partial Telephone Number.

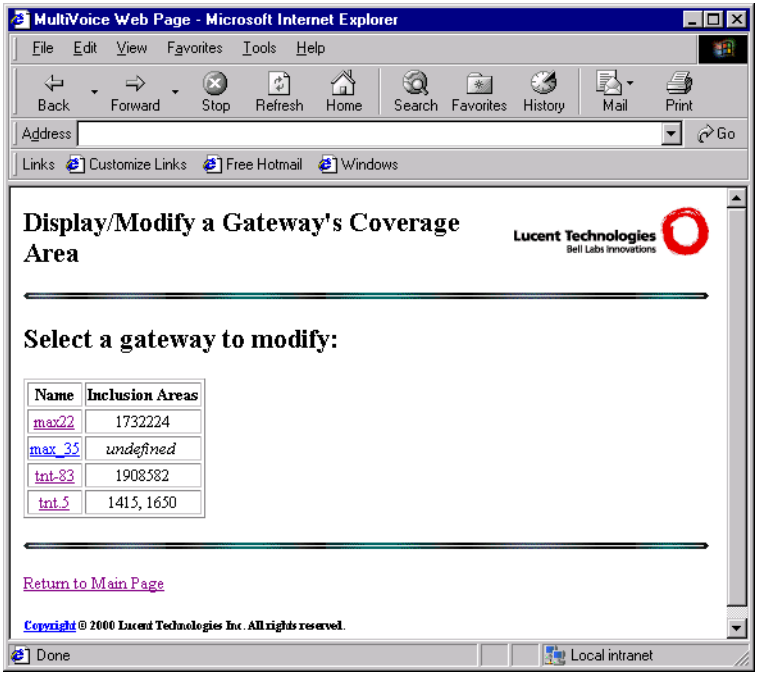
Once you have entered this information, click the Submit button to save it in the Gateway Coverage Area database.

Adding an Inclusion Area

To add Inclusion Areas for a Gateway coverage area:

1 From the Display/Modify a Gateway's Coverage Area page, click the Go button. A list of all Gateways with their associated coverage areas appears, as illustrated in Figure 4-16:

Figure 4-16. Select a gateway to modify page



2 Click the hyperlink for a displayed Gateway.

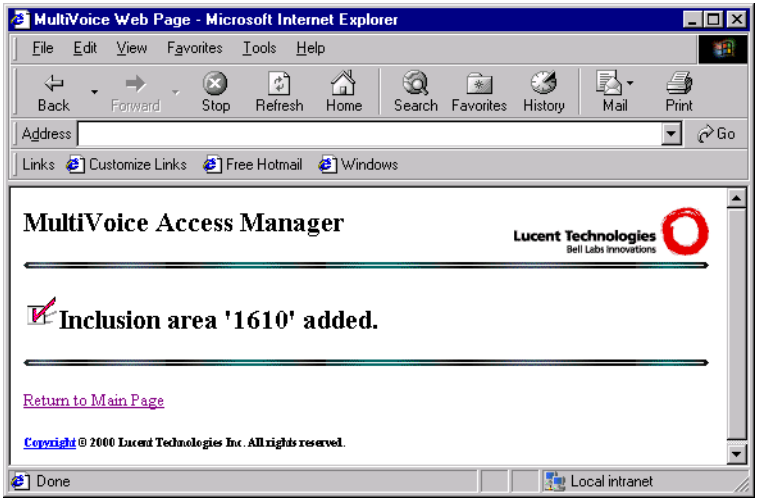
The Access Manager displays the selected Gateway coverage area on the Modify Coverage Area for a Gateway page, as illustrated in Figure 4-15:

3 Add a new Inclusion Area by typing a dial string in the Inclusion Area field.

4 To save your settings, click the Submit button.

The Access Manager confirms the saved changes by displaying a confirmation message, as illustrated by Figure 4-17:

Figure 4-17. Modified Coverage Area confirmation page

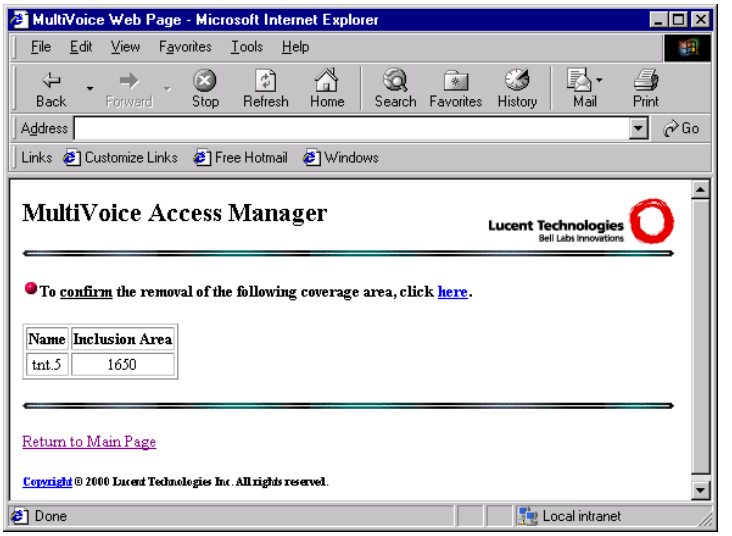


Removing an Inclusion Area

To remove Inclusion Areas from a Gateway coverage area, click a hyperlink displayed in the list of Inclusion Areas on the Modify Coverage Area for a Gateway page, as illustrated in Figure 4-15.

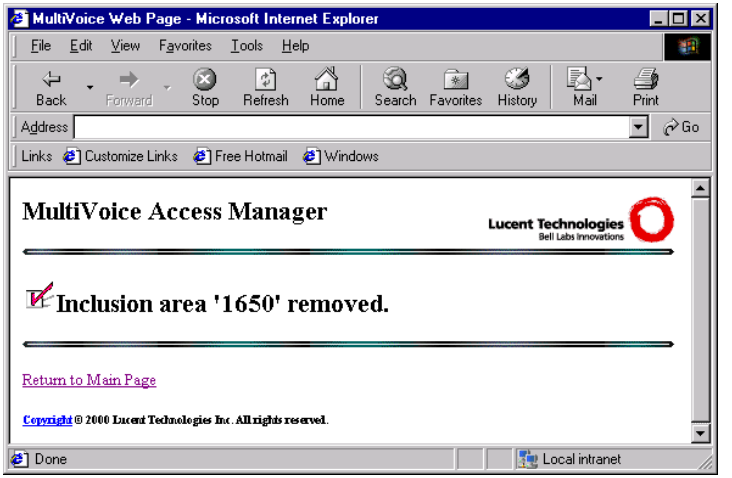
You are required to confirm the removal of the Inclusion Area selected by responding to the message shown in Figure 4-18. To remove the Inclusion Area displayed, click “here”. If you choose to cancel your removal request, you must click your browser’s Back button.

Figure 4-18. Confirm removal of Inclusion Area



After the Inclusion Area is removed from the Gateway Coverage Area database, a confirmation message displays, as shown in Figure 4-19.

Figure 4-19. Successful removal of Inclusion Area



Viewing modified coverage areas

Click your broswer's Back button to display a Gateway's modified coverage area. Changes to a Gateway's coverage area may not appear until the Modify Coverage Area for a Gateway page is reloaded.

Note: When you modify a coverage area for a Gateway, by either adding or removing Inclusion Areas, clicking the browser's Back button should update the 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.

Coverage area size

The maximum number of inclusion areas which may be assigned to a Gateway coverage area is controlled by the `listCapacity` parameter in the Gwct section of 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`. Changes to the `listCapacity` parameter are applied by stopping and restarting MVAM. (See "Starting MVAM" on page 2-25, and "Stopping MVAM" on page 2-32.) For details on initialization parameters, see Appendix A, "MVAM Initialization File."

Coverage area display

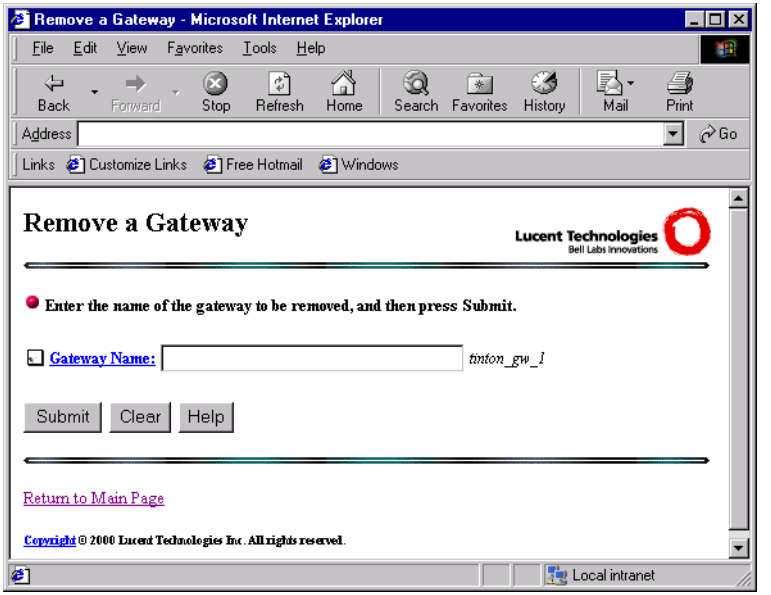
The maximum number of Inclusion Areas displayed for a Gateway coverage area, on lists of all Gateways, is controlled by the `displayCapacity` parameter in the Gwct section of the MVAM initialization file. Valid values for this variable range between one and 2,000. By default the size of a Gateway coverage area is limited to 25 Inclusion Areas.

This value is changed by editing the initialization file, `mvam.ini`. Changes to the `displayCapacity` variable are applied by stopping and restarting MVAM. (See "Starting MVAM" on page 2-25, and "Stopping MVAM" on page 2-32.) For details on initialization parameters, see Appendix A, "MVAM Initialization File."

Removing a Gateway

To remove one or more Gateways from the MultiVoice network, click the Remove a Gateway link on the Gateway Administration screen. The Remove a Gateway page, as illustrated in Figure 4-20, appears:

Figure 4-20. Remove a Gateway page



To remove a Gateway record, enter the following information on this page:

Parameter	Description
Gateway Name	This is an alpha-numeric string which uniquely identifies a Gateway. It must match the value in the Gateway database.

Once you have entered this information, click the Submit button to save your changes.

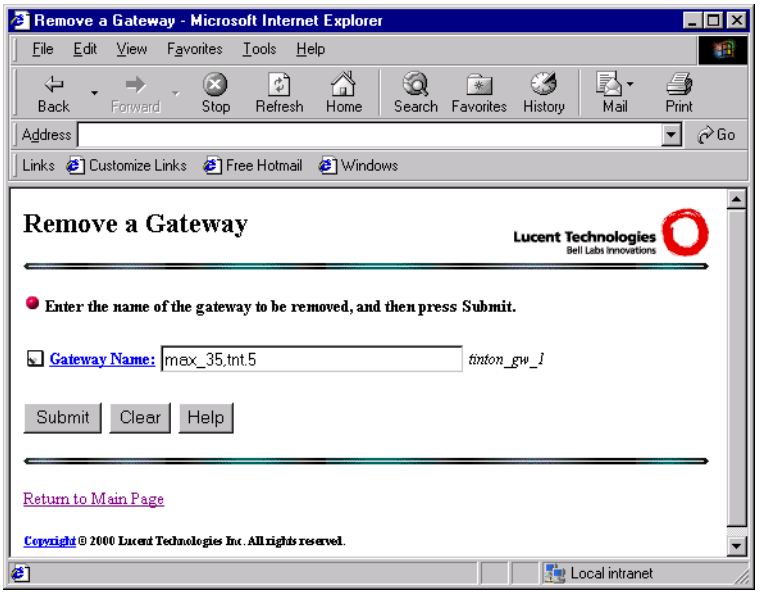
Removing multiple gateways

The Remove a Gateway page allows you to remove multiple Gateways in one operation by entering the Gateway Name of the Gateways you wish to remove, separating each with a comma, and clicking the Submit button.

Note: A comma is the only delimiter. Entering a comma and a space will return an error message.

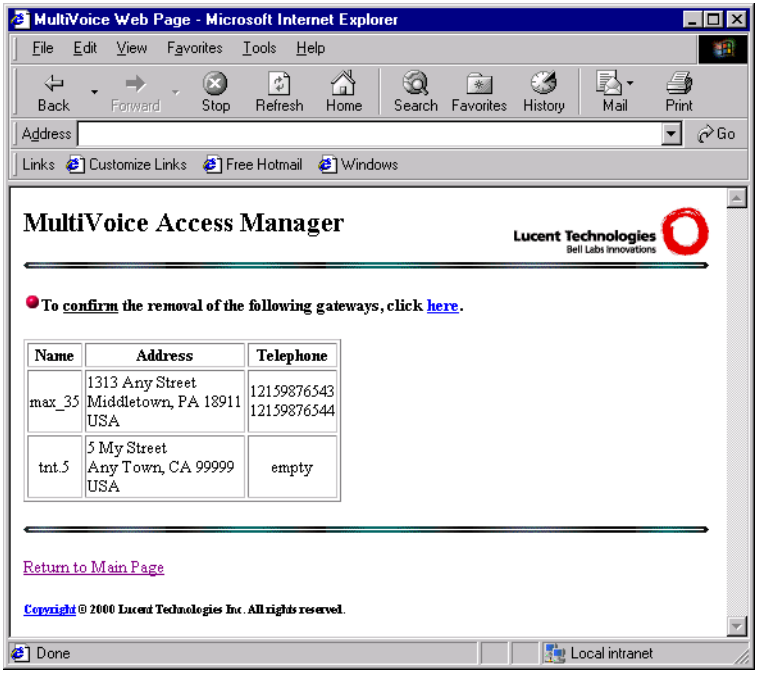
Figure 4-21 shows two Gateways (in the Gateway Name) field to be removed from the Gateways database.

Figure 4-21. Removing multiple Gateways



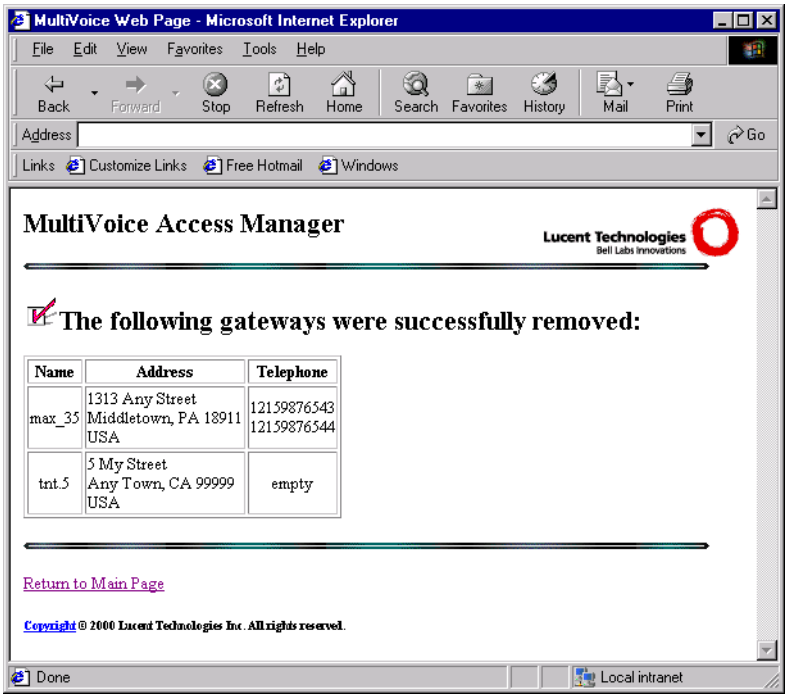
You are required to confirm the removal of the Gateways entered in the Gateway Name field by responding to the message shown in Figure 4-22. To remove all of the Gateways listed, click “here”. If you choose to cancel your removal request or to make any changes to the list of Gateways to be removed, you must click your browser’s Back button.

Figure 4-22. Confirm removal of Gateways



After each Gateway is validated and its Gateway record is removed from the Gateway database, a confirmation message displays, as shown in Figure 4-23.

Figure 4-23. Successful removal of Gateways



Configuring Logical Gateways

5

How MLG and ADMA Rules Work. 5-2

ADMA Rules 5-4

Adding an ADMA Rule 5-6

Displaying and modifying ADMA Rules. 5-9

Removing an ADMA Rule. 5-13

ADMA Rule Sets 5-15

Adding an ADMA Rule Set 5-16

Displaying and modifying ADMA Rule Sets. 5-18

Removing an ADMA Rule Set. 5-22

ADMA Gateway/Trunk Rules 5-24

Adding an ADMA Gateway/Trunk Rule 5-26

Displaying and modifying ADMA Gateway/Trunk Rules. 5-29

Removing an ADMA Gateway/Trunk Rule. 5-34

The MultiVoice Access Manager (MVAM) supports Multiple Logical Gateways (MLG) which allows each incoming call to a VoIP Gateway to have its own set of configuration parameters, rather than one set of configuration parameters for all incoming calls.

These Gateway configuration parameters are defined by Authentication, Dial Mode, and Announcements (ADMA) rules on MVAM. These rules can be applied on a per call basis according to the Gateway/trunk that received the call and the number dialed by the calling party.

Individual rules specific to a DNIS, “ADMA Rules”, determine the type of user authentication, dial mode, and announcements required for a call. These rules are then grouped into sets, “ADMA Rule Sets”, and associated with individual Gateway/Trunk IDs, “ADMA Gateway/Trunk Rules”.

Note: All ADMA rules (Rules, Rule Sets, and Gateway/Trunk Rules) are configured at the MVAM level and are seen in every virtual zone.

Note: Administrators must ensure that rules exist for every call that originates from a Gateway with MLG enabled. If a call does not match existing rules, the call will attempt to proceed based on the current MVAM Security Options. If MVAM does not have all the information needed to complete the call, unexpected results may occur.

How MLG and ADMA Rules Work

Note: The Gateway software version must be Release 8.0-103 for the ADMA rules to function properly.

When the MLG parameter is enabled on the Gateway that originates the call:

- The Gateway relinquishes control of authentication and dial mode—the VPN mode and the single-dial enable parameters become non-applicable.
- MVAM consults its ADMA databases to determine the authentication, dial mode, and announcements to use, if any, for the incoming call based on the gateway and trunk that the call was received on and the number dialed by the calling party.

When a call is placed to a Gateway (with MLG enabled):

1 The Gateway sends the Gateway Name, Trunk Id, DNIS (if available), and ANI (if available) to the MVAM.

2 MVAM uses the combination of Gateway Name and Trunk Id to search the Gateway/Trunk Rules database.

3 If a Rule Set Name is defined for the Gateway/Trunk combination, MVAM searches the Rule Sets database to identify the Rule for the Rule Set Name found.

If a Rule Set Name is not defined for the Gateway/Trunk Id combination, MVAM refers to the settings specified under the Security Options section.

4 The individual ADMA Rules are then searched using a DNIS prefix match.

5 If a match is found and the MVAM has all the required data to route the call, based on the ADMA parameters in the matching ADMA Rule (for example, ANI enabled, PIN disabled, single-stage dialing), MVAM will send the Gateway a confirmation and the call is routed.

If no match is found, MVAM refers to the settings specified under the Security Options section.

6 If a match is found, but the MVAM does not have the required data to route the call, based on the ADMA parameters in the matching ADMA rule (for example, dual-stage dialing, PIN enabled), the MVAM will continue to request data from the Gateway until the call can or cannot be authenticated/routed.

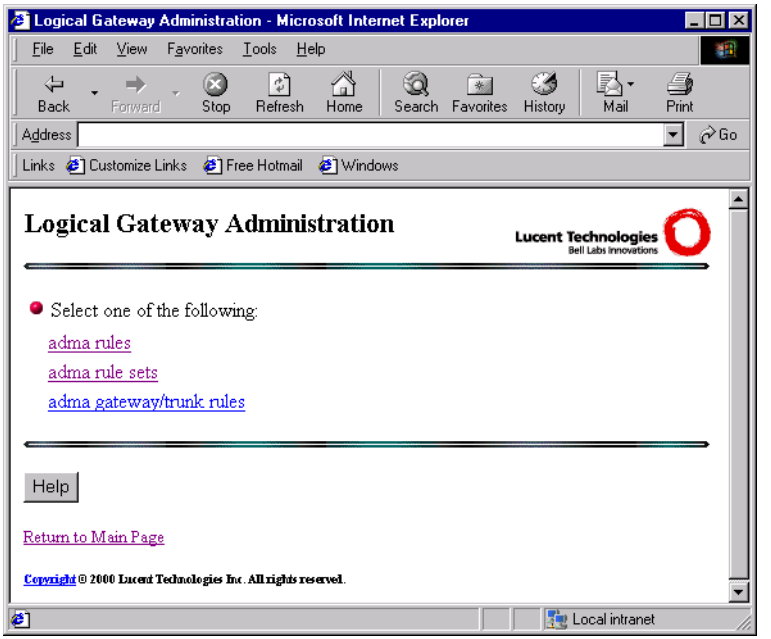
Note: The configuration parameters located in the ADMA Rules database override the same parameters specified on the Gateway when MLG is enabled on the Gateway and the Gateway/trunk and dialed number match a defined rule within the ADMA databases.

From the MVAM Main Page, you can access:

- ADMA Rules
- ADMA Rule Sets
- ADMA Gateway/Trunk Rules

In the Administration section of the MVAM main screen, click `logical gateways`. The Logical Gateway Administration page, as illustrated in Figure 5-1, appears:

Figure 5-1. Logical Gateway Administration page



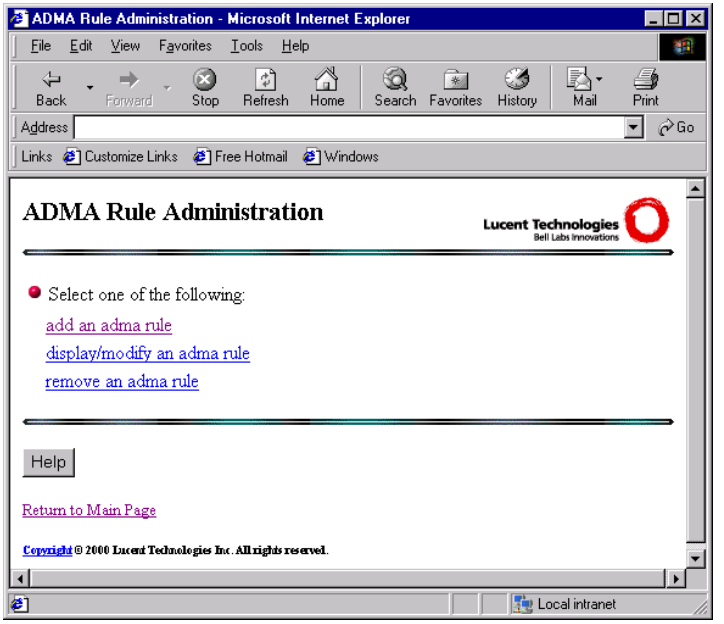
ADMA Rules

ADMA Rules specify the ADMA parameters related to authentication, single- and dual-stage dialing, and announcements, that apply to calls destined for a specific DNIS.

From the ADMA Rule Administration page as shown in Figure 5-2, you can:

- Add an ADMA Rule to the Rules database
- Display and modify an ADMA Rule
- Remove an ADMA Rule from the Rules database

Figure 5-2. ADMA Rule Administration page



The hyperlinks point to the following:

Option	Description
add an ADMA rule	This option adds a new ADMA Rule to the Rules database.
display/modify an ADMA rule	This option is used to display and modify ADMA Rule information retrieved from the Rules database.
remove an ADMA rule	This option is used to remove an existing ADMA Rule from the Rules database.

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

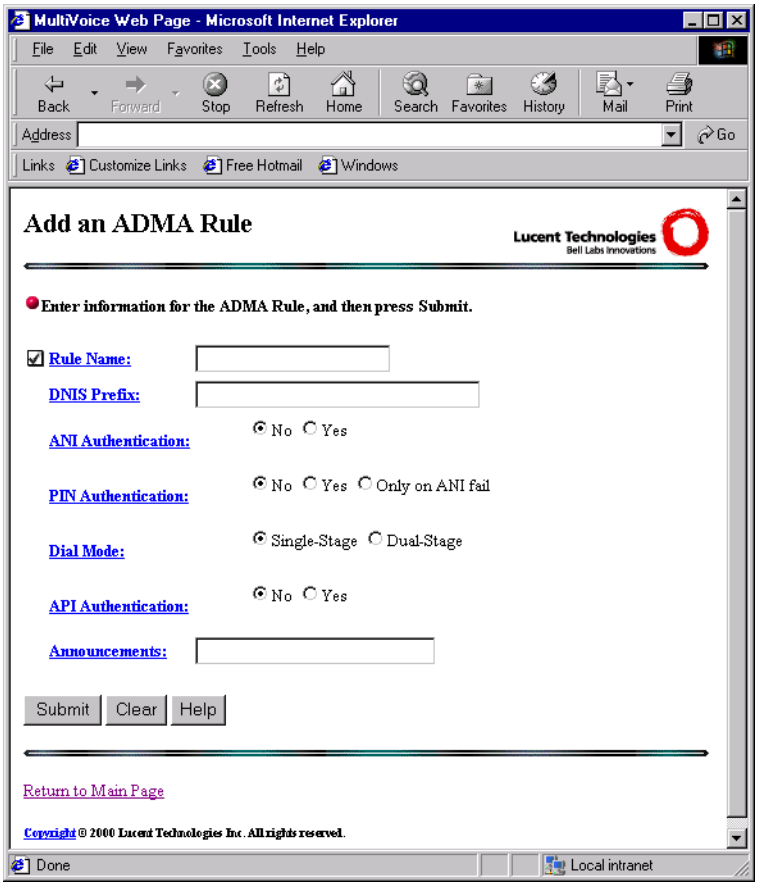
A check box to the left of any field name indicates that you must enter a value for the field before you click the Submit button.

Adding an ADMA Rule

The Add an ADMA Rule page, illustrated in Figure 5-3, is used to add a new ADMA Rule to the Access Manager's Rules database. This is accomplished by entering a Rule Name (required) for the ADMA Rule, entering a DNIS prefix (optional), changing the default authentication and dial mode settings (optional), and entering the location of the announcements associated with the Rule Name specified (optional).

To save the new ADMA Rule, click the Submit button.

Figure 5-3. Add an ADMA Rule page



To add an ADMA Rule, enter the following values on this page:

Parameter	Description
Rule Name	This is an alpha-numeric, case-sensitive string which uniquely identifies an ADMA Rule. This field supports a maximum of 50 characters.
DNIS Prefix	This is a numeric field that contains a Dialed Number Identification Service (DNIS) prefix which may be a complete or partial phone number dialed by the endpoint. The MVAM attempts to match the number dialed (DNIS) by the calling party to the longest digit match, from left to right, of a DNIS Prefix in the Rules Database. For example: 190858 is a better match than 1908, for the dialed number 19085821111. If the value for the DNIS Prefix is unspecified (default) in an ADMA Rule, any DNIS entered will be considered a DNIS Prefix match. This field supports a maximum of 30 digits.
ANI Authentication	Select whether the Automatic Number Identification (ANI), which identifies the calling telephone number, is required from the Gateway for authentication.

Parameter	Description
PIN Authentication	Select whether a Personal Identification Number (PIN), entered by the caller, is required from the Gateway for authentication. When set to "Only on ANI fail", the PIN will be required only if the Automatic Number Identification (ANI) of the caller's telephone number does not match a value in the User Alias field contained in the User Database. **Note:** When PIN Authentication is set to "Only on ANI fail", the ANI Authentication parameter, must be set to "Yes".
Dial Mode	This field indicates whether single- or dual-stage dialing is supported for calls following this ADMA Rule.
API Authentication	Select whether an API application (Yes) or MVAM (No) will perform authentication for an incoming call according to the ADMA rule.
Announcements	This alpha-numeric field specifies the location of the announcements files. This field supports a maximum of 25 characters. **Note:** The voice announcements parameter must be set to Yes (enabled) on the Gateway for MVAM to use the announcements directory specified in this field.

Once the Rule Name has been entered (required), and any changes are made (optional) to the authentication, dial mode, and announcements fields, click the Submit button to save this ADMA Rule.

Saving the settings

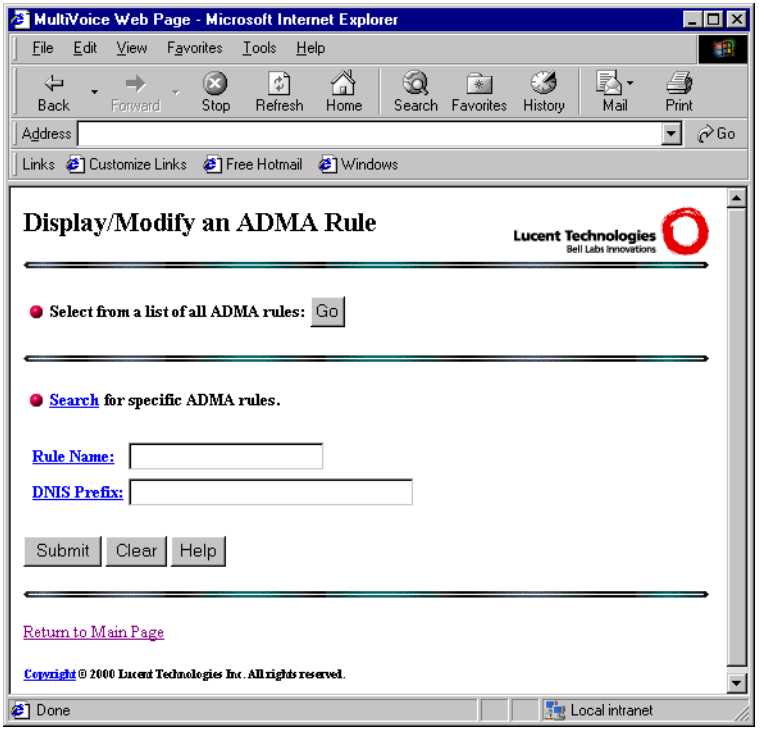
Changes to the Rules database do not take effect until you save them to the MVAM database files. To save the settings, click the Submit button in the lower-left section of the screen. A message will appear at the bottom of the screen confirming the successful addition of the ADMA Rule entered or providing a reason the rule could not be added, for example, “Rule Name ‘Rule1’ is not unique.” The Add an ADMA Rule Page will remain open and active to allow you to add additional rules.

Displaying and modifying ADMA Rules

The Display/Modify an ADMA Rule page, illustrated in Figure 5-4, is used to select an existing ADMA Rule, which is stored on the Access Manager. Selection may be done by either:

- Clicking the Go button to display a list of all ADMA Rules; then clicking one of the Rule Name hyperlinks to retrieve that information.
- Entering a Rule Name and/or DNIS Prefix (or search strings for either field) on this page; then clicking the Submit button.

Figure 5-4. Display/Modify an ADMA Rule page



To retrieve an ADMA Rule, enter either one, or both, of following values on this page:

Parameter	Description
Rule Name	This is a 50-character (maximum), alpha-numeric, case-sensitive string which uniquely identifies an ADMA Rule.

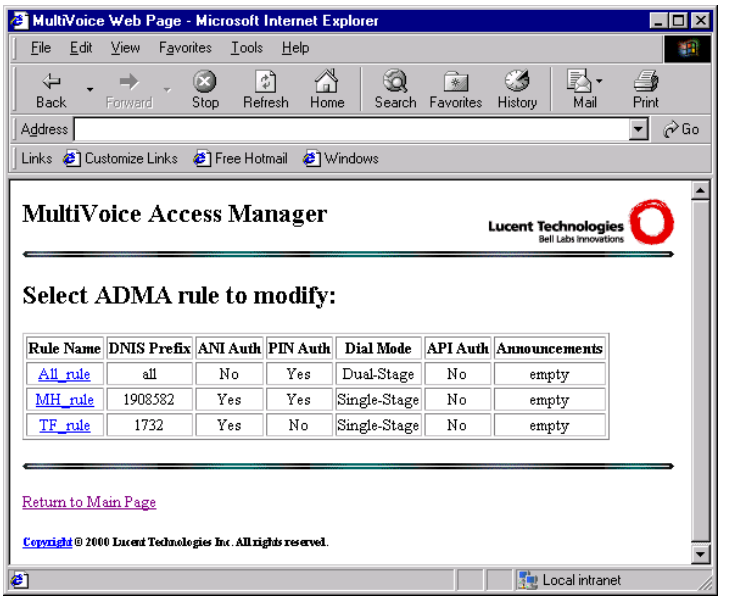
Parameter	Description
DNIS Prefix	This is a numeric field that contains a Dialed Number Identification Service (DNIS) prefix which may be a complete or partial phone number dialed by the endpoint. If the value for the DNIS Prefix is unspecified (default) in an ADMA Rule, any DNIS entered will be considered a DNIS Prefix match. This field supports a maximum of 30 digits.

Selecting from a list of all ADMA Rules

To select a ADMA Rule record from a list of known ADMA Rules:

1 From the Display/Modify an ADMA Rule page, click the Go button. A list of all ADMA Rules appears, as illustrated in Figure 5-5:

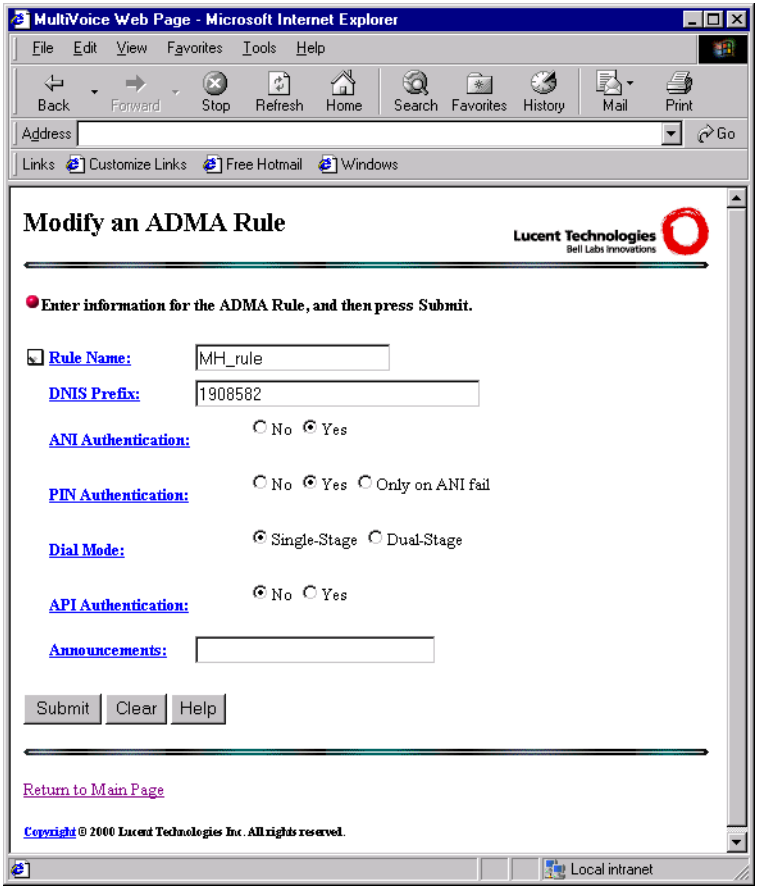
Figure 5-5. Select an ADMA Rule to modify page



2 Click the name of the ADMA Rule you wish to modify. (For a longer list, the screen has a scroll bar at its right edge.)

The Access Manager displays the selected ADMA Rules record on the Modify the ADMA Rule page, as illustrated in Figure 5-6:

Figure 5-6. Modify an ADMA Rule page

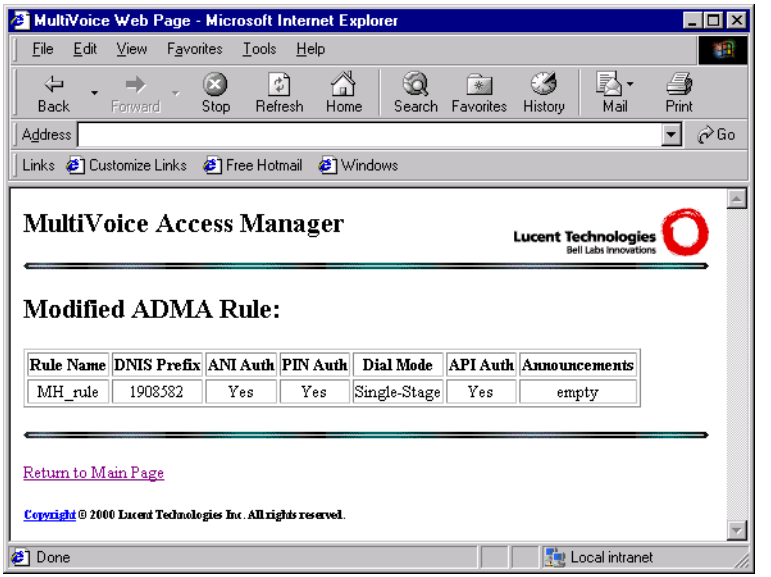


3 Modify any field, except Rule Name, by typing in or selecting the new information.

4 To save the settings, click the Submit button.

The Access Manager confirms the saved changes by displaying the Modified ADMA Rule page, as illustrated by Figure 5-7.

Figure 5-7. Modified ADMA Rules page



Selecting an ADMA Rule using wildcard searches

The wildcard character “%” is supported in all fields of the Gateway, Gatekeeper, Terminal, ADMA, and User search forms. For example, entering “d%” in the Rule Name field on a search form will cause all rules whose names begin with “d” to be displayed. Once the search criteria is entered, click the Submit button. MVAM will search its Rules database and return the rules found that match your search criteria.

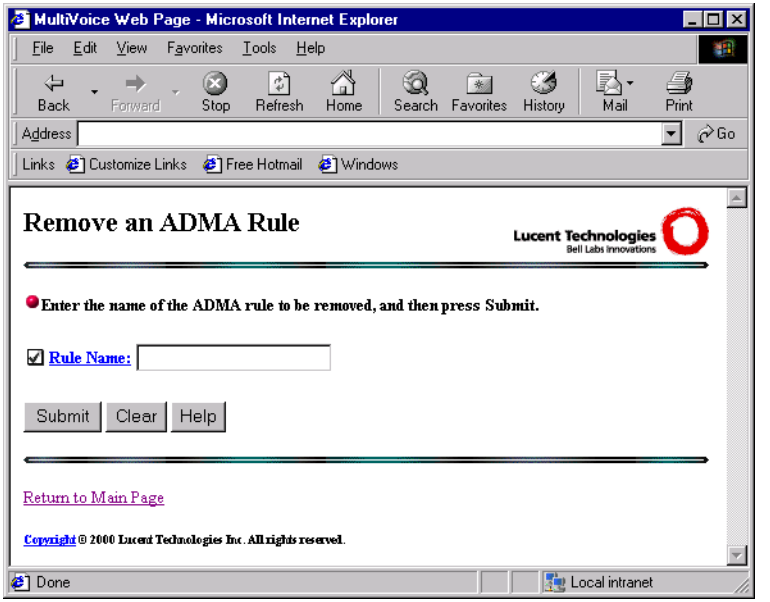
Removing an ADMA Rule

The Remove an ADMA Rule page, as illustrated in Figure 5-8, deletes one or more ADMA Rule records from the Access Manager’s Rules database. This is

accomplished by entering one or more ADMA Rule Names in the edit field, separating each by a comma, then clicking the Submit button.

Note: A comma is the only valid delimiter when removing multiple entries. Entering a comma and a space between entries will return an error message.

Figure 5-8. Remove an ADMA Rule page



To remove an ADMA Rule record, enter the following information on this page:

Parameter	Description
Rule Name	This is an alpha-numeric string which uniquely identifies an ADMA Rule in the Rules database.

Note: Removing an ADMA Rule will cause that ADMA Rule to be removed from any ADMA Rule Set with which it is associated.

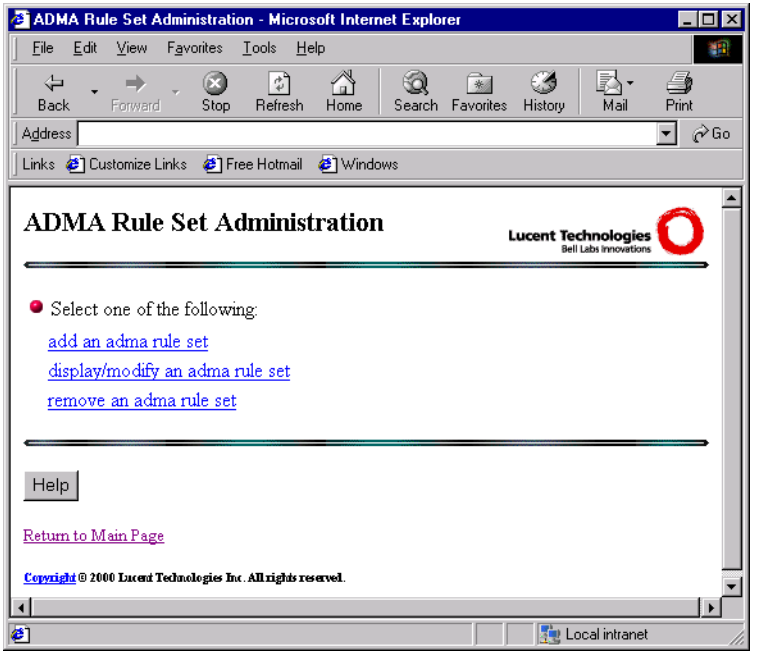
ADMA Rule Sets

ADMA Rule Sets contain one or more ADMA Rules. These Rule Sets will be associated with specific Gateway and Trunk IDs.

From the ADMA Rule Administration page as shown in Figure 5-9, you can:

- Add an ADMA Rule Set to the Rule Sets database
- Display and modify an ADMA Rule Set
- Remove an ADMA Rule Set from the Rule Sets database

Figure 5-9. ADMA Rule Set Administration page



The hyperlinks point to the following:

Option	Description
add an ADMA rule set	This option adds a new ADMA Rule Set to the Rule Sets database.
display/modify an ADMA rule set	This option is used to display and modify ADMA Rule Sets information retrieved from the Rule Sets database.
remove an ADMA rule set	This option is used to remove an existing ADMA Rule Set from the Rule Sets database.

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

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.

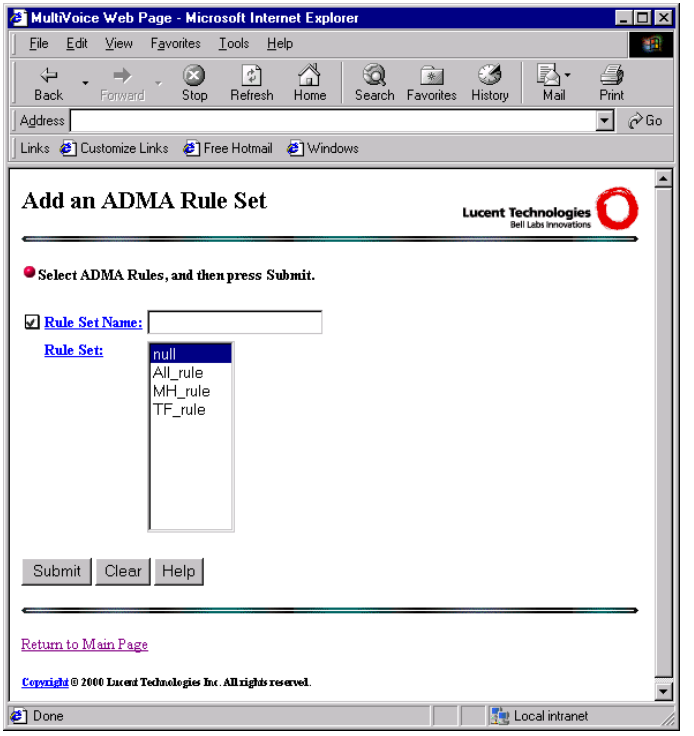
Adding an ADMA Rule Set

The Add an ADMA Rule Set page, illustrated in Figure 5-10, is used to add a new ADMA Rule Set to the Access Manager's Rule Sets database. This is accomplished by entering a Rule Set Name (required) for the ADMA Rule Set, and specifying the ADMA Rule or Rules associated with this Rule Set Name.

Note: When selecting ADMA Rules for a ADMA Rule Set, no two ADMA Rules selected may have the same DNIS.

To save the new ADMA Rule Set, click the Submit button.

Figure 5-10. Add an ADMA Rule Set page



To add an ADMA Rule Set, enter, or select, the following values on this page:

Parameter	Description
Rule Set Name	This is a 50-character (maximum), alpha-numeric, case-sensitive string which uniquely identifies an ADMA Rule Set.
Rule Set	This is a pull-down list of all administered ADMA Rules. Select one or more ADMA Rules that will be associated with the Rule Set Name. You may also choose to have no ADMA Rules associated with this Rule Set by selecting “null” from the pull-down list.

Note: To select multiple ADMA Rules in a series, click the first rule in the series, and press the Shift key while clicking the last rule in the series you wish to include in the Rule Set. To select multiple ADMA Rules (not in a series), press the CTRL key while clicking the rules you wish to include in the Rule Set.

Once the Rule Set Name has been entered, and the ADMA Rules have been selected, click the Submit button to save this ADMA Rule set.

Saving the settings

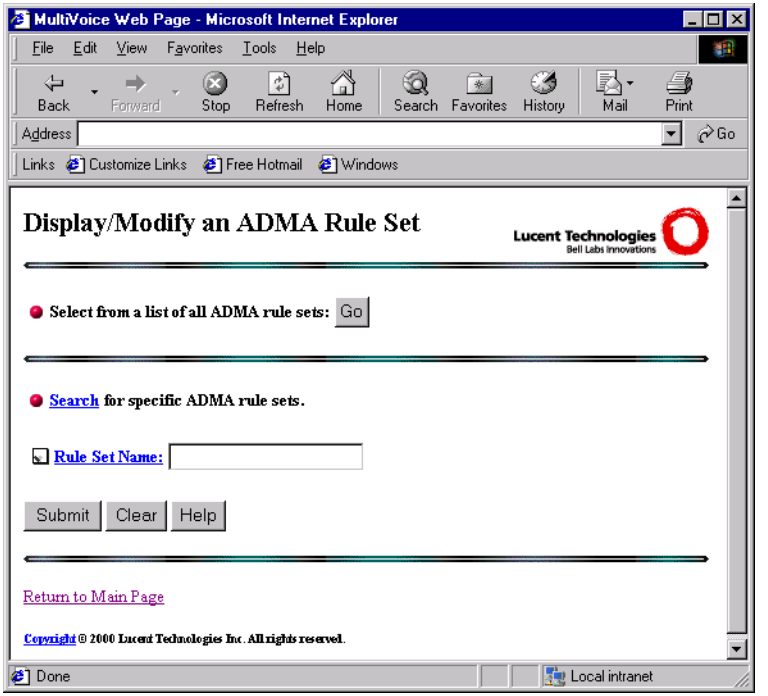
Changes to the Rule Sets database do not take effect until you save them to the MVAM database files. To save the settings, click the Submit button in the lower-left section of the screen.

Displaying and modifying ADMA Rule Sets

The Display/Modify an ADMA Rule Sets page, illustrated in Figure 5-11, is used to select an existing ADMA Rule Set, which is stored on the Access Manager. Selection may be done by either:

- Clicking the Go button to display a list of all ADMA Rule Sets; then clicking one of the Rule Set Name hyperlinks to retrieve that information.
- Entering a Rule Set Name (or search string) on this page; then clicking the Submit button.

Figure 5-11. Display/Modify an ADMA Rule Sets page



To retrieve an ADMA Rule Set, enter the following value on this page:

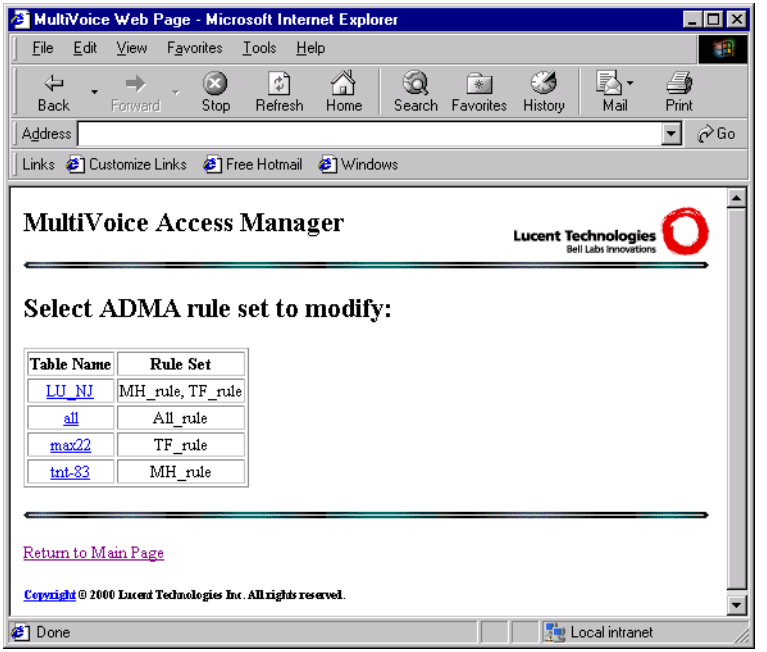
Parameter	Description
Rule Set Name	This is a 50-character (maximum), alpha-numeric, case-sensitive string which uniquely identifies an ADMA Rule Set.

Selecting from a list of all ADMA Rule Sets

To select a ADMA Rule Set record from a list of known ADMA Rule Sets:

1 From the Display/Modify an ADMA Rule Set page, click the Go button. A list of all ADMA Rule Sets appears, as illustrated in Figure 5-12:

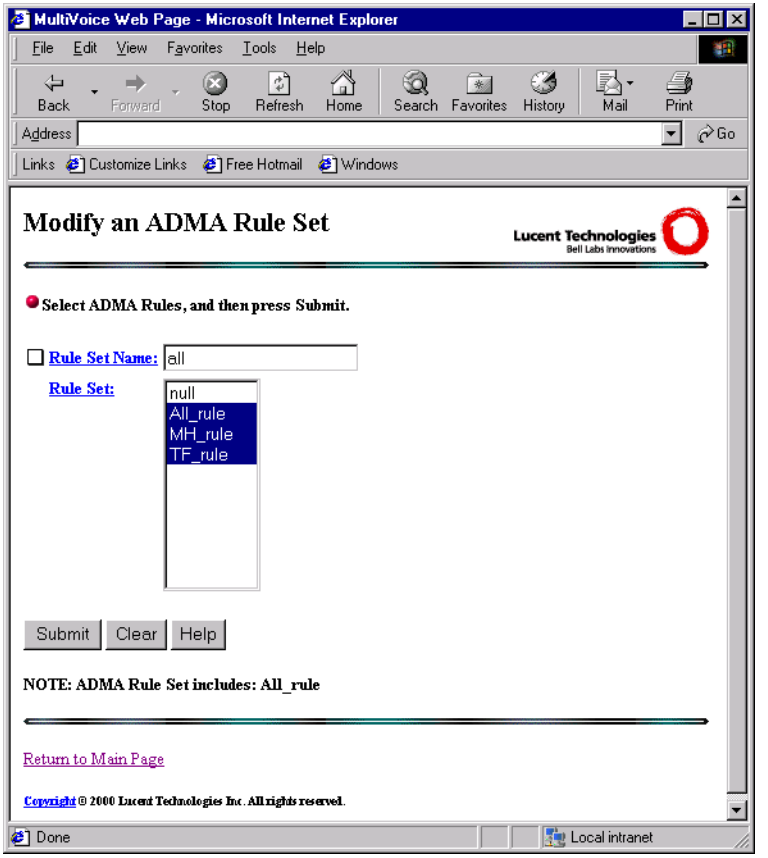
Figure 5-12. Select an ADMA Rule Set to modify page



2 Click the name of the ADMA Rule Set you wish to modify. (For a longer list, the screen has a scroll bar at its right edge.)

The Access Manager displays the selected ADMA Rule Sets record on the Modify the ADMA Rule Set page, and lists, in a Note, the ADMA Rules included in the ADMA Rule Set to be modified, as illustrated in Figure 5-13:

Figure 5-13. Modify an ADMA Rule Set page

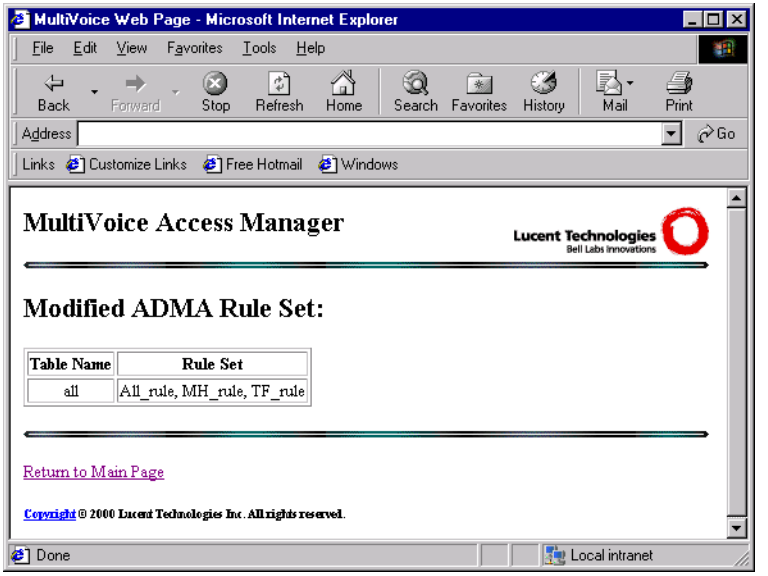


3 Change your selection of ADMA Rules in the Rule Sets pull-down list.

4 To save the settings, click the Submit button.

The Access Manager confirms the saved changes by displaying the Modified ADMA Rule Set page, as illustrated by Figure 5-14. The Rule Set selected will appear in the Rule Set column.

Figure 5-14. Modified ADMA Rule Sets page



Selecting an ADMA Rule Set using wildcard searches

The wildcard character “%” is supported in all fields of the Gateway, Gatekeeper, Terminal, ADMA, and User search forms. For example, entering “d%” in the Rule Set Name field on a search form will cause all rule sets whose names begin with “d” to be displayed. Once the search criteria is entered, click the Submit button. MVAM will search its Rule Sets database and return the rule sets found that match your search criteria.

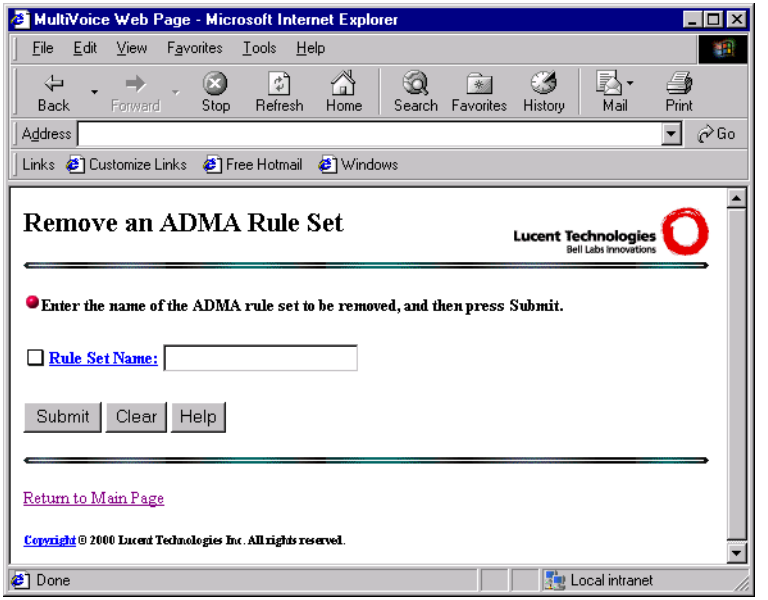
Removing an ADMA Rule Set

The Remove an ADMA Rule Set page, as illustrated in Figure 5-15, deletes one or more ADMA Rule Set records from the Access Manager’s Rule Sets database.

This is accomplished by entering one or more ADMA Rule Set Names in the edit field, separating each by a comma, then clicking the Submit button.

Note: A comma is the only valid delimiter when removing multiple entries. Entering a comma and a space between entries will return an error message.

Figure 5-15. Remove an ADMA Rule Set page



To remove an ADMA Rule Set record, enter the following information on this page:

Parameter	Description
Rule Set Name	This is a 50-character (maximum), alpha-numeric, case-sensitive string which uniquely identifies an ADMA Rule Set.

Note: Removing an ADMA Rule Set will cause any ADMA Gateway/Trunk Rule that references the specified rule set to be automatically removed from the Gateway/Trunk Rules database.

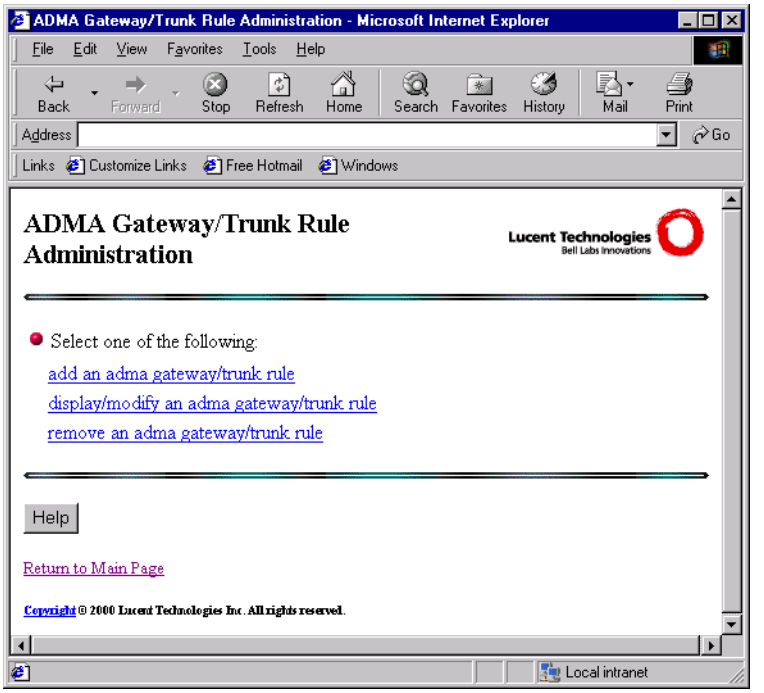
ADMA Gateway/Trunk Rules

ADMA Gateway/Trunk Rules associate a specific Gateway and trunk with an ADMA Rule Set. The ADMA Rule Set is applied to any call arriving over the Gateway/Trunk whose DNIS matches a DNIS Prefix of one of the ADMA Rules.

From the ADMA Gateway/Trunk Rule Administration page as shown in Figure 5-16, you can:

- Add an ADMA Gateway/Trunk Rule to the Gateway/Trunk Rules database
- Display and modify an ADMA Gateway/Trunk Rule
- Remove an ADMA Gateway/Trunk Rule from the Gateway/Trunk Rules database

Figure 5-16. ADMA Gateway/Trunk Rule Administration page



From the ADMA Gateway/Trunk Rule Administration page, the hyperlinks point to the following:

Option	Description
add an ADMA Gateway/trunk rule	This option adds a new ADMA Gateway/Trunk Rule to the Gateway/Trunk Rules database.
display/modify an ADMA Gateway/trunk rule	This option is used to display and modify ADMA Gateway/Trunk Rule information retrieved from the Gateway/Trunk Rules database.
remove an ADMA Gateway/trunk rule	This option is used to remove an existing ADMA Gateway/Trunk Rule from the Gateway/Trunk Rules database.

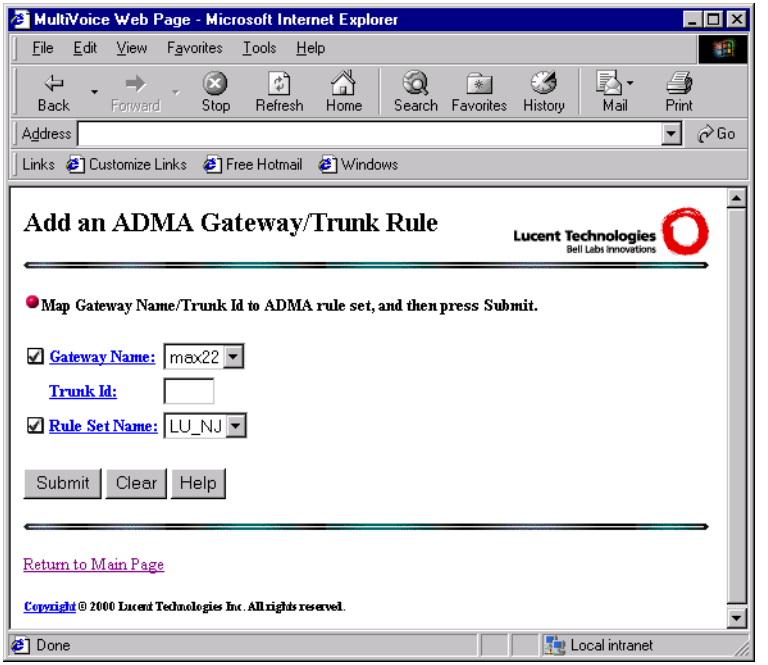
Note: You can get on-line help for the screen by clicking the Help button, or for specific fields by clicking any underlined field name.

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.

Adding an ADMA Gateway/Trunk Rule

The Add an ADMA Gateway/Trunk Rule page, illustrated in Figure 5-17, is used to add a new ADMA Gateway/Trunk Rule to the Access Manager's Gateway/Trunk Rules database. This is accomplished by specifying a Gateway, a Trunk ID, and a Rule Set Name.

To save the new ADMA Gateway/Trunk Rule, click the Submit button.



To add an ADMA Gateway/Trunk Rule, specify the following values on this page:

Parameter	Description
Gateway Name	This is pull-down list of all administered Gateways on the MVAM. Only one Gateway may be selected.

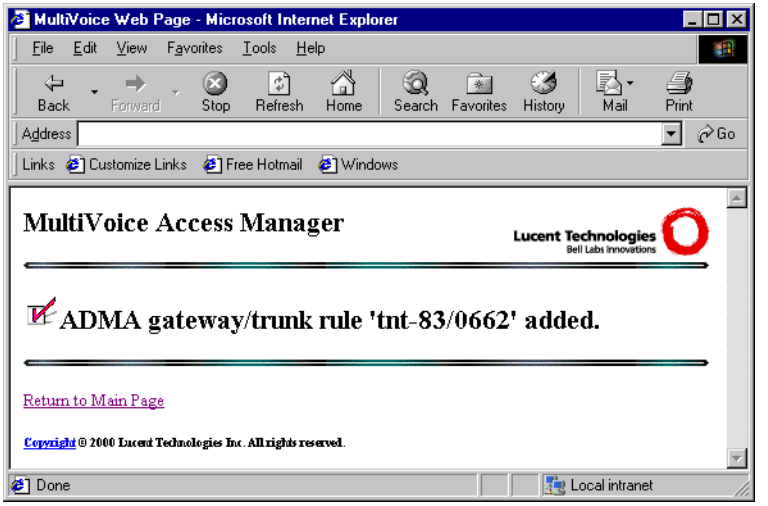
Parameter	Description
Trunk ID	This is a numeric field that specifies the trunk group on the Gateway selected that will be associated with the Rule Set selected. **Note:** The Trunk ID specified must be a defined trunk group on the specified Gateway. If the value for the Trunk ID is unspecified (default), all trunks on the Gateway selected will be associated with the Rule Set Name selected. This field supports 4 digits. The value of each digit may be 0-9.
Rule Set Name	This is a pull-down list of all ADMA Rule Sets administered on the MVAM. Only one Rule Set may be selected.

Once you select the Gateway Name (required) and Rule Set Name (required), and enter a Trunk ID (optional), click the Submit button to save this ADMA Gateway/Trunk Rule.

Saving the settings

Changes to the Gateway/Trunk Rules database 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 screen. A confirmation message, as shown in Figure 5-17, displays indicating that the ADMA Gateway/Trunk Rule was added successfully. If the rule could not be added, an error message will display.

Figure 5-17. Addition of ADMA Gateway/Trunk Rule Confirmed

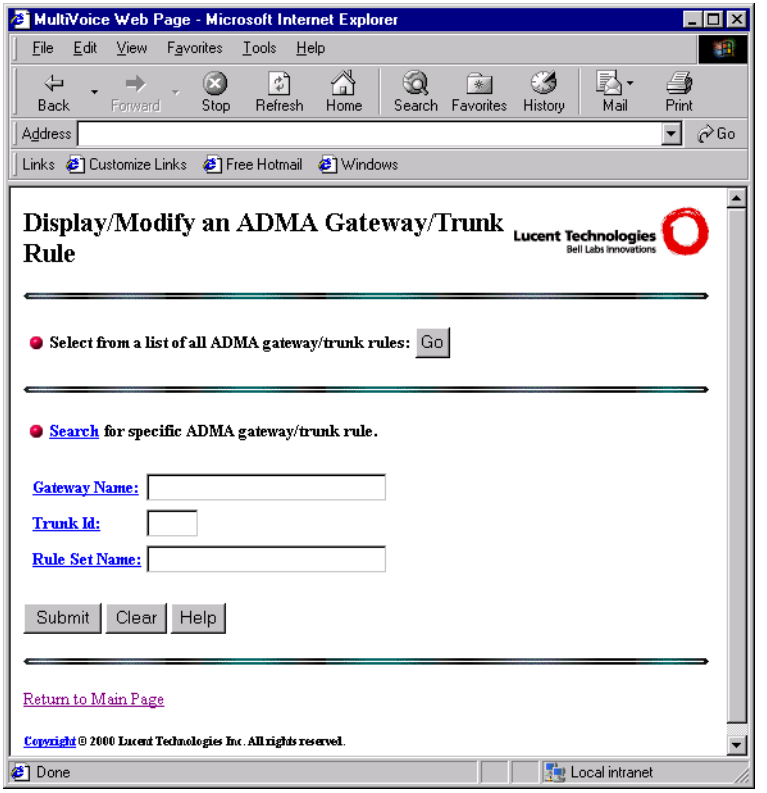


Displaying and modifying ADMA Gateway/Trunk Rules

The Display/Modify an ADMA Gateway/Trunk Rule page, illustrated in Figure 5-18, is used to select an existing ADMA Gateway/Trunk Rule, which is stored on the Access Manager. Selection may be done by either:

- Clicking the Go button to display a list of all ADMA Gateway/Trunk Rules; then clicking one of the Gateway Name hyperlinks to retrieve that information.
- Entering a Gateway Name, Trunk ID, and/or Rule Set Name (or search strings for these fields) on this page; then clicking the Submit button.

Figure 5-18. Display/Modify an ADMA Gateway/Trunk Rule page



To retrieve an ADMA Gateway/Trunk Rule, enter one or more of the following values on this page:

Parameter	Description
Gateway Name	This is pull-down list of all administered Gateways on the MVAM. Only one Gateway may be selected.

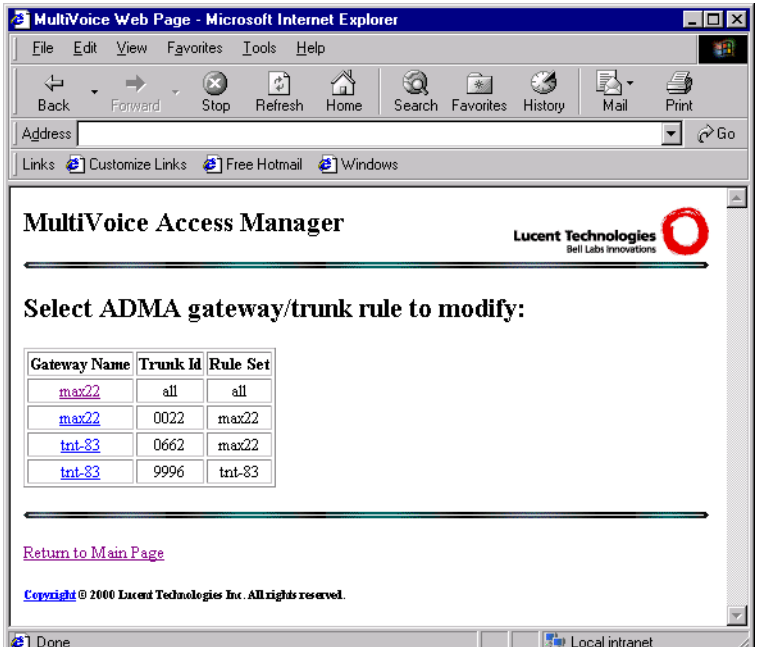
Parameter	Description
Trunk ID	This is a numeric field that specifies the trunk group on the Gateway selected that will be associated with the Rule Set selected. **Note:** The Trunk ID specified must be a defined trunk group on the specified Gateway. If the value for the Trunk ID is unspecified (default), all trunks on the Gateway selected will be associated with the Rule Set Name selected. This field supports 4 digits. The value of each digit may be 0-9.
Rule Set Name	This is a pull-down list of all ADMA Rule Sets administered on the MVAM. Only one Rule Set may be selected.

Selecting from a list of all ADMA Gateway/Trunk Rules

To select a ADMA Gateway/Trunk Rule record from a list of known ADMA Gateway/Trunk Rules:

1 From the Display/Modify an ADMA Gateway/Trunk Rule page, click the Go button. A list of all ADMA Gateway/Trunk Rules appears, as illustrated in Figure 5-19:

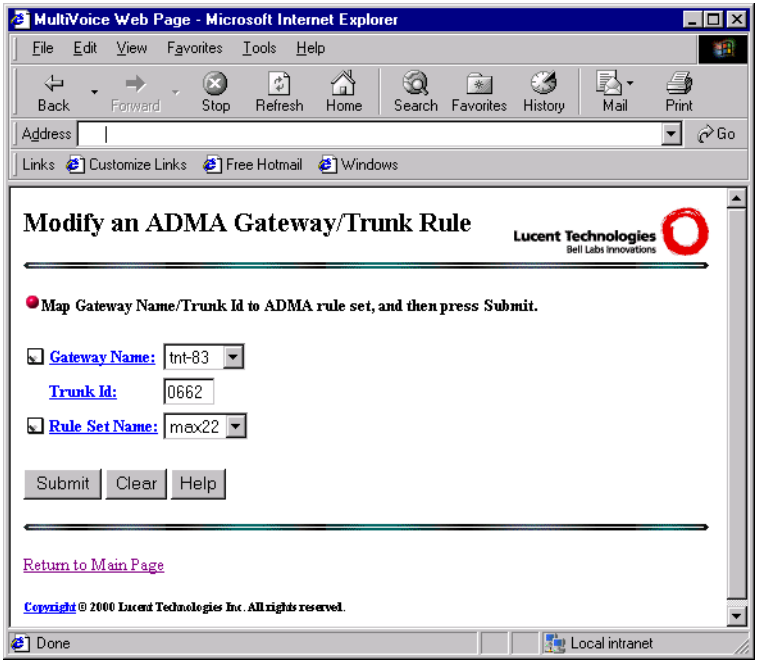
Figure 5-19. Select an ADMA Gateway/Trunk Rule to modify page



2 Click the Gateway name of the ADMA Gateway/Trunk Rule you wish to modify. (For a longer list, the screen has a scroll bar at its right edge.)

The Access Manager displays the selected ADMA Gateway/Trunk Rules record on the Modify the ADMA Gateway/Trunk Rule page, as illustrated in Figure 5-20:

Figure 5-20. Modify an ADMA Gateway/Trunk Rule page

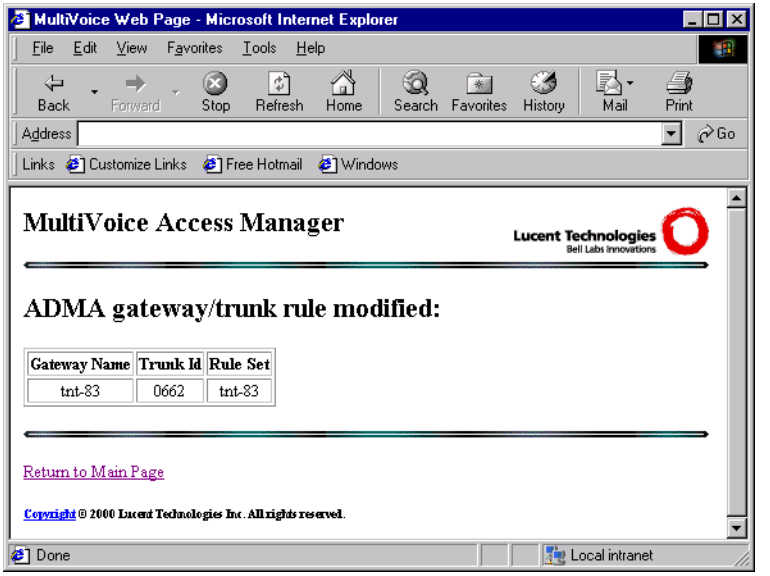


3 Modify the Rule Set Name by changing the selection in the pull-down list of Rule Set Name.

4 To save the settings, click the Submit button.

The Access Manager confirms the saved changes by displaying the Modified ADMA Gateway/Trunk Rule page, as illustrated by Figure 5-21.

Figure 5-21. Modified ADMA Gateway/Trunk Rules page



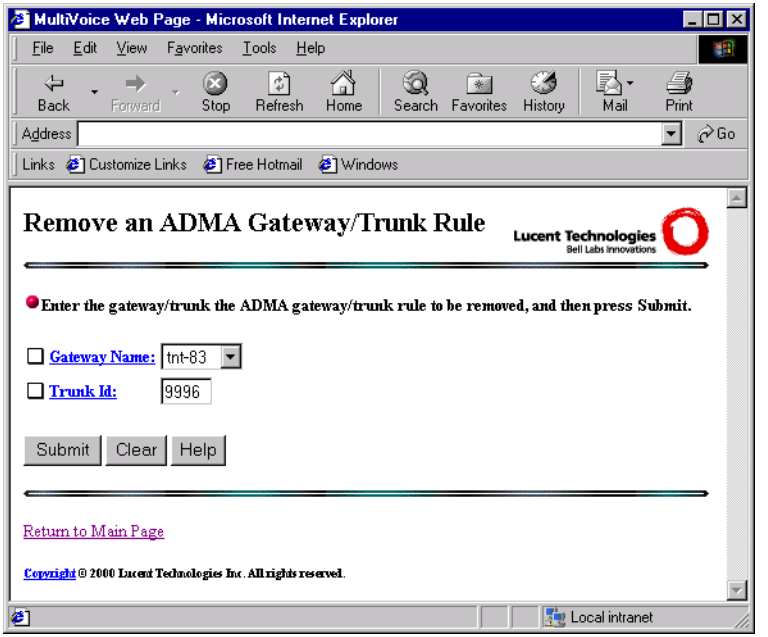
Selecting an ADMA Gateway/Trunk Rule using wildcard searches

The wildcard character "%" is supported in all fields of the Gateway, Gatekeeper, Terminal, ADMA, and User search forms. For example, entering "d%" in the Gateway Name field on a search form will cause all Gateways whose names begin with "d" to be displayed. Once the search criteria is entered, click the Submit button. MVAM will search its Gateway/Trunk Rules database and return the Gateway/Trunk Rules that match your search criteria.

Removing an ADMA Gateway/Trunk Rule

The Remove an ADMA Gateway/Trunk Rule page, as illustrated in Figure 5-22, deletes an ADMA Gateway/Trunk Rule record from the Access Manager's Gateway/Trunk Rules database. This is accomplished by selecting a Gateway Name and entering an associated Trunk ID, then clicking the Submit button.

Figure 5-22. Remove an ADMA Gateway/Trunk Rule page



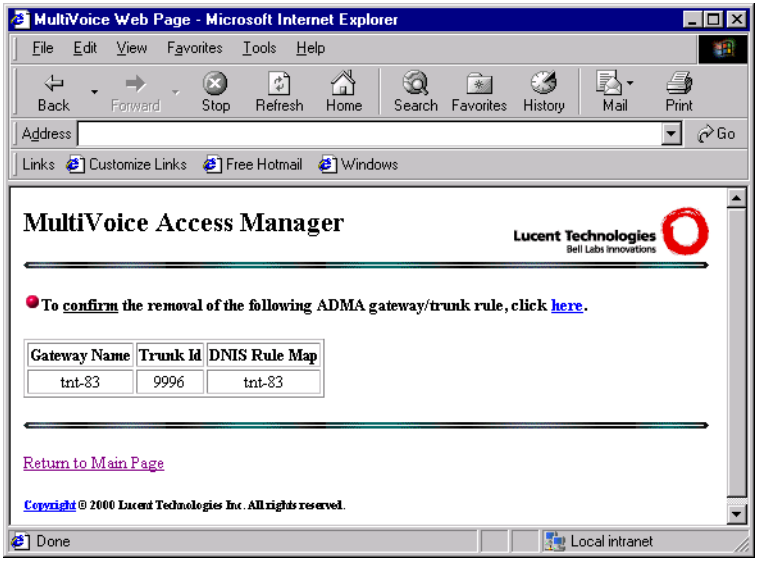
To remove an ADMA Gateway/Trunk Rule record, enter the following information on this page:

Parameter	Description
Gateway Name	This is pull-down list of all administered Gateways on the MVAM. Only one Gateway may be selected.
Trunk ID	This is a numeric field that specifies the trunk group on the Gateway selected that will be associated with the Rule Set selected. **Note:** The Trunk ID specified must be a defined trunk group on the specified Gateway. If the value for the Trunk ID is unspecified (default), all trunks on the Gateway selected will be associated with the Rule Set Name selected. This field supports 4 digits. The value of each digit may be 0-9.

Note: Only one ADMA Gateway/Trunk Rule may be removed at a time.

After entering the Gateway Name and Trunk ID, click the Submit button. MVAM will check its ADMA databases to match the Gateway/Trunk ID entered with an entry in the Gateway/Trunk Rules database. If a matching entry is found, a verification message will display, as shown in Figure 5-23.

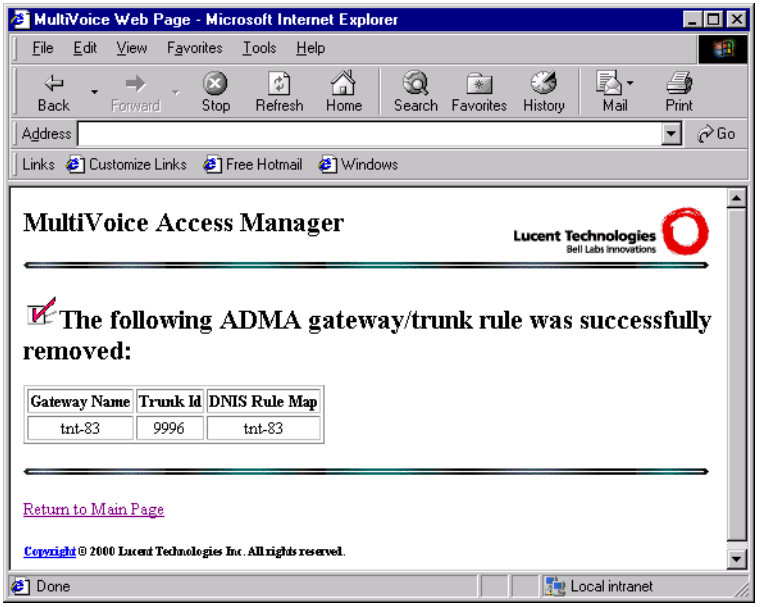
Figure 5-23. Verification to Remove an ADMA Gateway/Trunk Rule



You will be prompted to verify the removal of the ADMA Gateway/Trunk Rule you entered before it is removed from the Gateway/Trunk Rules Database. Click “here” to confirm the removal of the Gateway/Trunk Rule or click the Back button on your browser to return to the Remove an ADMA Gateway/Trunk Rule page.

Once you have confirmed the removal of the Gateway/Trunk Rule, a message displaying the successful removal of the rule is displayed, as shown in Figure 5-24.

Figure 5-24. Removal of ADMA Gateway/Trunk Rule Confirmed



Peer Gatekeeper Administration 6

Gatekeeper-to-Gatekeeper communications. 6-1

Adding a Gatekeeper 6-4

Displaying and modifying Gatekeeper information. 6-8

Displaying and modifying Gatekeeper coverage areas 6-13

Removing a Gatekeeper 6-19

Gatekeeper-to-Gatekeeper communications

The MultiVoice Access Manager supports Gatekeeper-to-Gatekeeper communications. This allows calls to be routed between Gateways which are registered with different Access Managers (Gatekeepers), or in different Gatekeeper virtual zones.

Each Access Manager in a MultiVoice system maintains a database of peer Gatekeepers, which contains a Gatekeeper's identifier (i.e., a unique name) and an associated IP address.

Each peer Gatekeeper is also assigned its own coverage area. These coverage areas define the telephone numbers which a peer Gatekeeper is responsible for covering. Overlapping coverage areas are also supported for Gatekeepers.

From the Access Manager, you can:

- Add peer Gatekeepers to the Gatekeeper database
- Display and modify peer Gatekeeper information

- Display and modify Gatekeeper coverage areas
- Remove Gatekeepers from the MultiVoice network

Note: When you add, modify, or delete Gatekeepers in MVAM, the Gatekeeper Identifier denotes the name the peer Gatekeepers use to identify themselves to other Gatekeepers and Gatekeeper virtual zones configured on your network.

Definition of an H.323 zone

According to the ITU-T H.323 standard, one H.323 Gatekeeper oversees and works with a number of H.323 endpoints. The Gatekeeper and the endpoints associated with it are referred to as an H.323 zone. In previous releases, a MultiVoice Access Manager managed a single zone (itself and many MultiVoice Gateways).

Definition of an Access Manager (Gatekeeper) virtual zone

A Gatekeeper virtual zone is a subset of all MultiVoice Gateways which are administered and registered with a single MultiVoice Access Manager. Each virtual zone is managed by a virtual Gatekeeper which exists on the same server as the Access Manager. Each virtual Gatekeeper has its own set of distinct Gateway, Gatekeeper, terminal, and user databases, which are separate and distinct from other databases maintained for the Access Manager itself, or other virtual Gatekeepers which exist on the same server.

In the Administration section of the MVAM main page, click `gatekeepers`. The Gatekeeper Administration page, as illustrated in Figure 6-1, appears:

Figure 6-1. Gatekeeper Administration page



These hyperlinks point to the following:

Option	Description
add a gatekeeper	This option adds a new peer Gatekeeper to the Gatekeeper database.
display/modify a gatekeeper's general information	This option is used to display and modify Gatekeeper information retrieved from the peer Gatekeeper database.
display/modify a gatekeeper's coverage area	This option is used to display and modify peer Gatekeeper coverage areas retrieved from the Gatekeeper database.
remove a gatekeeper	This option is used to remove one or more existing Gatekeeper from the peer Gatekeeper database.

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

Adding a Gatekeeper

The Add a Gatekeeper page, illustrated in Figure 6-2, is used to add a new peer Gatekeeper to the Access Manager's Gatekeeper database. This is accomplished by entering a Gatekeeper identifier and an IP address for the peer Gatekeeper.

Figure 6-2. Add a Gatekeeper page



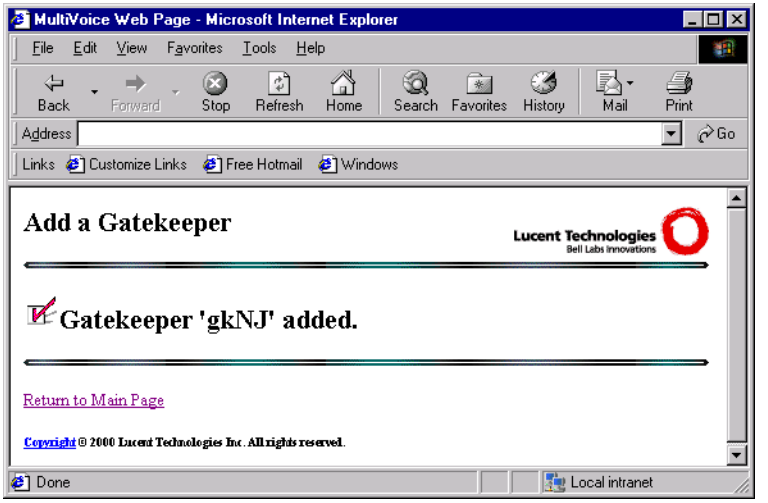
To add a peer Gatekeeper, enter the following values on this page:

Parameter	Description
Gatekeeper Identifier	This is an alpha-numeric string which uniquely identifies a peer Gatekeeper. This is either: • The network name of the Access Manager server for a real H.323 zone, or • The Access Manager name and zone identifier for a Gatekeeper virtual zone.
IP Address	This is the network address assigned to the Access Manager server where the peer Gatekeeper or Gatekeeper virtual zone reside.

Once values have been entered for both fields, click the Submit button to save this peer Gatekeeper.

After the Gatekeeper is added to the Gatekeepers database, a confirmation message displays, as shown in Figure 6-3.

Figure 6-3. Successful addition of Gatekeeper



Saving the settings

Changes to the Gatekeeper database 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 a Gatekeeper Administration screen.

Understanding Gatekeeper databases

For multi-zone call routing to work, each Access Manager must know about the other Gatekeepers on the network, and their respective coverage areas. This information is stored in the Gatekeeper table and Gatekeeper coverage table.

Gatekeeper table

The Gatekeeper table (gk.txt) stores the Gatekeeper identifiers, usually the network name of the Access Manager server, and IP addresses of peer Gatekeepers. The parameters used to identify Gatekeepers in this file must meet the following criteria:

Parameter	Description
Gatekeeper Identifier	This is an alpha-numeric string which uniquely identifies a peer Gatekeeper.
Gatekeeper IP Address[a]	This is the network address assigned to the Access Manager server where the peer Gatekeeper or Gatekeeper virtual zone reside.

a. The same IP address may be used for more than one Gatekeeper Identifier, if the Access Manager at that IP address is configured to support virtual-zone call routing. More than one virtual Gatekeeper would then be associated with an IP address.

A Gatekeeper Identifier may be either of the following:

Value	Description
gkID	This is the name by which the Access Manager is known to the MultiVoice network. This is usually the same as the network name of the system where the Access Manager is installed.
gkID.zone	This identifies a Gatekeeper virtual zone. This consists of the Access Manager name and a zone name which exists on that Access Manager.

Gatekeeper coverage table

The Gatekeeper coverage table (gkc.txt) stores the coverage information for the gatekeepers in the Gatekeeper table. The parameters used to identify Gatekeepers in this file must meet the following criteria:

Parameter	Description
Gatekeeper Identifier	This is an alpha-numeric string which uniquely identifies a peer Gatekeeper.
Coverage Area[a]	A Coverage Area, or calling area, defines the telephone numbers where a peer Gatekeeper can connect calls. It consists of a set of Inclusion Areas, which, in combination, identify all of the telephone numbers which may be routed through a peer Gatekeeper.

a. The same rules concerning the size and formatting of Gateway coverage areas are applied to these Gatekeeper coverage areas.

Note: For more information on coverage areas, see “Displaying and modifying coverage areas” on page 4-18.

The database files, `gk.txt` and `gkc.txt`, may be populated on one Access Manager and then manually copied to the other Access Managers or Gatekeeper virtual zones.

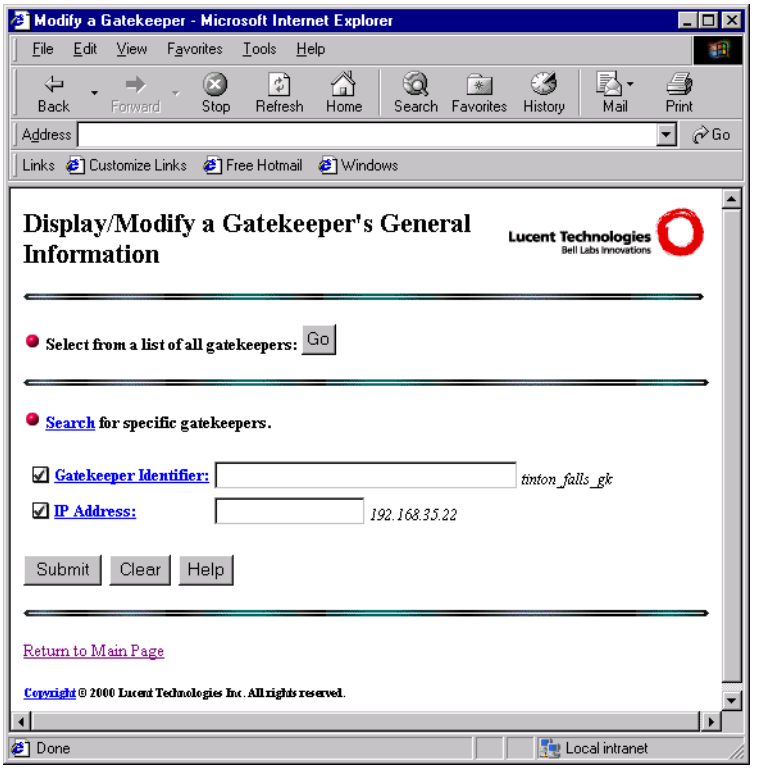
Displaying and modifying Gatekeeper information

The Display/Modify a Gatekeeper’s General Information page, illustrated in Figure 6-4, is used to select an existing peer Gatekeeper’s record, which is stored on the Access Manager. Selection may be done by either:

- Clicking the Go button to display a list of all peer Gatekeepers records; then clicking one of the Gatekeeper Identifier hyperlinks to retrieve that information.

- Entering a Gatekeeper identifier, a Gatekeeper IP address, or search strings on this page; then clicking the Submit button.

Figure 6-4. Display/Modify a Gatekeeper's General Information page



To retrieve a peer Gatekeeper, enter the following values on this page:

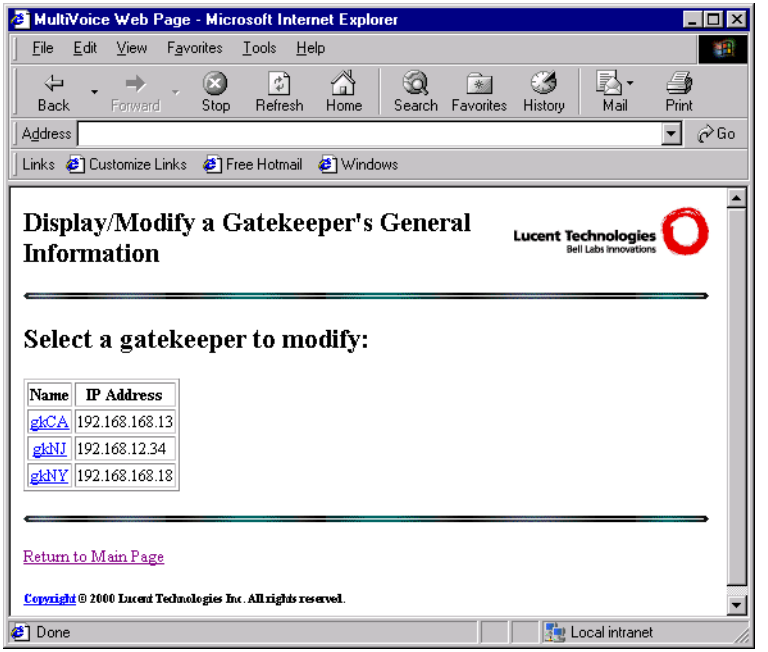
Parameter	Description
Gatekeeper Identifier	This is an alpha-numeric string which uniquely identifies a peer Gatekeeper. This is either: • The network name of the Access Manager server for a real H.323 zone, or • The Access Manager name and zone identifier for a Gatekeeper virtual zone.
IP Address	This is the network address assigned to the Access Manager server where the peer Gatekeeper or Gatekeeper virtual zone reside.

Selecting from a list of all gatekeepers

To select a Gatekeeper record from a list of known peer Gatekeepers:

1 From the Display/Modify a Gatekeeper's General Information page, click the Go button. A list of all Gateways appears, as illustrated in Figure 6-5:

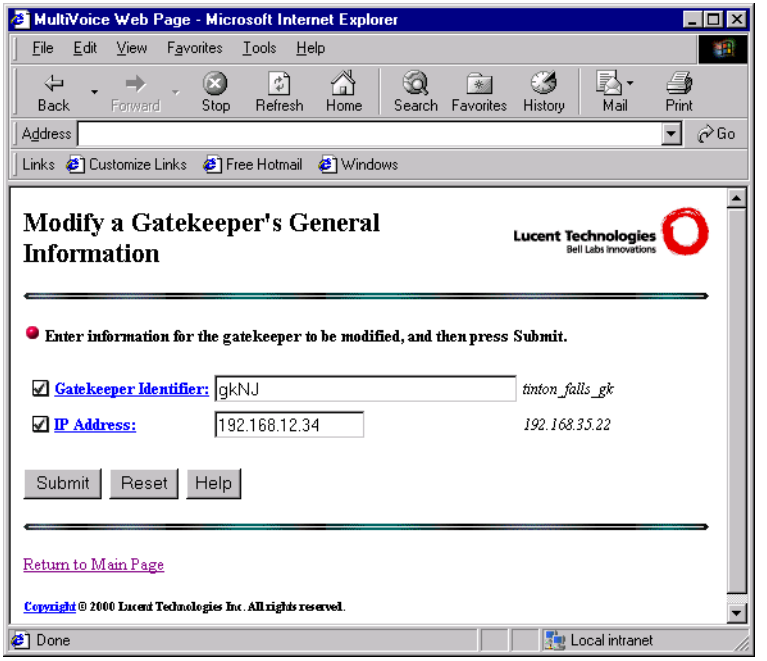
Figure 6-5. Select a Gatekeeper to modify page



2 Click the name of the Gatekeeper you wish to modify. (For a longer list, the screen has a scroll bar at its right edge.)

The Access Manager displays the selected Gatekeeper record on the Modify a Gatekeeper's General Information page, as illustrated in Figure 6-6:

Figure 6-6. Modify a Gatekeeper's General Information page

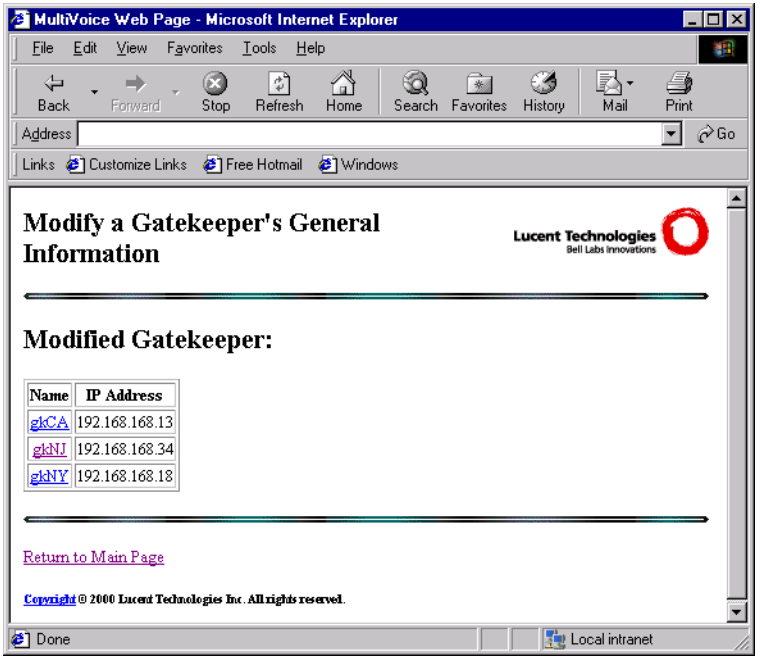


3 Modify any field by typing in the new information.

4 To save the settings, click the Submit button.

The Access Manager confirms the saved changes by displaying the Modified Gatekeeper information page, as illustrated by Figure 6-7. The changes appear next to the Name hyperlink of the modified Gatekeeper.

Figure 6-7. Modified Gatekeeper page



Selecting a gatekeeper using wildcard searches

The wildcard character “%” is supported in all fields of the Gateway, Gatekeeper, Terminal, ADMA, and User search forms. For example, entering “d%” in the Gatekeeper Identifier field on a search form will cause all Gatekeepers whose Gatekeeper Identifiers begin with “d” to be displayed. Once values have been entered for both fields, click on Submit to save this peer Gatekeeper.

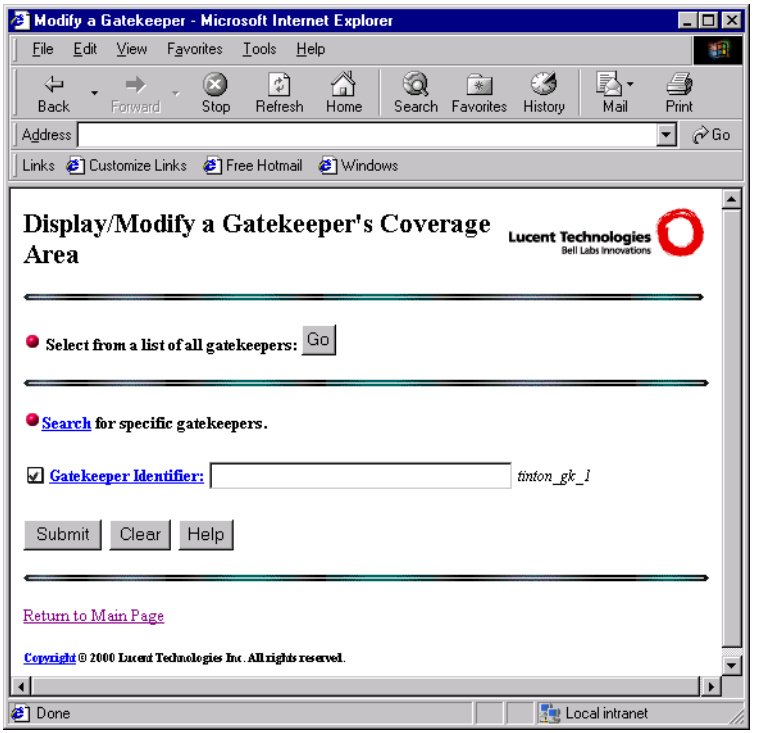
Displaying and modifying Gatekeeper coverage areas

The Display/Modify a Gatekeeper Coverage Areas option is used to select a peer Gatekeeper coverage area, and subsequently add or delete inclusion areas.

The Display/Modify a Gatekeeper's Coverage Area page, illustrated in Figure 6-8, is used to select an existing peer Gatekeeper's coverage area by either:

- Clicking the Go button to display a list of all peer Gatekeepers' coverage area; then clicking one of the Gatekeeper identifiers hyperlinks to retrieve that table.
- Entering a Gatekeeper Identifier on the screen; then clicking the Submit button.

Figure 6-8. Display/Modify a Gatekeeper's Coverage Area page

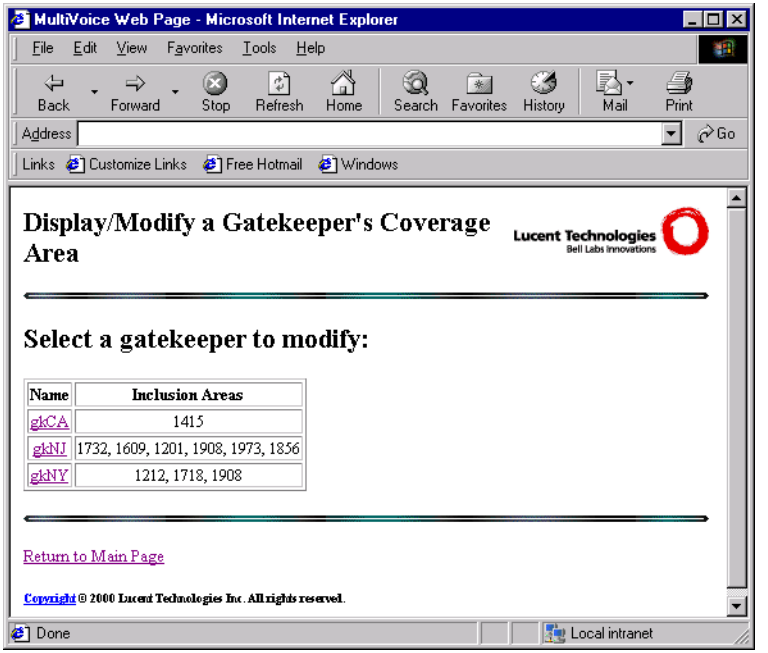


Selecting from a list of all Gatekeeper coverage areas

To select a Gatekeeper from a list of all Gatekeeper coverage areas:

1 From the Display/Modify a Gatekeeper's Coverage Area page, click the Go button. A list of all Gatekeepers and their coverage areas appears, as illustrated in Figure 6-9:

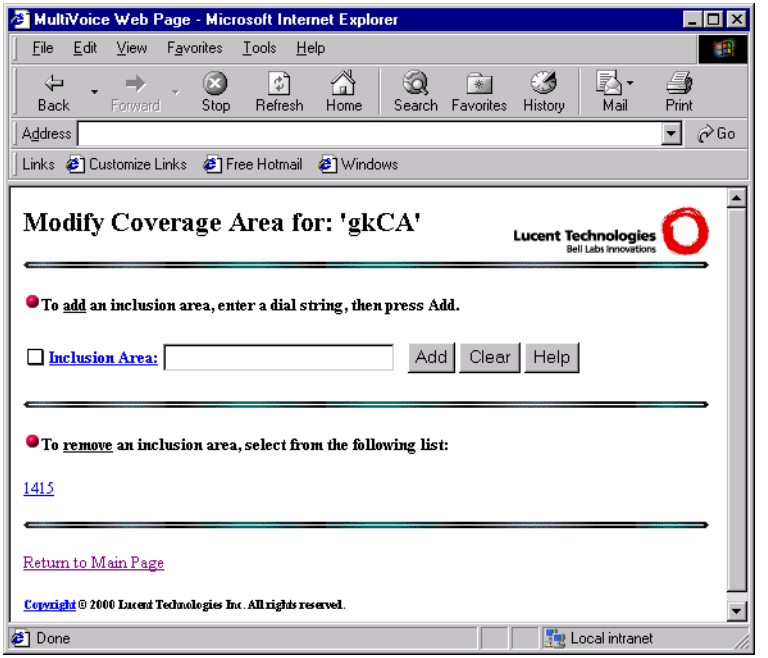
Figure 6-9. Select a Gatekeeper to modify page



2 Click the hyperlink for a displayed Gatekeeper. (For a longer list, the screen has a scroll bar at its right edge.)

The Access Manager displays the selected Gatekeeper's coverage areas on the Modify Coverage Area for a specific Gatekeeper page, as illustrated in Figure 6-10:

Figure 6-10. Modify Coverage Area for a Gatekeeper page



Once the peer Gatekeeper coverage area is retrieved, the Access Manager will display the inclusion areas for the Gatekeeper selected.

To add a new inclusion area, enter the following information on this page:

Parameter	Description
Inclusion Area	This is a numeric string which uniquely identifies the destination telephone numbers which are connected through the selected Gatekeeper. It is specified by a Complete or Partial Telephone Number.

Once you have entered this information, click the Submit button to save it in the Gatekeeper coverage area database.

Adding an Inclusion Area

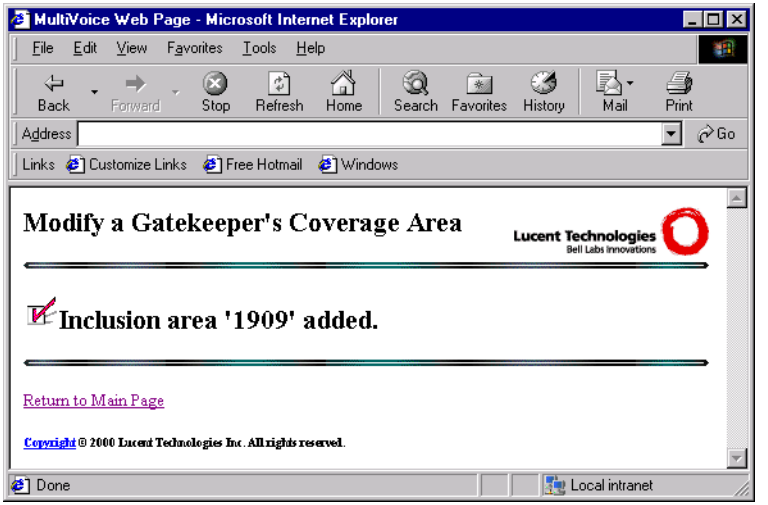
To add Inclusion Areas for a Gatekeeper coverage area:

1. From the Display/Modify a Gatekeeper's Coverage Area page, click the Go button. A list of known peer Gatekeepers with their associated coverage areas appears, as illustrated in Figure 6-9.
2. Click the hyperlink for a displayed Gatekeeper.

   The Access Manager displays the selected Gatekeeper coverage area on the Modify Coverage Area for a Gatekeeper page, as illustrated in Figure 6-10.
3. Add a new Inclusion Area by typing a dial string in the Inclusion Area field.
4. To save your settings, click the Submit button.

   The Access Manager confirms the saved changes by displaying a confirmation message, as illustrated by Figure 6-11:

Figure 6-11. Modified Coverage Area configuration page

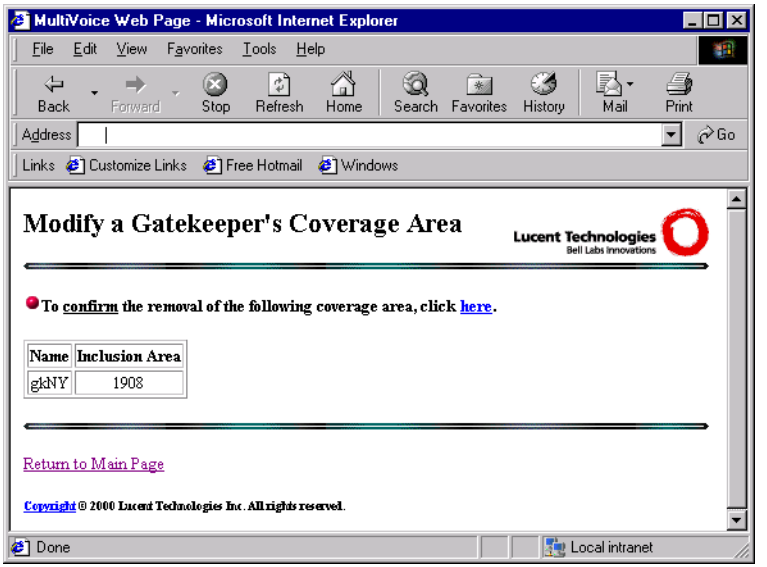


Removing an Inclusion Area

To remove an Inclusion Areas from a Gatekeeper coverage area, click a hyperlink displayed in the list of Inclusion Areas on the Modify Coverage Area for a Gatekeeper page, as illustrated in Figure 6-10.

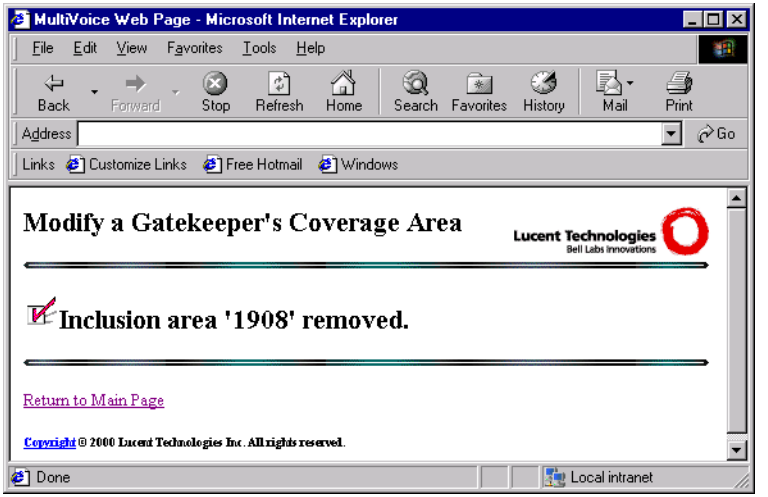
You are required to confirm the removal of the Inclusion Area selected by responding to the message shown in Figure 6-12. To remove the Inclusion Area displayed, click “here”. If you choose to cancel your removal request, you must click your browser’s Back button.

Figure 6-12. Confirm removal of Inclusion Area



After the Inclusion Area is removed from the Gatekeeper Coverage Area database, a confirmation message displays, as shown in Figure 6-13.

Figure 6-13. Successful removal of Inclusion Area



Viewing modified coverage areas

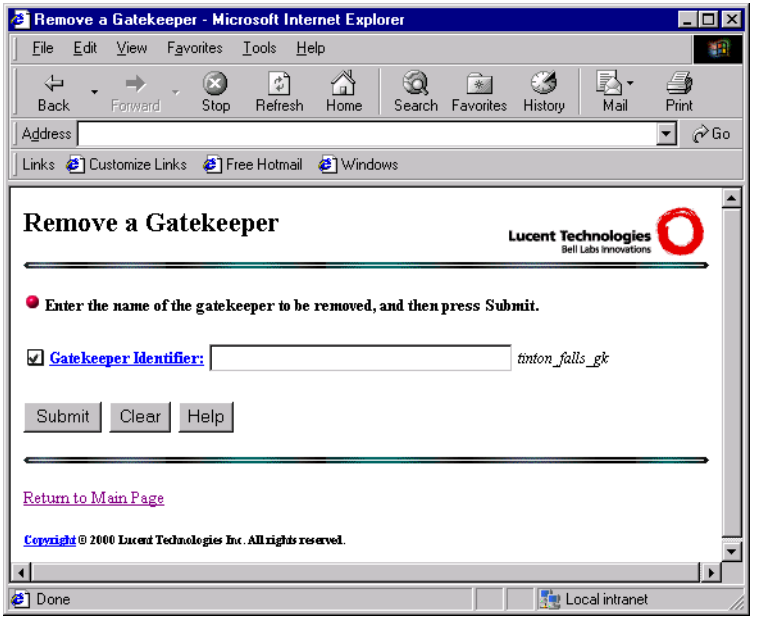
Once you have modified a Gatekeeper's coverage area, click your browser's Back button to display the changes you made. Changes to a Gatekeeper coverage area may not appear until the Modify Coverage Area for a Gatekeeper page is reloaded.

Note: When you modify a coverage area, by either adding or removing Inclusion Areas, clicking the browser's Back button should update the 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.

Removing a Gatekeeper

The Remove a Gatekeeper page, as illustrated in Figure 6-14, deletes a peer Gatekeeper record from the Access Manager's Gatekeeper database. This is accomplished by entering a Gatekeeper Identifier in the edit field, then clicking the Submit button.

Figure 6-14. Remove a Gatekeeper page



To remove a Gatekeeper record, enter the following information on this page:

Parameter	Description
Gatekeeper Identifier	This is an alpha-numeric string which uniquely identifies a peer Gatekeeper in the Gatekeeper database.

Once you have entered this information, click the Submit button to save your changes.

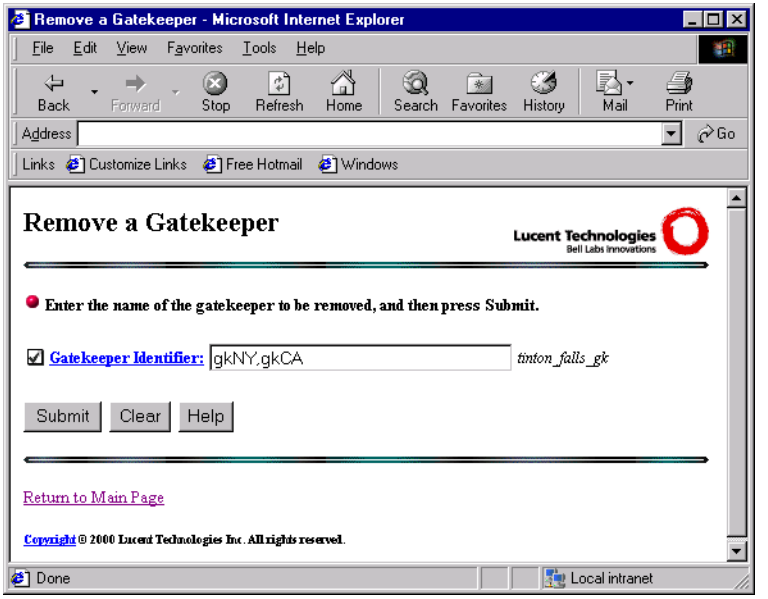
Removing multiple gatekeepers

Multiple Gatekeepers may be removed in one operation by entering the Gatekeeper Identifiers of the Gatekeepers you wish to remove, separating each with a comma, and clicking the Submit button.

Note: A comma is the only valid delimiter. Entering a comma and a space between entries will return an error message.

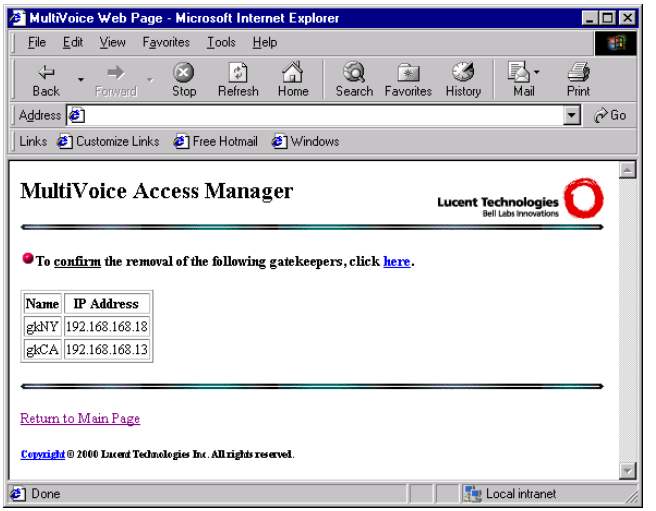
Figure 6-15 shows two Gatekeepers (gkNY and gkCA) in the Gatekeeper Identifier field to be removed from the Gatekeeper database.

Figure 6-15. Removing multiple gatekeepers



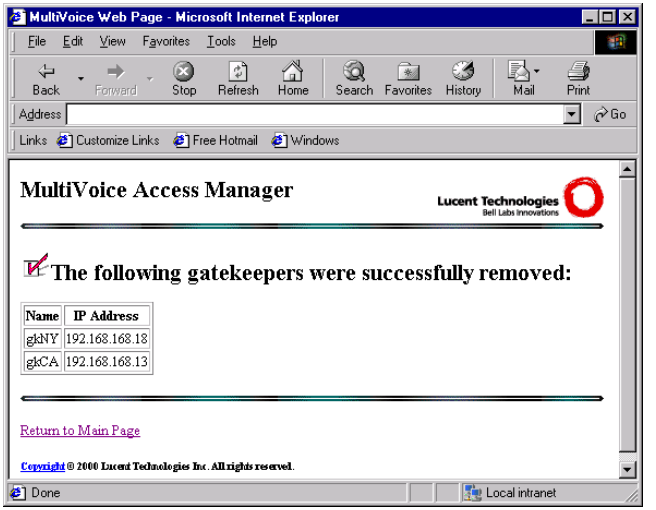
You are required to verify the removal of the gatekeepers entered in the Gatekeeper Identifier field by responding to a removal verification message as shown in Figure 6-16. To remove all of the gatekeepers listed, click “here”. If you choose to cancel your removal request or to make any changes to the list of gatekeepers to be removed, you must click your browser’s Back button.

Figure 6-16. Verify removal of gatekeepers



After each gatekeeper is validated and its record is removed from the Gatekeeper database, a confirmation message displays, as shown in Figure 6-17.

Figure 6-17. Successful removal of gatekeepers



Terminal Administration

7

Adding a Terminal 7-3

Displaying and modifying Terminal information. 7-6

Removing a Terminal 7-11

PC terminals are supported as registered endpoints in a MultiVoice VoIP network. This includes PC terminal administration, registration, and routing. The Access Manager allows provisioning of PC terminal endpoints, as if they were Gateways, through the Web-based administration interface.

Terminals may be administered and authenticated using their H.323 Ids or E.164 addresses in the registration process. This allows the Access Manager to route calls from PC terminals to phones and from phones to PC terminals. Calls to PC terminals are routed using their E.164 address or their coverage area numbers.

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

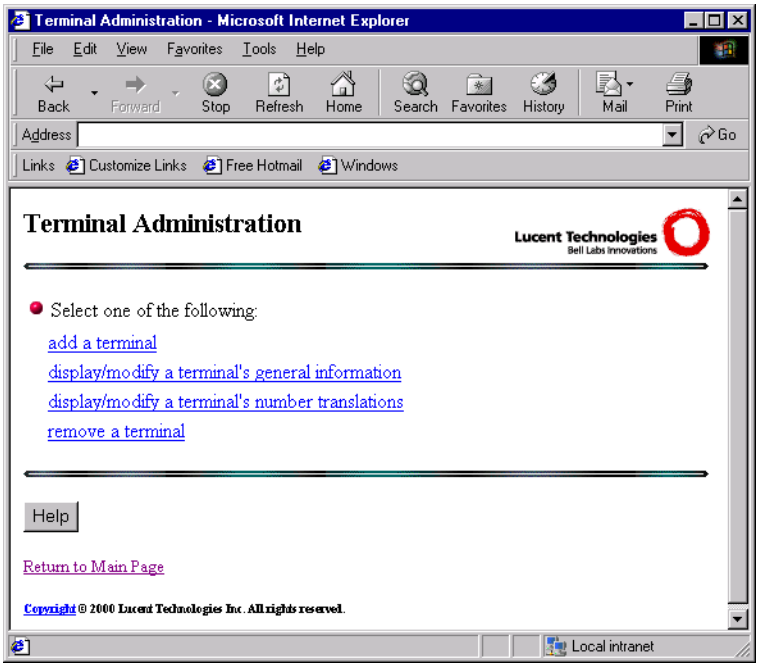
- Registration, Admission and Status (RAS) messaging with a Gatekeeper
- The G.711 audio coder/decoder (required)
- The G.729(a) and G.723.1 audio coder/decoders (optional).

Terminals can be provisioned for a Gatekeeper or a virtual zone. Terminals are identified by using either/both H.323Id or/and E.164 address. Both the H.323Id and E.164 Address information fields are required entries for each terminal record.

When a terminal endpoint sends a registration request, the Access Manager authenticates the terminal using H.323Id or/and E.164 address. Terminals can send H.323Id or/and E.164 address information in their registration request. The Gatekeeper uses either or both H.323Id and E.164 Address information to authenticate the user. When H.323Id information is not sent by the registration request, the Gatekeeper will use the E.164 address information to verify the terminal.

In the Administration section of the MVAM main screen, click `terminals`. The Terminal Administration page, as illustrated in Figure 7-1, appears:

Figure 7-1. Terminal Administration Page



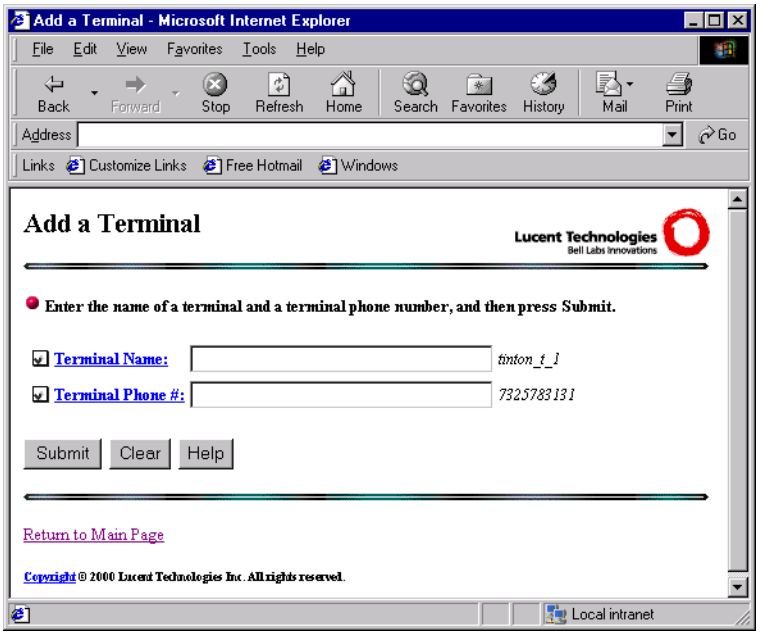
The Terminal Administration menu provides the following options:

Option	Description
add a terminal	This option is used to add an H.323 compliant terminal (PC), for PC-to-phone call routing, to the Terminal Database. Both a Terminal Name and a Terminal Phone are required to add the terminal to the database.
display/modify a terminal's general information	This option is used to retrieve and modify the contents of a Terminal Database record.
display/modify the terminal number translations	This option is used to retrieve and modify the assigned ingress number translation table. This number translation table is used by the Access Manager for routing in-bound calls from this terminal.
remove a terminal	This option is used to delete one or more H.323 compliant terminals (PC) from the Terminal Database.

Adding a Terminal

The Add a Terminal page, illustrated in Figure 7-2, is used to add new H.323-compliant terminals to the Access Manager's terminal database. This is accomplished by entering a Terminal Name and Terminal Telephone on this page.

Figure 7-2. Add a Terminal page



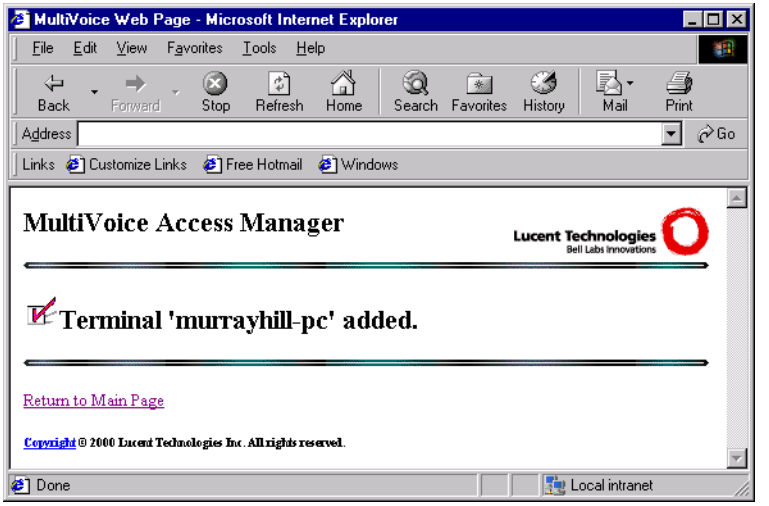
To add a terminal, enter the following values on this page:

Parameter	Description
Terminal Name	This is an alpha-numeric string which uniquely identifies an H.323-compliant terminal. This should be the identification string sent by the PC client when it sends an admission or registration request to the Access Manger. • Examples: `jane-pc`, `neptune-pc`
Terminal Phone #	This is the fully qualified E.164 address associated with this PC client. This is a minimum of eight (8) characters.

Once values have been entered for both fields, click the Submit button to save this terminal.

After the terminal is added to the Terminals database, a confirmation message displays, as shown in Figure 7-3.

Figure 7-3. Successful addition of Terminal



Understanding Terminal databases

The Terminal Database is used to maintain records of all the administered H.323 compliant terminals which are administered by this Access Manager. These records include the following required information:

Parameter	Description
Terminal Name	This is an alpha-numeric string which uniquely identifies an H.323-compliant terminal.
Terminal Phone #	This is the fully qualified E.164 address associated with this PC client.

This information is used by the Access Manager for authenticating registration and admission request (RAS) messages from the PC client.

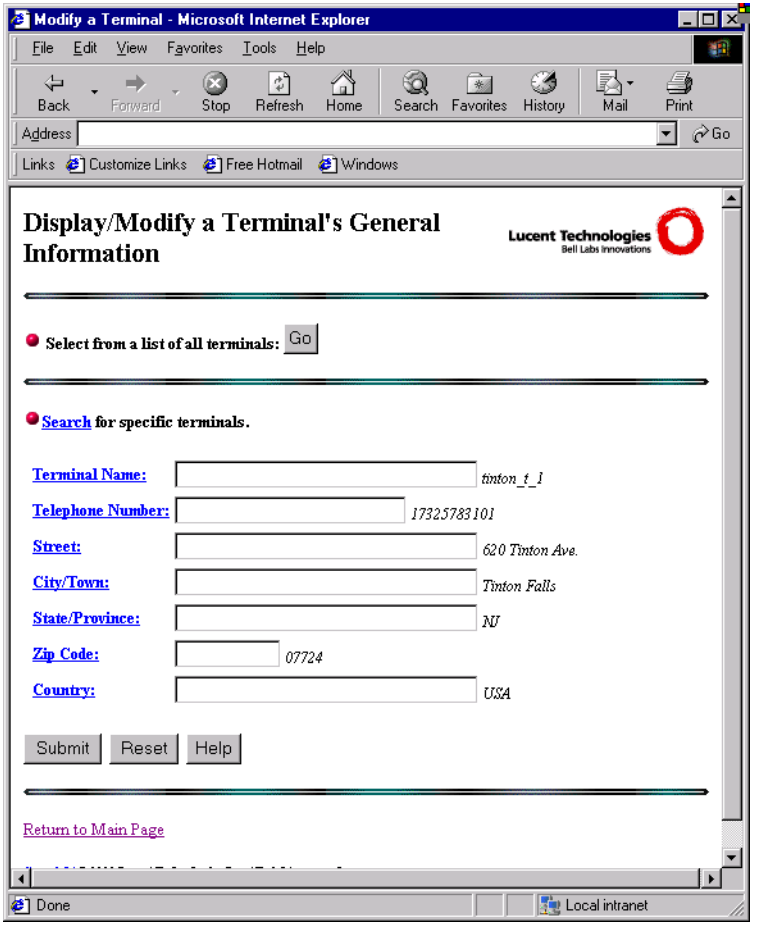
Optional administrative information which may be included for each terminal includes location information (i.e., street address, city, state/province, county, zip/postal code).

Displaying and modifying Terminal information

The Display/Modify a Terminals's General Information page, illustrated in Figure 7-4, is used to select an existing terminal record, which is stored on the Access Manager. Selection may be done by either:

- Clicking the Go button to display a list of all terminal records; then clicking on one of the terminal identifier hyperlinks to retrieve that information.
- Entering a Terminal Name, a Telephone Number, address information, or search strings on this page; then clicking the Submit button.

Figure 7-4. Display/Modify a Terminal's General Information page



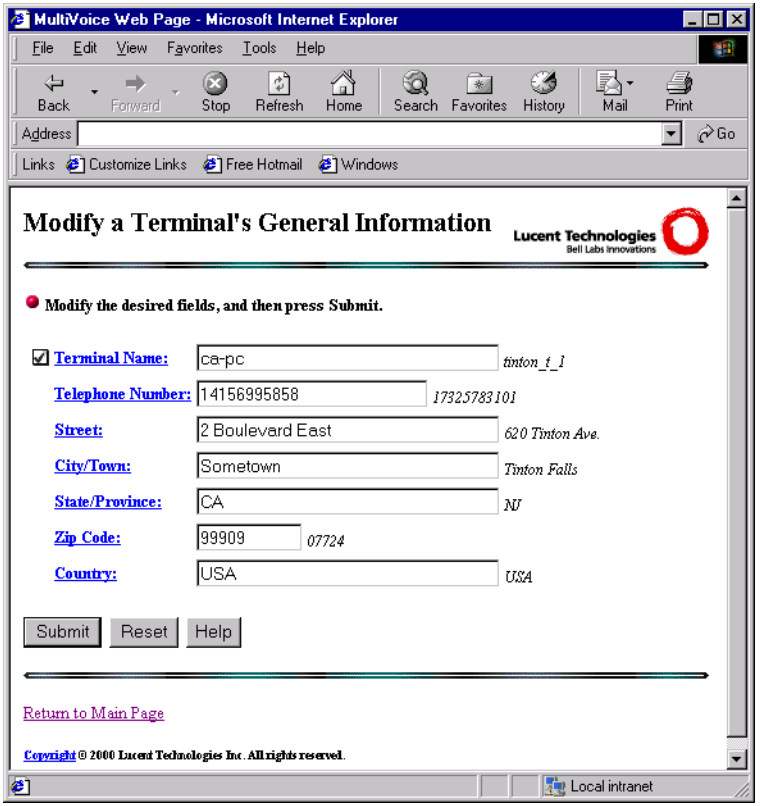
To retrieve a terminal, enter the following values on this page:

Parameter	Description
Terminal Name	This is an alpha-numeric string which uniquely identifies an H.323 compliant terminal. This should be the identification string sent by the PC client when it sends an admission or registration request to the Access Manger. • Examples: `jane-pc`, `neptune-pc`
Telephone Number	This is the fully qualified E.164 address associated with this PC client. This is a minimum of eight (8) characters
Street	This is the address associated with this terminal's premises/location.
City/Town	This is the city, town, or municipality associated with this terminal's premises/location.
State/Province	This is the state, province, or region associated with this terminal's premises/location.
Zip Code	This is the zip or postal code associated with this terminal's premises/location.
Country	This is the country associated with this terminal's premises/location.

The wildcard character "%" is supported in all fields of the Gateway, Gatekeeper, Terminal, ADMA, and User search forms. For example, entering "d" in the Terminal Name field on a search form will cause all terminals whose names begin with "d" to be displayed.

Once a terminal is selected, the Access Manager will display the associated terminal record on the Modify a Terminal's General Information page, as illustrated in Figure 7-5:

Figure 7-5. Modify a Terminal's General Information page

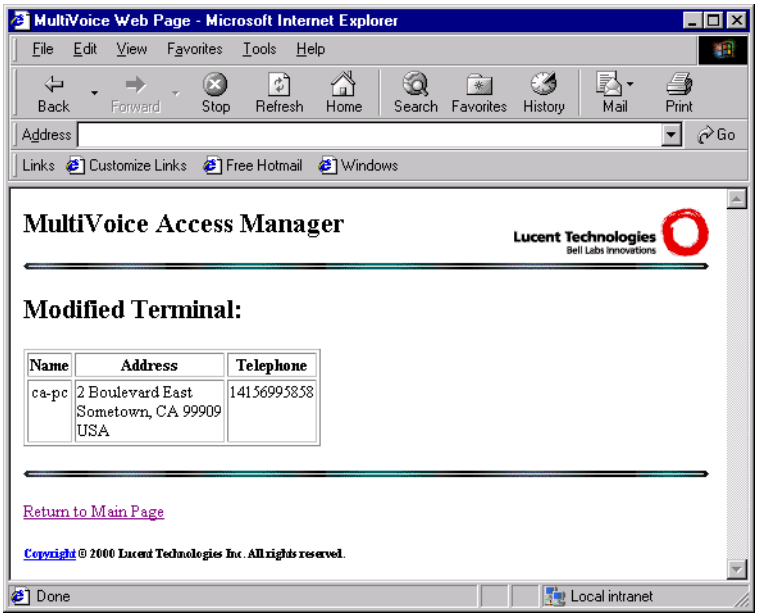


Revise terminal record information by entering information on any of the fields displayed on this page, then click the Submit button to save those changes. Click the Reset button to clear any changes you have made on this page, displaying the original values.

Note: You cannot use the Reset button to erase information already submitted to the database. Once changes are submitted, you must re-enter the old information on the Modify a Terminal form, then click the Submit button to record these changes.

The Access Manager confirms the saved changes by displaying the Modified Terminal information page, as illustrated by Figure 7-6:

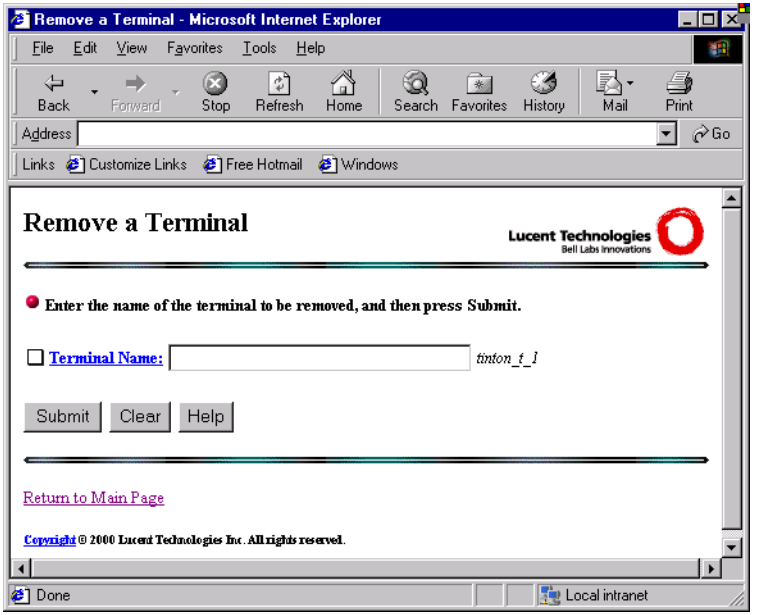
Figure 7-6. Modified Terminal page



Removing a Terminal

The Remove a Terminal page, as illustrated in Figure 7-7, deletes one or more peer terminal records from the Access Manager's terminal database.

Figure 7-7. Remove a Terminal page



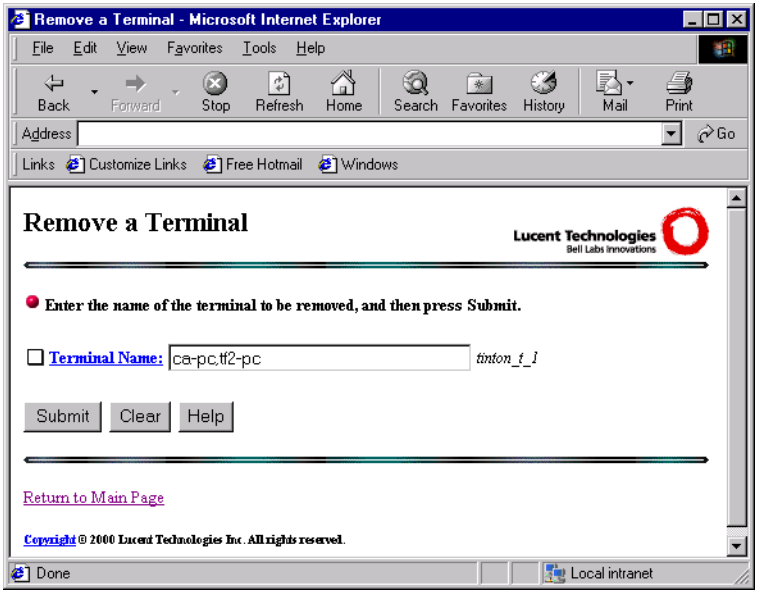
To remove one or more peer terminal records from the MultiVoice Access Manager:

1 In the Terminal Identifier field, enter the Terminal Identifier of the peer terminal you wish to remove. To remove multiple terminals, enter the Terminal Identifier of the terminals you wish to remove, separating each with a comma.

Note: A comma is the only valid delimiter. Entering a comma and a space between entries will return an error message.

Figure 7-8 shows two terminals (ca-pc and tf2-pc) in the Terminal Name field to be removed from the terminal database.

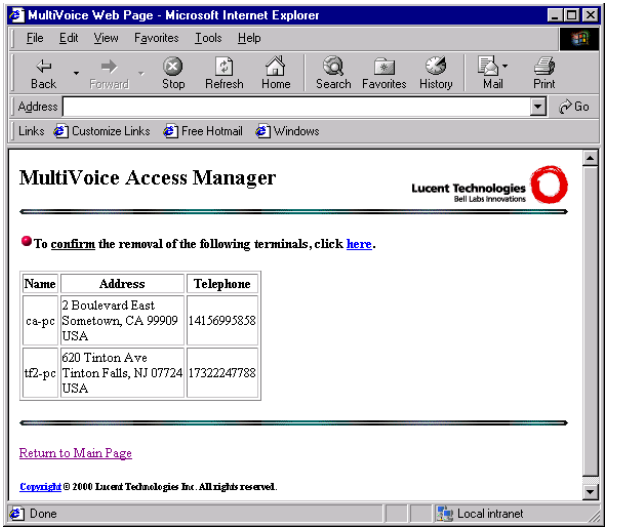
Figure 7-8. Removing multiple terminals



2 Click the Submit button.

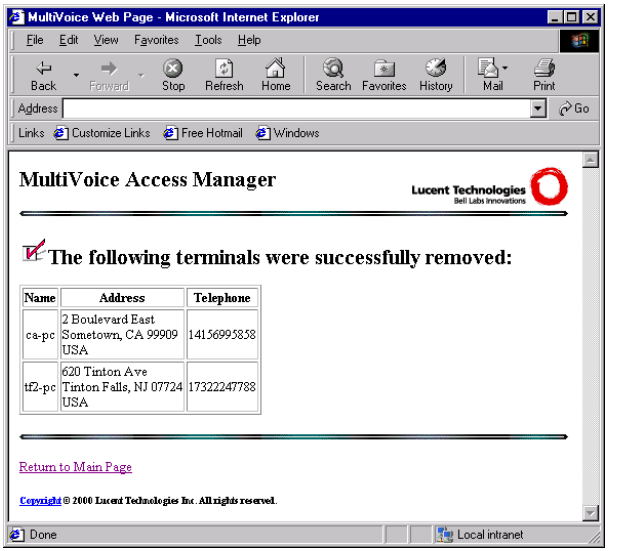
3 After clicking the Submit button, you are required to verify the removal of the terminals entered in the Terminal Name field by responding to a removal verification message as shown in Figure 7-9. To remove all of the terminals listed, click “here”. If you choose to cancel your removal request or to make any changes to the list of terminals to be removed, you must click the Back button on your browser.

Figure 7-9. Verify removal of terminals



After each terminal is validated and its record is removed from the terminal database, a confirmation message displays, as shown in Figure 7-10.

Figure 7-10. Successful removal of terminals



Using Number Translations

8

Digit stripping and number translations 8-1
Adding Number Translation Tables 8-4
Displaying and modifying a Number Translation Table 8-9
Remove a Number Translation Table 8-15
Using number translations with terminals 8-19

Digit stripping and number translations

For long distance and international calls, MultiVoice Access Manager translates the long distance international telephone numbers dialed on the originating Gateway into the local dial string used to complete the call by the destination Gateway.

Translation rules are defined within MVAM and associated with particular Gateways. Each Gateway is assigned an inbound (ingress) and an outbound (egress) translation rule table. The inbound table defines translation rules that convert inbound dialed numbers to canonical form numbers used for coverage area routing, and the outbound table defines rules to convert canonical form numbers to outbound dialed numbers. For PC terminal endpoints, a single, optional inbound translation table may be defined to convert inbound dialed numbers from the PC endpoint to canonical form.

Each Number Translation Table contains a collection of records, which define a search and replace rule (e.g., search for “011” and replace it with “1234”). Using

these tables each Gateway then dials the appropriate telephone number to complete the call.

Number translation processing

When number translation is enabled:

1. The Gateway where the call originates sends the dialed number string to the Access Manager.
2. The Access Manager compares the dialed number string against entries in the inbound translation table, to obtain an intermediate canonical form of the destination telephone number.
3. The Access Manager uses the intermediate canonical form of the destination telephone number to select a destination Gateway, which will connect the call.
4. The Access Manager compares the intermediate canonical destination telephone number to the outbound translation table for the destination Gateway, to produce the actual dialed number string.
5. The destination Gateway dials the translated telephone number.

Number translation table administration

Translation table administration is performed through the Web-based administration interface. Translation table administration includes:

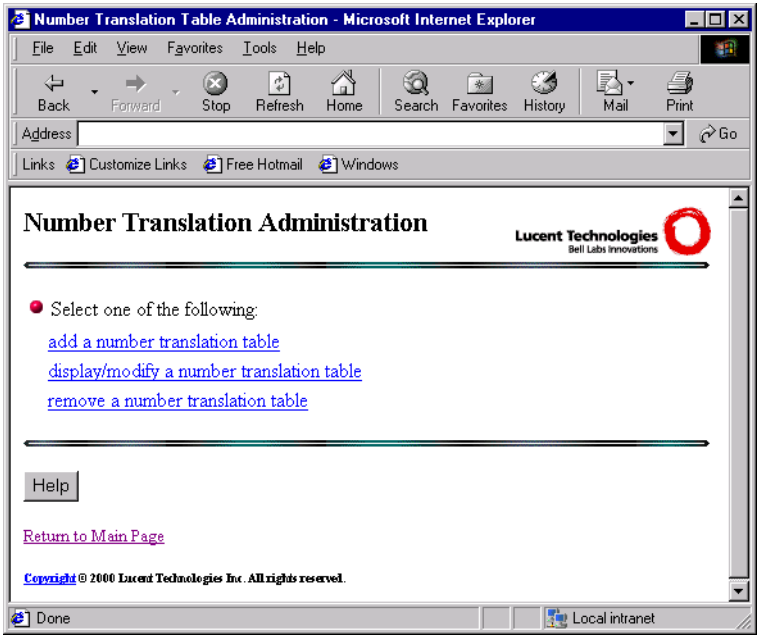
- creating translation tables
- adding/deleting/modifying number translations
- linking translation tables, as either ingress or egress translation tables, to Gateways
- unlinking translation tables from Gateways
- linking translation tables, as ingress translation tables, for terminal calling
- unlinking translation tables from Gateways
- deleting translation tables

Note: The ingress translated number is the one placed in the called party number field of the call record, and it is also the one used to route the call.

Number Translation Administration page

In the Administration section of the Access Manager main screen, click `number translations`. The Number Translations Administration page, as illustrated in Figure 8-1, appears. This page contains hyperlinks to pages which allow number translation tables to be added, displayed, modified, and removed.

Figure 8-1. Number Translations Administration page



These areas include:

Option	Description
add a number translation table	Selecting this option opens a page where the MultiVoice administrator may create number translation tables.
display/modify a number translation table	Selecting this option opens a page where the MultiVoice administrator may display and/or modify existing number translation tables stored on the MultiVoice Access Manager.
remove a number translation table	Selecting this option opens a page where the MultiVoice administrator may select and remove one or more existing number translation table from the database.

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

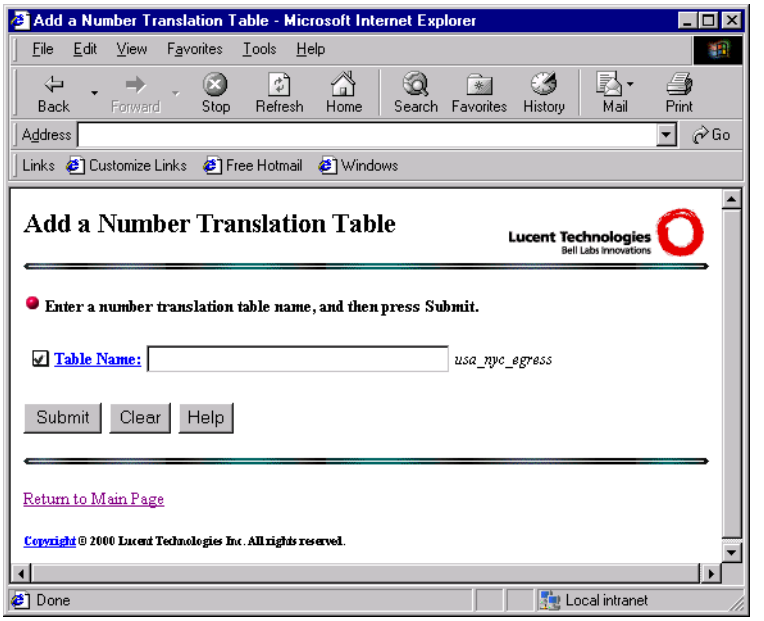
Access Manager screens display sample entry data to the right of each text field. A check box to the left of any field name indicates that you must enter a value for the field before you click the Submit button.

Adding Number Translation Tables

The Add a Number Translation Table page, illustrated in Figure 8-2, is used to add new ingress (inbound) and egress (outbound) translation tables to the Access Manager's translation table database. This is accomplished by entering a table name in the Table Name field.

Table names should be unique, and indicate whether that table contains inbound or outbound translation information (i.e., *max111_outbound*). To save the new Table Name, click the Submit button.

Figure 8-2. Add a Number Translation Table page



To create a number translation table, enter the following value on this page:

Parameter	Description
Table Name	This is the identifier used for a number translation table. Translation table names should be unique, and indicate whether that table contains inbound or outbound translation information (i.e., max111_outbound).

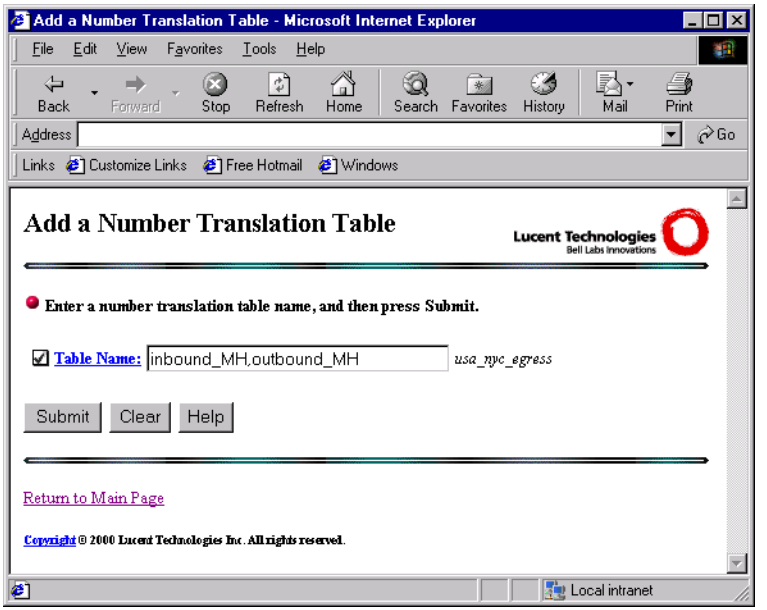
Click the Submit button to save the new table name.

Adding multiple number translation tables

Multiple Number Translation tables may be added in one operation by entering the Table Name of the Number Translation tables you wish to add, separating each with a comma, and clicking the Submit button.

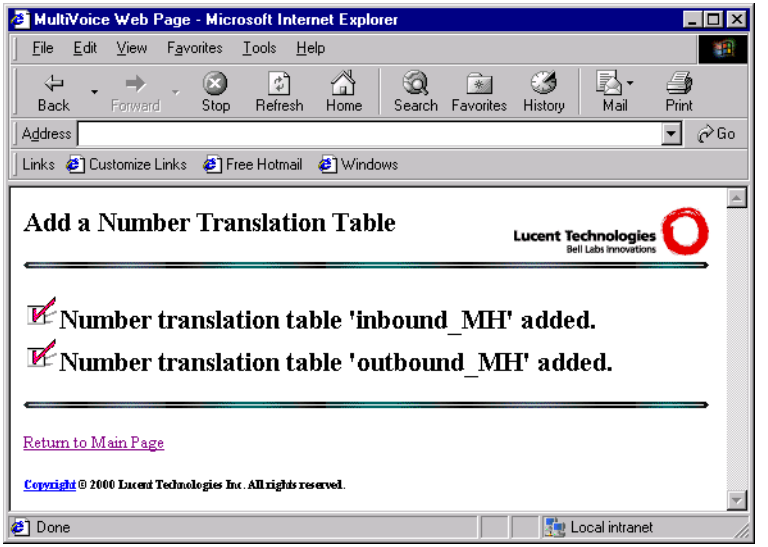
Figure 8-3 shows two Number Translation tables (inbound_MH and outbound_MH) in the Table Name field to be added to the Number Translation Tables database.

Figure 8-3. Adding multiple Number Translation tables



After the Number Translation tables are added to the Number Translation tables database, a confirmation message displays, as shown in Figure 8-4.

Figure 8-4. Successful addition of Number Translation tables



Understanding number translation databases

For number translations to work, each Access Manager must have a defined set of translation tables, containing sets of translation rules. This information is stored in the number translation table list and in the ingress and egress translation tables.

Number translation table list

The number translation table list (nxtl.txt) database, located in the `mvam/db` directory, contains a list of all the number translation tables currently available for the Access Manager to use when performing call routing.

The entries in this file include the following:

Parameter	Description
Table Name	This is the identifier used for a number translation table. Translation table names should be unique, and indicate whether that table contains inbound or outbound translation information (i.e., *max111_outbound*).

Number translation tables

Each number translation table is kept in its own file in the db/nxts' subdirectory. File names should be unique, and indicate whether that table contains inbound or outbound translation information (i.e., *max111_outbound*).

Translation table parameters

Each translation table, which is created through the Web-based administration interface, includes the following information:

Parameter	Description
Number Translation Table Name	This is the identifier used for a number translation table.
Number Translation Search String[a]	This is the prefix or dial string which the Access Manager uses to search the translation rules in a number translation table. • For inbound translation tables, the Search String is used to identify numbers which must be translated to the canonical form of the dialed telephone number, which is used for routing calls to the appropriate connecting Gateway or routing Gatekeeper. • For outbound translation tables, the Search String is used to identify telephone numbers which must be converted to localized dial strings before a Gateway can connect the call.

Parameter	Description
Number Translation Replace String[a]	This is the prefix or dial string which the Access Manager substitutes for the Number Translation Search String before connecting the telephone call. • For inbound translation tables, the Replacement String is used to translate dialed numbers to their canonical form before the call is routed to the appropriate connecting Gateway or routing Gatekeeper. • For outbound translation tables, the Replacement String is used to convert the canonical form of the dialed telephone number to the localized dial string, which is used by the Gateway to actually connect the call.

a. Translation rules such as “something to nothing” and “nothing to something” are allowed. “nothing to nothing” is not allowed.

Translation rules

Each number translation table contains a set of entries, translation rules, which are applied to dial strings received by the Gateway. Each rule specifies how dial strings should be revised by Access Manager, before sending them to the destination Gateway.

Translation rules operate on digits from left to right in the dialed number string. The Access Manager checks for matches of the left-most digits in the dialed number string against rule entries in the appropriate number translation table.

Displaying and modifying a Number Translation Table

The display/modify a number translation table option is used to:

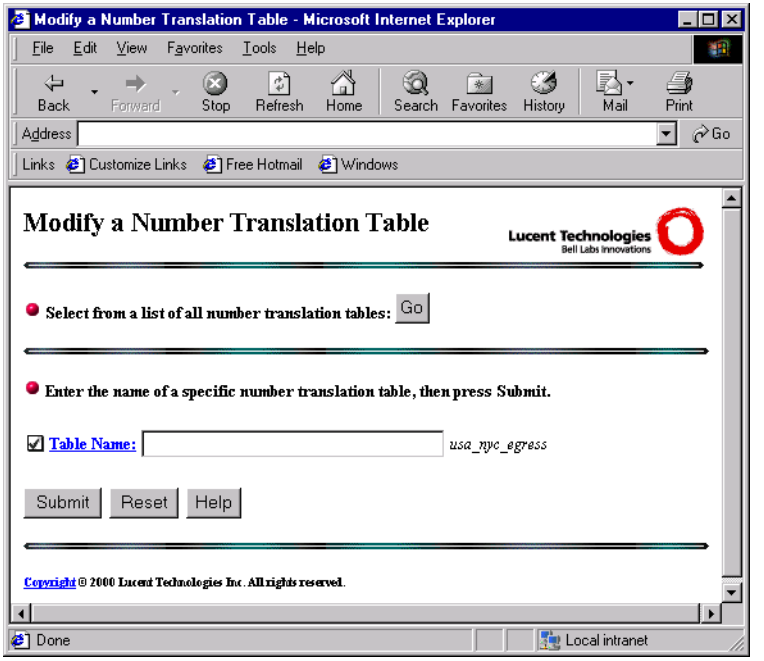
- Select a number translation table from the Access Manager number translation table database,

- Create rules for number translations for the selected table.

The Modify a Number Translation Table page, illustrated in Figure 8-5, is used to select an existing number translation table which is stored on the Access Manager. Selection may be done by either:

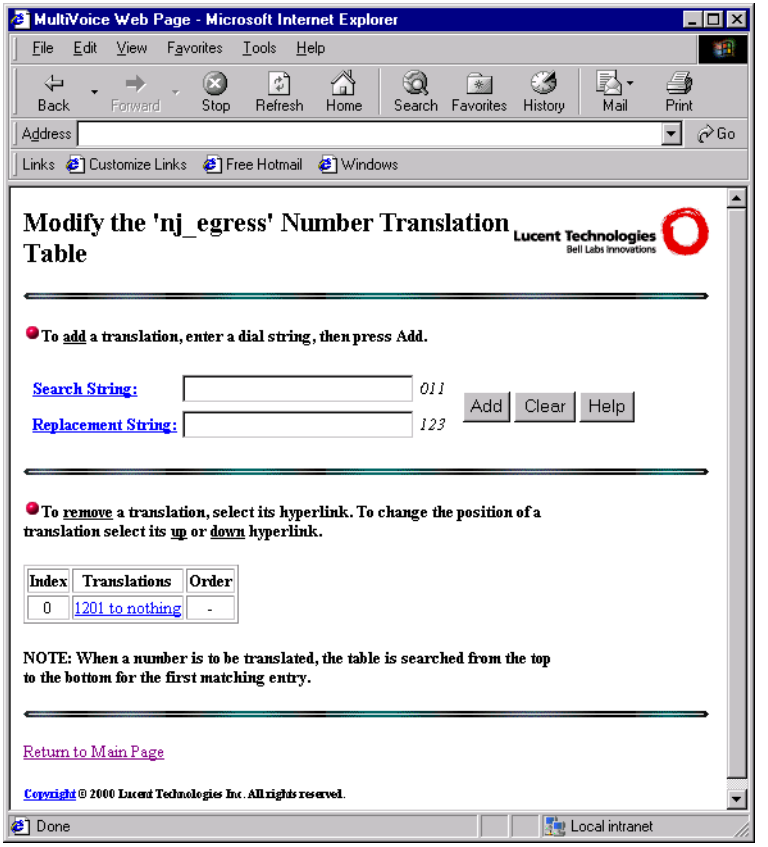
- Clicking the Go button to display a list of all number translation tables; then clicking one of the table name hyperlinks to retrieve that table.
- Entering a table name in the Table Name edit field; then click the Submit button.

Figure 8-5. Modify a Number Translation Table selection screen



Once the table is selected, the Access Manager will redraw the Modify a Number Translation page, as illustrated in Figure 8-6, displaying the table name and any rules already defined for that table.

Figure 8-6. Modify the Number Translation Table screen



To add a new translation rule, enter the following values on this page:

Parameter	Description
Search String	This is the prefix or dial string which the Access Manager uses to search the translation rules in a number translation table.

Parameter	Description
Replacement String	This is the prefix or dial string which the Access Manager substitutes for the Search String before connecting the telephone call.

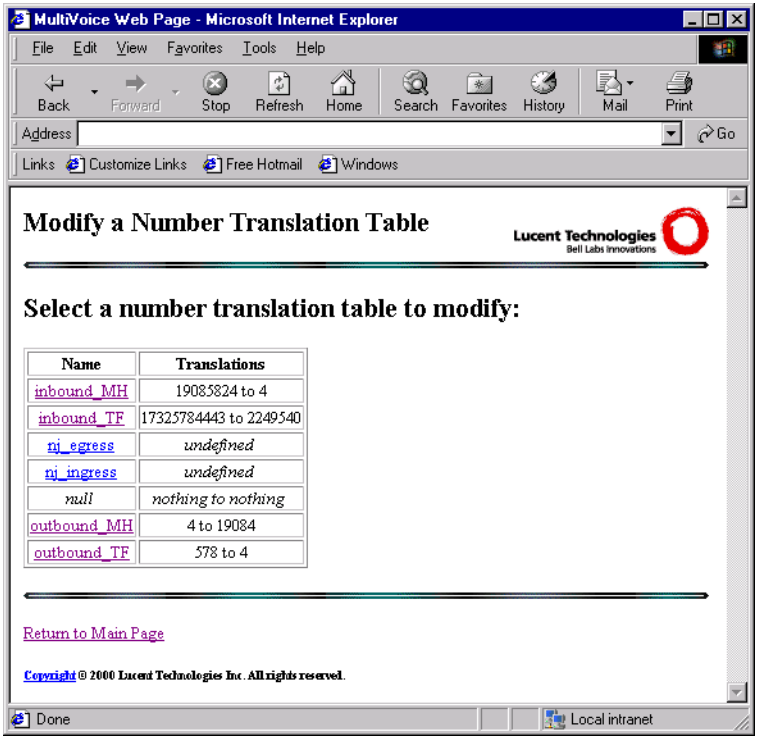
Once values have been entered for both fields, click the Submit button to save this rule.

Selecting from a list of all translation tables

To select a number translation table from a list of all current tables:

1 From the Display/Modify a number translation table page, click the Go button. A list of all current number translation tables appears, as illustrated in Figure 8-7:

Figure 8-7. Select a number translation table to modify page



2 Click the Name hyperlink for a displayed translation table. (For a longer list, the screen has a scroll bar at its right edge.)

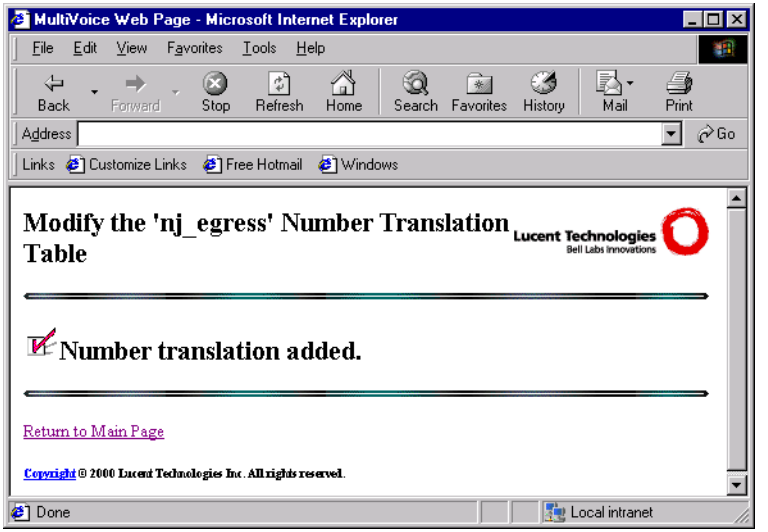
The Access Manager displays the selected translation table on the Modify a Number Translation Table page, as illustrated in Figure 8-6.

3 Modify any field by typing in the new information.

4 To save the settings, click the Submit button.

The Access Manager displays a confirmation message, as illustrated by Figure 8-8. The changes appear next to the Name hyperlink of the modified Gatekeeper.

Figure 8-8. Modify the Number Translation Table confirmation page



Removing translation rules

If you wish to remove an existing translation rule:

1 Open the Modify Number Translation Table page, as illustrated by Figure 8-6.

2 Click the rule you wish to remove in the Translations column.

Note: You are NOT prompted to confirm the removal of the rule selected.

The Access Manager will confirm the removal of the translation rule. When the Modify Number Translation Table page is reloaded, the revised rule table is displayed.

Re-ordering translation rules

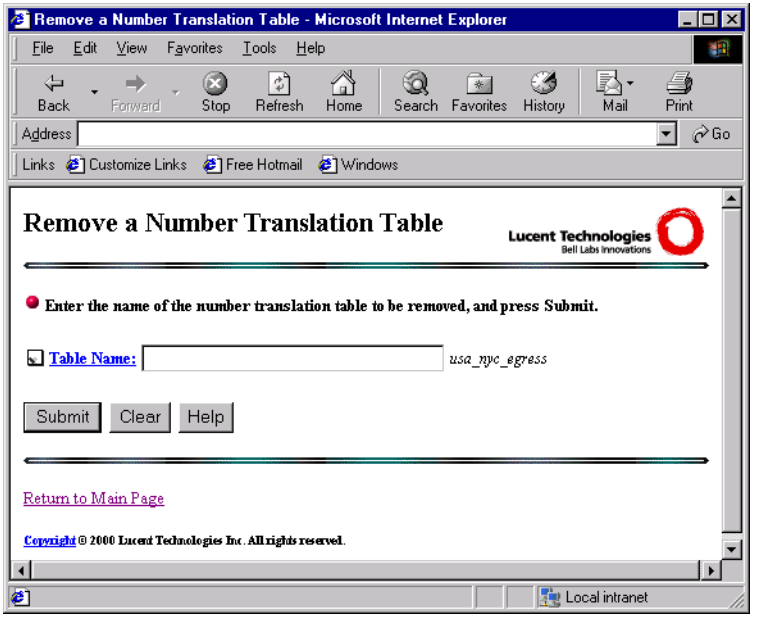
To change the order of the translation rules, select its Order hyperlink, moving the rule up or down in the search order.

Remove a Number Translation Table

Note: Before removing a Number Translation Table, determine if it is an actively used Number Translation table.

The Remove a Number Translation Table page, as illustrated in Figure 8-9, deletes one or more translation tables from the Access Manager's translation table database. This is accomplished by entering Number Translation Table Name(s) in the edit field, then clicking the Submit button.

Figure 8-9. Remove a Number Translation Table



Note: You may remove a Number Translation table even after it has been assigned to a Gateway as an ingress or egress translation table, or as the Terminal ingress translation table.

Removing an active Number Translation table

If the Number Translation table you wish to remove, is actively in use:

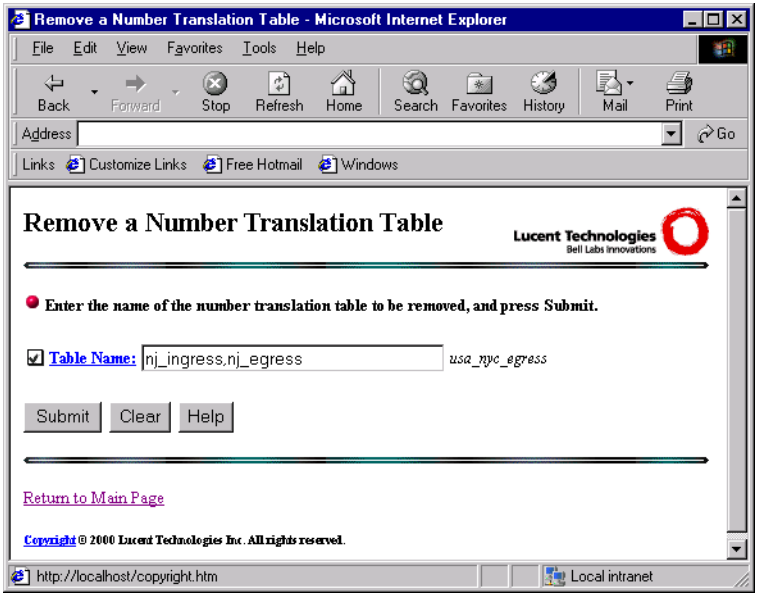
1. Define a Number Translation table to replace the Number Translation table you wish to remove.
2. Administer the Gateway that is using the Number Translation table you wish to remove, with the newly defined Number Translation table.
3. When the Number Translation table you wish to remove is no longer actively in use, follow the instructions to Remove a Number Translation table.

Removing multiple number translation tables

The Remove a Number Translation page allows you to remove Number Translation Tables from the Access Manager's Number Translation Table database. Multiple Number Translation tables may be removed in one operation by entering the Table Name of the Number Translation tables you wish to remove, separating each with a comma, and clicking the Submit button.

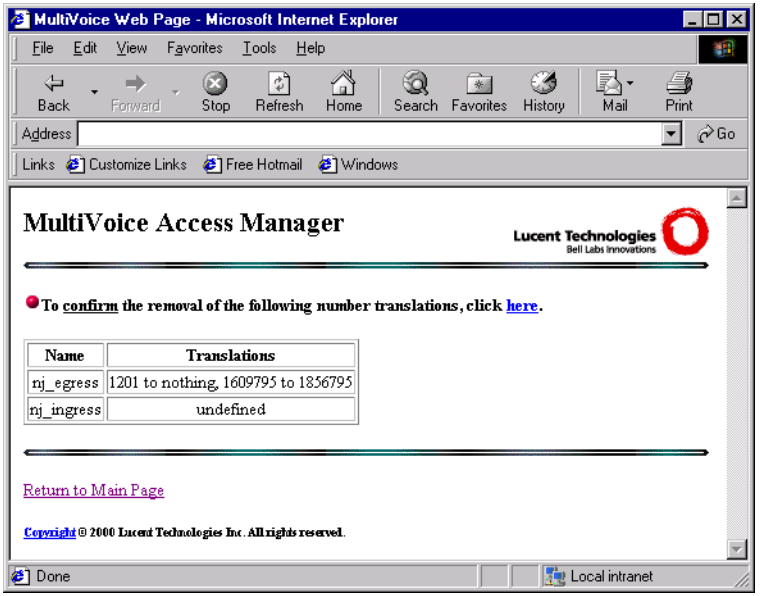
Figure 8-10 shows two Number Translation tables (nj_ingress and nj_egress) in the Table Name field to be removed from the Number Translation tables database.

Figure 8-10. Removing multiple Number Translation tables



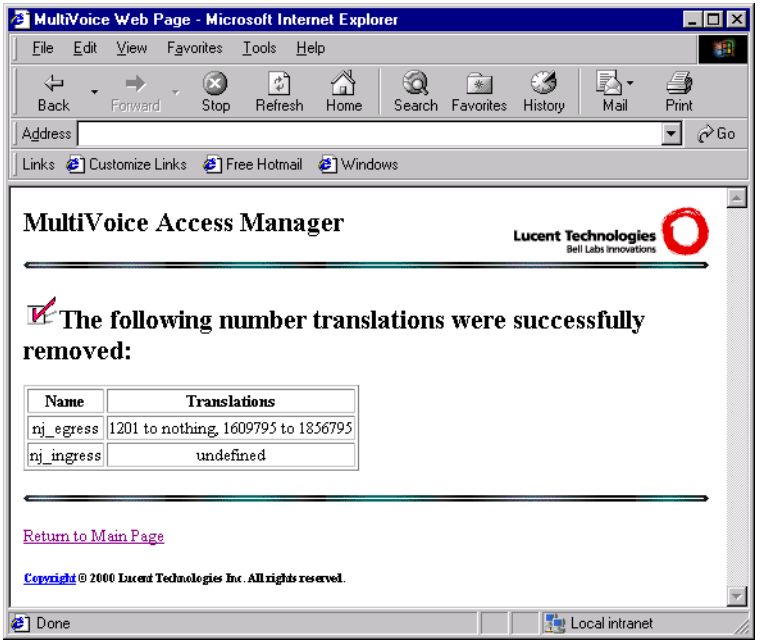
You are required to verify the removal of the Number Translation tables entered in the Table Name field by responding to a removal verification message as shown in Figure 8-11. To remove all of the Number Translation tables listed, click “here”. If you choose to cancel your removal request or to make any changes to the list of Number Translation tables to be removed, you must click your browser’s Back button.

Figure 8-11. Verify removal of Number Translation tables



After each Table Name is validated and its record is removed from the Number Translation tables database, a confirmation message displays, as shown in Figure 8-12.

Figure 8-12. Successful removal of Number Translation tables

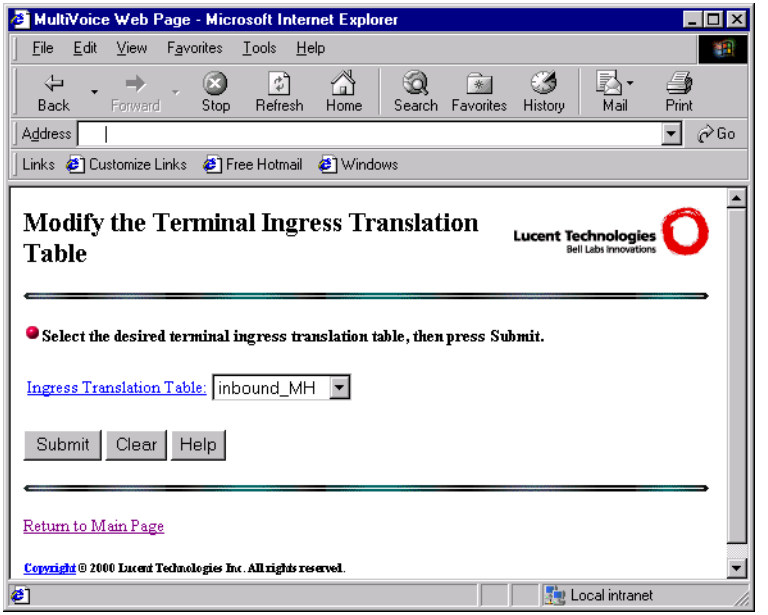


Using number translations with terminals

The Modify the Terminal Ingress Translation Table page, as illustrated in Figure 8-13, assigns a number translation table for processing calls received from H.323 compliant terminals. Calls dialed from registered PC terminals will use this table to perform inbound number translation.

This page is accessed by clicking the `terminals` hyperlink on the MultiVoice Access Manager administration menu.

Figure 8-13. Modify the Terminal Ingress Translation Table page



To modify the ingress table assignments, enter the following values on this page:

Parameter	Description
Ingress Translation Table	This identifies the number translation table the Access Manager will use for routing inbound calls received from a H.323-compliant terminal. This pull-down list contains a list of all the number translation tables. This table contains the translation rules MVAM will apply to dialed telephone numbers, to generate the canonical form of the destination telephone number; which is used for Gateway or Gatekeeper routing.

Click the Submit button to save changes to this page.

Configuring MultiVoice Users

9

Adding user records 9-3

Displaying and modifying user information. 9-6

Removing user records 9-11

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.

It provides options for:

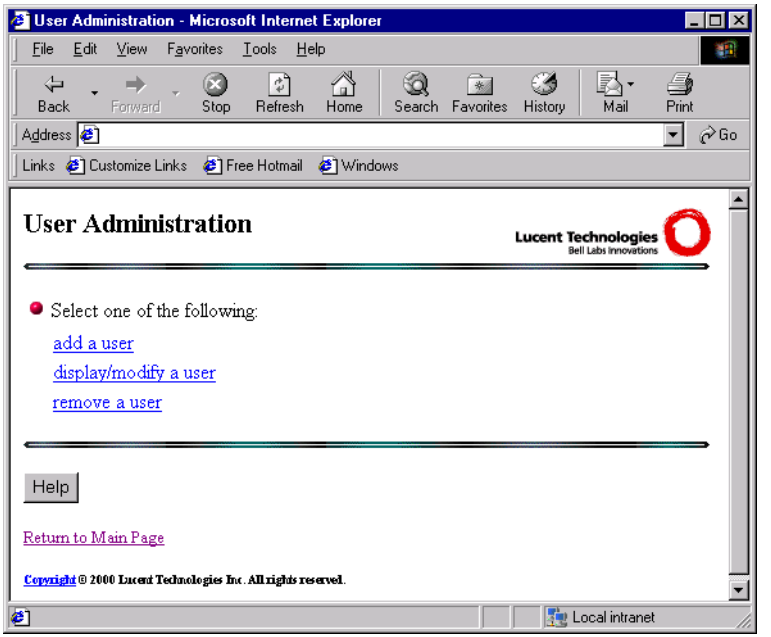
- Adding user records
- Displaying and modifying user information
- Removing user records

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

Note: (For Windows NT servers only.) If you 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.

From the Access Manager main screen, select the hyperlink `users` to display the User Administration page, as illustrated in Figure 9-1:

Figure 9-1. User Administration page



From this page, you may perform the following user administration tasks:

Option	Description
add a user	This option is used to add a new user to the Access Manager's user database.
display/modify a user	This option is used to display and modify user information retrieved from the user database.
remove a user	This option is used to remove an existing user record from the user database.

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

Access Manager screens display 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.

Adding user records

To add a user to the MultiVoice network, click `add a user` on the User Administration screen. The Add a User page, as illustrated in Figure 9-2, appears:

Figure 9-2. Add a User page



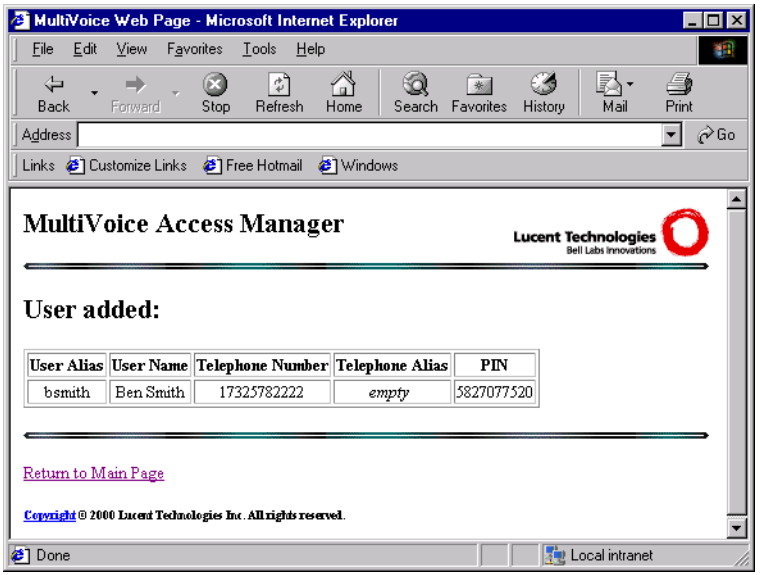
To create a new user record, enter the following information on this page:

Parameter	Description
User Alias	This is an alpha-numeric string which uniquely identifies a user. When the ANI Required check box is selected on the Security Options page, the Calling Line ID (CLID) of a user's telephone number is collected and compared to the value of the User Alias to authenticate the caller.

Once you have entered this information, click the Submit button to save the user record.

If the new user is created successfully, a confirmation message containing the user record information, including the PIN generated by the Access Manager displays, as illustrated by Figure 9-3.

Figure 9-3. User Add confirmation page



Understanding the user database records

This page, and all the pages for user administration, manipulate the data fields which make up the user database record. This includes values for the following fields:

Parameter	Description
User Alias	This is an alpha-numeric string which uniquely identifies a user. When the ANI Required check box is selected on the Security Options page or a matching ADMA rule is defined with ANI Authentication enabled, the Calling Line ID (CLID) of a user's telephone number is collected and compared to the value of the User Alias to authenticate the caller. 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.
User Name	This is an alpha-numeric string which is the full name of a user. It is not necessarily unique.
Telephone Number	This is the telephone number of a user. If the user is to be contacted using his corresponding Telephone Alias, the telephone number must be complete.
Telephone Alias	This is a unique numeric dial string which can be used to address an administered user with the MultiVoice Access Manager's Alias Dialing feature. **Note:** Alias dialing is not supported in a MultiVoice network.
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 admits calls, it does not check for user PIN numbers, even if they have been assigned PIN numbers.

For complete information about each field, see the MVAM on-line help.



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 page. This will render the compromised information obsolete.

Displaying and modifying user information

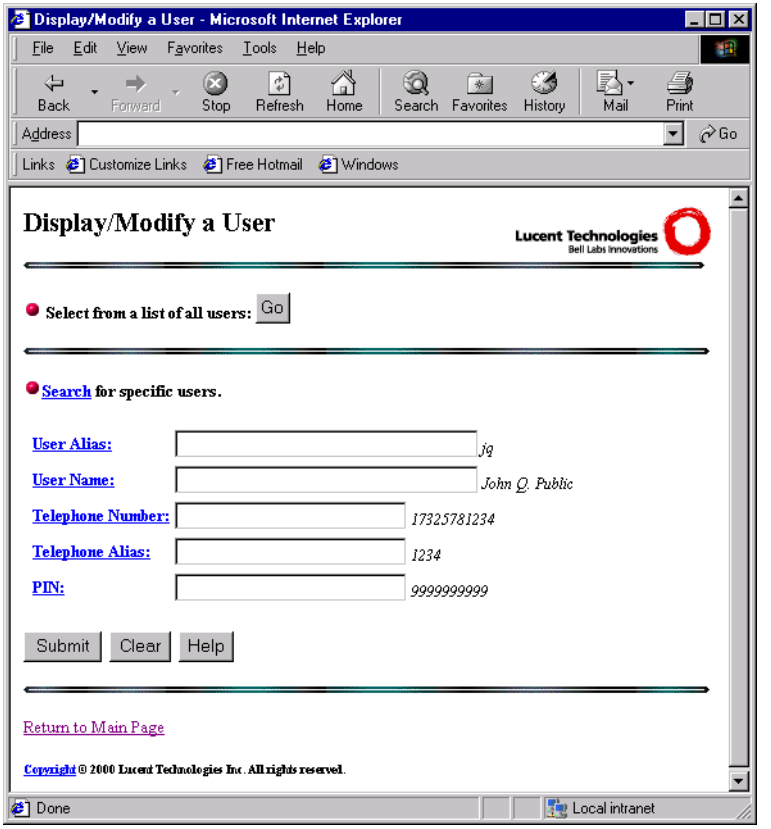
To update a user's database record, click the `display/modify a user` hyperlink on the User Administration page. This option is used to:

- Select and display specific MultiVoice user information from the user database,
- Modify the information displayed in that database record.

Upon selection of this option, the Display/Modify a User page, illustrated in Figure 9-4, appears. This page is used to select a MultiVoice user. Selection may be done by:

- Clicking the Go button to display a list of all MultiVoice user records; then clicking a hyperlink to open a specific user record.
- Entering a wildcard entry for User Alias, or some combination of user information on this screen; then clicking the Submit button to:
  - Retrieve all matching user records,
  - Then clicking a hyperlink to open a specific user record.
- Entering a specific User Alias

Figure 9-4. Display/Modify a User page

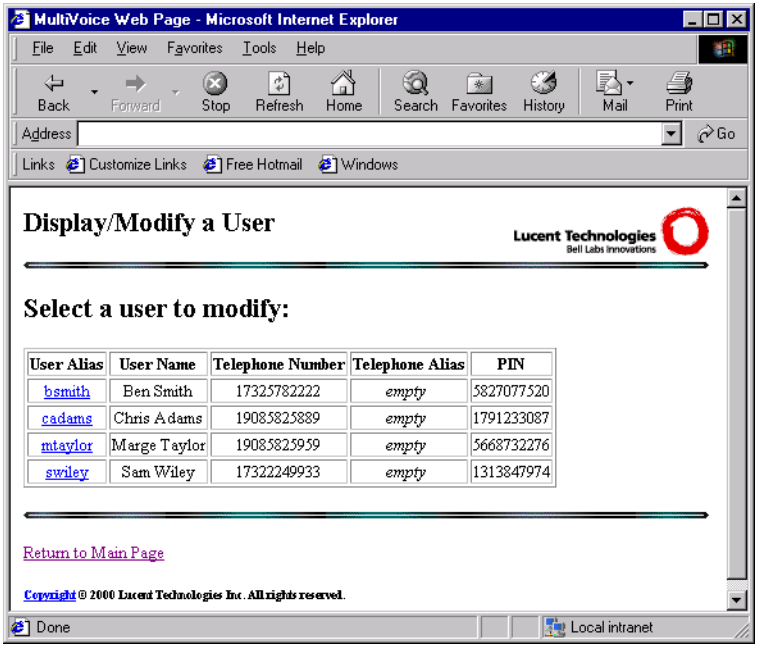


Selecting from a list of all users

To select a user record from a list of all MultiVoice users:

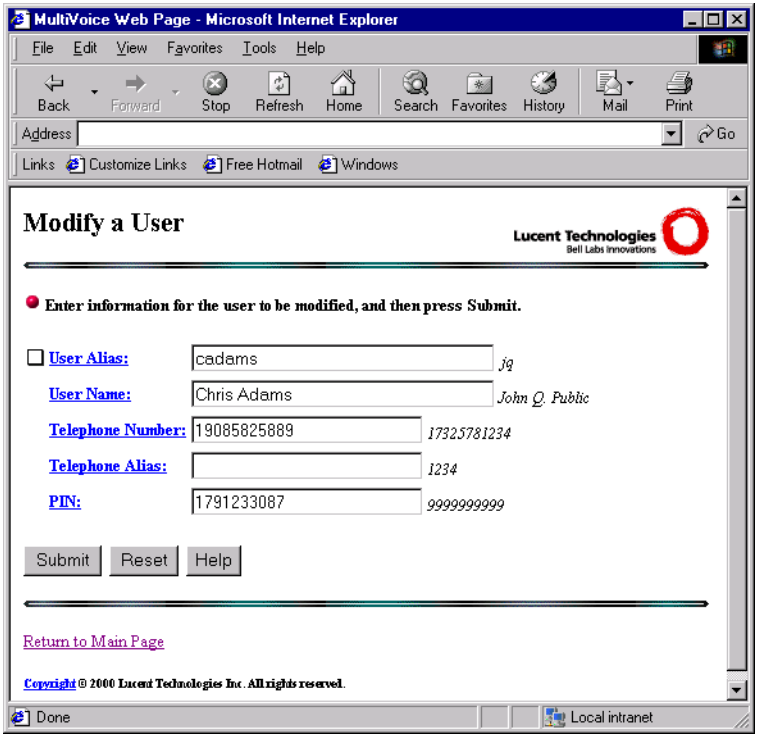
1 From the Display/Modify a User page, click the Go button. The Select a user to modify page appears, displaying a list of all user records, as illustrated in Figure 9-5:

Figure 9-5. Select a user to modify page



2 Click the hyperlink for the User Alias associated with the record you wish to modify. The Modify a User page appears, as illustrated by Figure 9-6:

Figure 9-6. Modify a User page

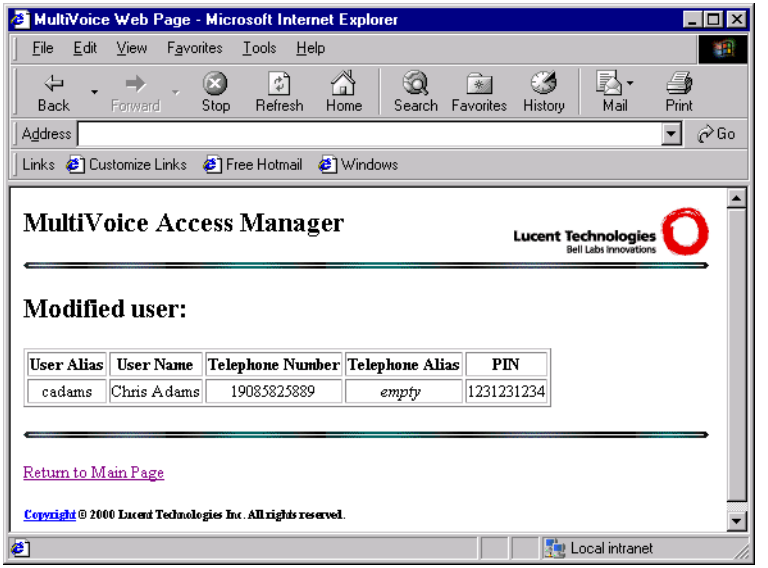


Modify any of the fields by typing in new information.

3 Click the Submit button to save your changes.

The Access Manager confirms the saved changes by displaying the Modified User information page, as illustrated by Figure 9-7:

Figure 9-7. Modified User page



Selecting a user using wildcard searches

The wildcard character “%” is supported in all fields of the Gateway, Gatekeeper, Terminal, ADMA, and User search forms. For example, entering “d%” in the User Alias field on a search form will cause all Users whose User Alias begins with “d” to be displayed.

The wildcard character may appear at either the beginning or the end of an entry. Once all your search criteria is entered on the screen, press Submit to display any matches for your search criteria.

Modifying user PINs

A PIN is automatically generated by the MultiVoice Access Manager whenever a new user is added to the User Database. Once created, a PIN can be modified through the Modify a User screen. The following constraints apply when modifying user PINs:

- A PIN may only contain digits.
- The PIN length cannot be greater than 24 digits.
- The PIN must be unique, relative to all users in the database.

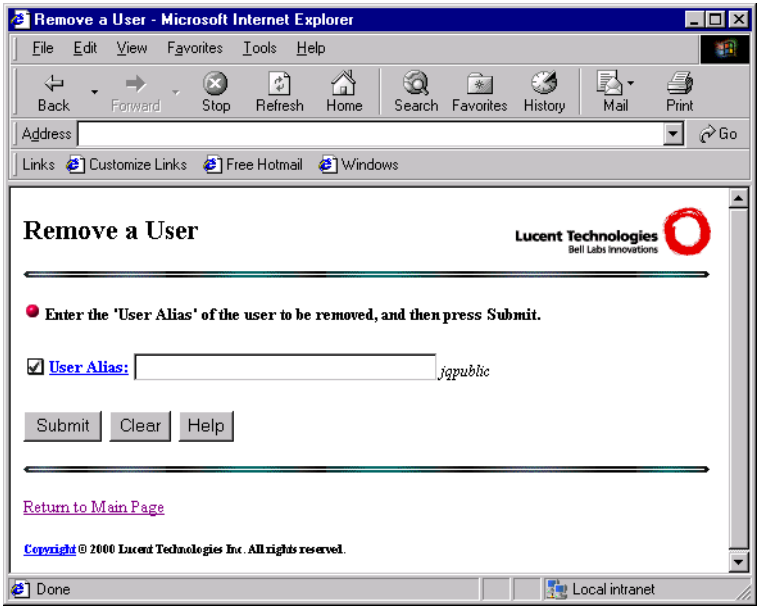
To modify a user PIN, highlight the entry in the `PIN` edit field. Type in the new PIN for this user, then click the Submit button.

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

Removing user records

To remove one or more Users from the MultiVoice Access Manager, click the Remove a User link on the User Administration screen. The Remove a User page, as illustrated in Figure 9-8, appears:

Figure 9-8. Remove a User page



To remove a User record, enter the following information on this page:

Parameter	Description
User Alias	This is an alpha-numeric string which uniquely identifies a user.

Once you have entered this information, click the Submit button to save your changes.

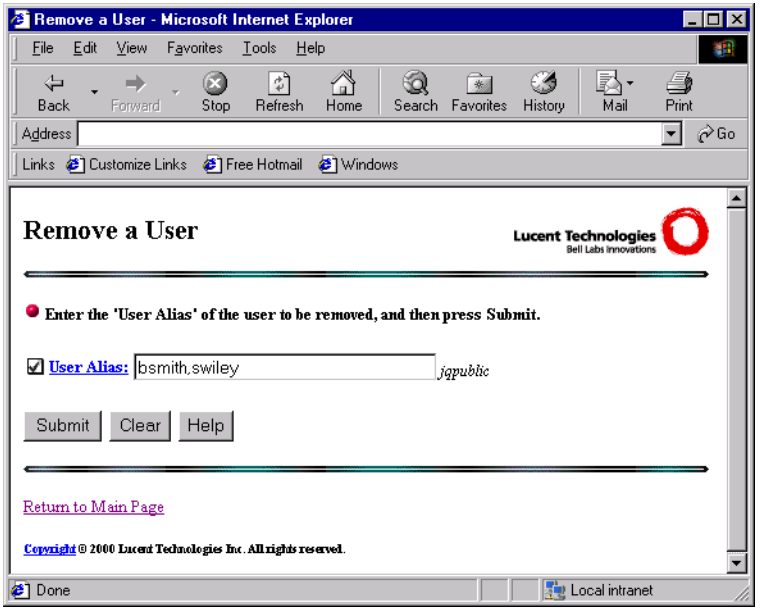
Removing multiple users

The Remove a User page allows you to remove multiple users in one operation by entering the User Alias of the Users you wish to remove, separating each with a comma, and clicking the Submit button.

Note: A comma is the only delimiter. Entering a comma and a space will return an error message.

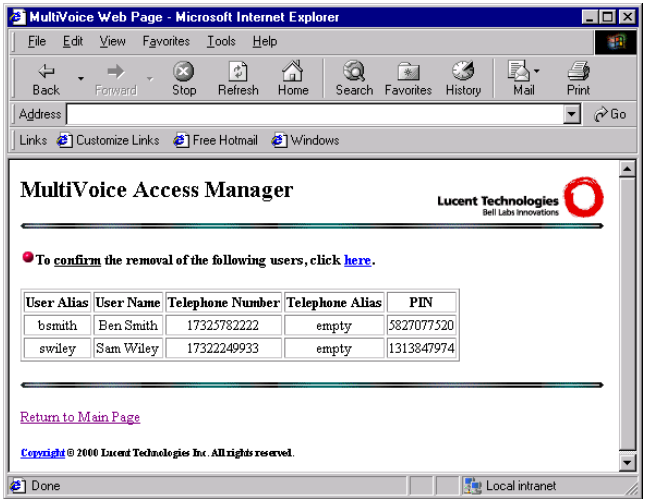
Figure 9-10 shows two users (bsmith and swiley) to be removed from the User database.

Figure 9-9. Removing multiple users



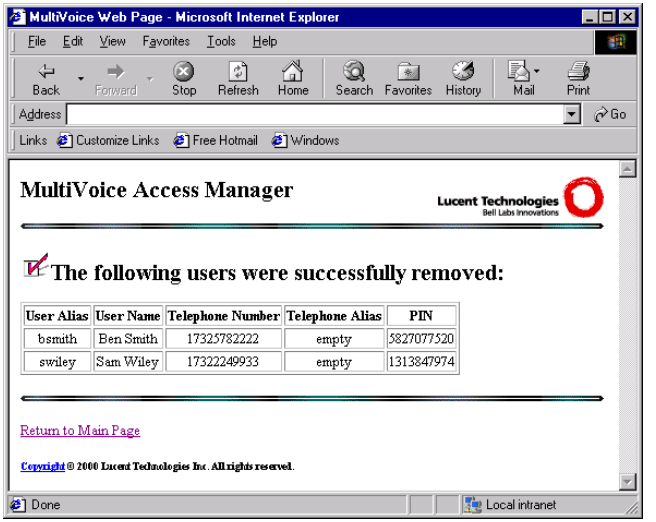
You are required to confirm the removal of the Users entered in the User Alias field by responding to the message shown in Figure 9-10. To remove all of the Users listed, click “here”. If you choose to cancel your removal request or to make any changes to the list of Users to be removed, you must click your browser’s Back button.

Figure 9-10. Verify removal of users



After each User Alias is validated and its user record is removed from the user database, a confirmation message displays, as shown in Figure 9-11.

Figure 9-11. Successful removal of users



MultiVoice Administration

10

Setting Gateway-to-Gatekeeper registration policy 10-1
Retrieving MultiVoice statuses. 10-3
Active call status. 10-7
Testing call routes. 10-9
Viewing log files. 10-14
Displaying MVAM version 10-25
License Administration 10-26

Setting Gateway-to-Gatekeeper registration policy

In order to process calls, the Gateways and Gatekeepers in a MultiVoice network must:

- know that the other exists, and how to locate them
- successfully register Gateway-to-Gatekeeper

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

Identifying Gateways and Gatekeepers

To establish communications between an Access Manager and MultiVoice Gateway:

- Enter the IP address of the system running MVAM for:
  - Ethernet > Mod Config > VOIP Options >GK IP Adrs on the MAX 1800, 2000 or 6000
  - VOIP { 0 0 } > gatekeeper-ip on the MAX TNT
- Use the gateways > add a gateway hyperlink of the Access Manager's Web-based interface to add the MultiVoice Gateway to the Gateway database. The Gateway Name should be the same as the value of:
  - System > Sys Config > Name on the MAX 1800, 2000, or 6000
  - sys > name on the MAX TNT

  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 4-4.

If this MultiVoice network uses secondary Gatekeepers, set the following to the IP address of the Access Manager system, which will take over registration/call routing if the primary Gatekeeper is unavailable.

- Ethernet > Mod Config > VOIP Options > 2ndGK IP parameter on the MAX 1800, 2000, or 6000
- VOIP {0 0} > gatekeeper-ip-sec on the MAX TNT

Setting Gateway-to-Gatekeeper registration policy

To enable a MultiVoice Gateway to register with a MultiVoice Access Manager, you must assign complimentary values to the registration parameters on both platforms. Registration options are located under:

- Ethernet > Mod Config > VOIP Options for MAX 1800/2000/6000 Gateways
- VOIP { 0 0 } profile for MAX TNT Gateways
- Options > Registration Options hyperlink of the Access Manager's Web-based interface

Complimentary values must be assigned as the respective MultiVoice platforms as follows:

Platform	Parameter	Default Value
MAX 1800/2000/6000	Keepalive Timer	120 (seconds)
MAX TNT	gatekeeper-keepalive	
MultiVoice Access Manager	Gateway Registration Period	

After the appropriate values are set on both the Gatekeeper and Gateway, restart the MultiVoice Gateway, it should automatically register with the Access Manager. See “Starting MVAM” on page 2-25.

Managing registration grace periods

The Access Manager allows for a grace period between registrations, in addition to the Gateway Registration Period, for Gateway keep-alive registrations. This grace period reduces the likelihood a Gateway will become unregistered due to:

- differences between system clocks on Gateways and Gatekeepers
- delays caused by network attenuation, (i.e., distances and transmission speeds)
- delays caused by the volume of network traffic.

During this interval, set using the Options > Registration Options > Registration Period Margin parameter, Gateways will continuously make registration attempts until they either register with the Gatekeeper or exhaust all attempts. Gateway parameters which control re-registration activity should be adjusted to optimize keep-alive registration.

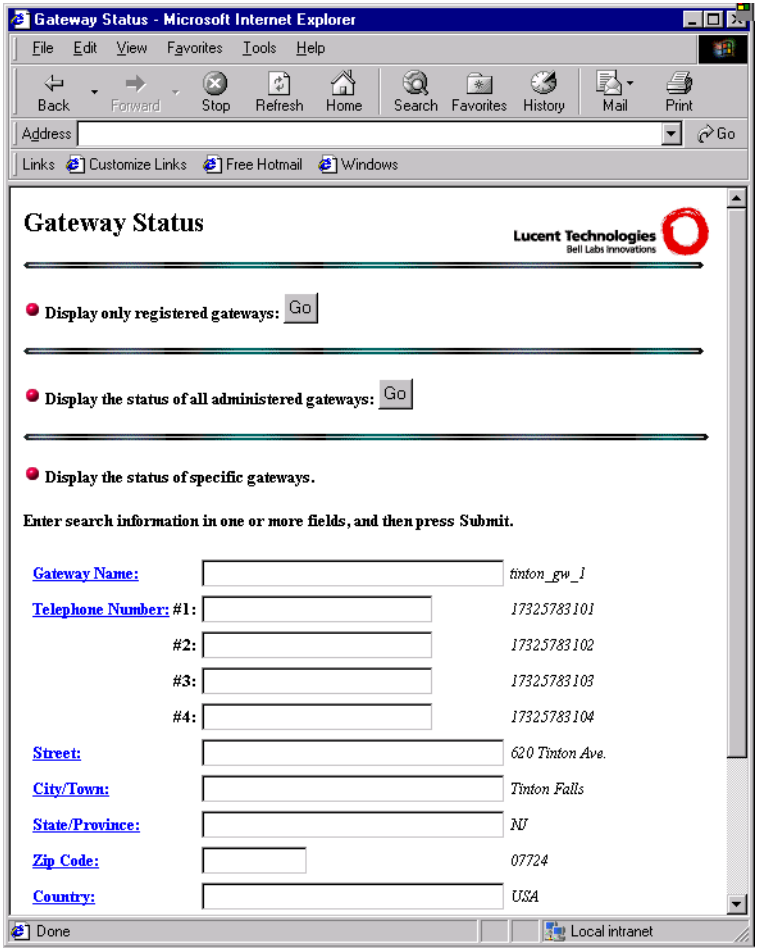
Retrieving MultiVoice statuses

The Access Manager can report the statuses for Gateways, terminals, and active calls.

Gateway Status

To display the status of any or all MultiVoice Gateways, use the `Status: Gateways` hyperlink on the MVAM main menu. The Gateway Status selection page, as illustrated in Figure 10-1, appears.

Figure 10-1. Gateway Status selection page

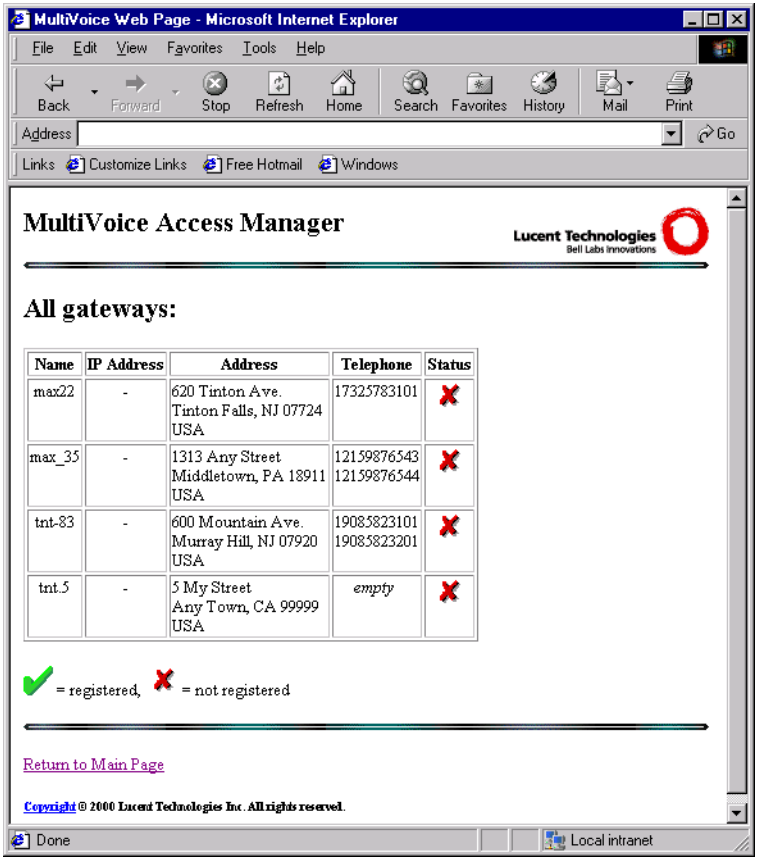


From the Gateway Status screen, you may:

- Click the Go button to display the status of all registered Gateways.
- Click the Go button to display the status of all administered Gateways regardless of registration status.
- Enter a Gateway Name, then click the Submit button to get the status of a specific Gateway.
- Enter information in any field, then click the Submit button to retrieve the statuses for all Gateways matching your criteria.

Clicking the Go button for `Display the status of all administered gateways` displays a status report as illustrated by Figure 10-2.

Figure 10-2. All gateways status report



The Status column identifies each MultiVoice Gateway as either registered, identified by a green check mark, or not registered, identified by a red X.

Wildcard searches

The wildcard character, %, is supported in all fields in this form. For example, entering d% in the Gateway Name field will cause all gateways whose name begins with “d” to be displayed when you submit this form. The wildcard character may appear at either the beginning or the end of an entry.

Terminal status

The Terminal Status display shows a record for each registered H.323 terminal (PC). Terminals register with the Access Manager as controlled by the PC client software running on the terminal.

Each record contains a name, IP address, location address (if defined) and telephone number (E.164 address) associated with the registered terminal. For example:

Name	IP address	Address	Telephone
?	198.65.23.6	empty	17325551212
nm	201.135.65.9	Tinton Falls, NJ	17325550000

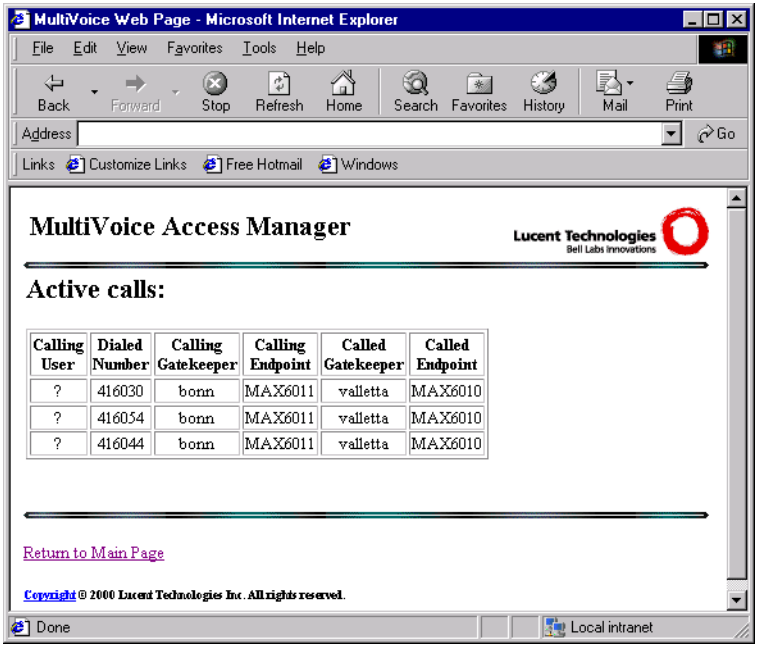
where:

Parameter	Description
Name	This is the network name or terminal id sent by the H.323 Terminal as part of the call request.
IP address	This is the IP address sent by the H.323 Terminal as part of the call request.
Address	This is the street address, City /Town, State/Province, Zip Code, or Country where this terminal is located. The value for this field is *empty* when this information is not included in the terminal database.
Telephone	This is the qualified E.164 address associated with the H.323 Terminal. This is usually sent by the H.323 Terminal as part of the call request.

Active call status

To display a list of active calls, use the `Status: Calls` hyperlink on the MVAM main menu. The Active call log page, as illustrated in Figure 10-3, appears.

Figure 10-3. Active call log



This report displays a record for each active call in progress. Each record contains the origin and destination of the call. This information includes:

Parameter	Description
Calling User	The administered user alias of the called party (or ?). This identifies the calling party by user alias as defined in the User Database of the calling Gatekeeper. A ? is displayed when authorization is not enabled.
Dialed Number	The telephone number of the called party. When number translation is used, this will be the translated dial string. If it is not used, this will be the user entered dial string.

Parameter	Description
Calling Gatekeeper	This is the Gatekeeper Identifier of the Access Manager or Gatekeeper virtual zone which handled the call admission request from the Calling Endpoint (e.g., gkNJ, gkNJ.Eatontown).
Calling Endpoint	This is the Gateway Name of the MultiVoice Gateway, or terminal identifier, where the call request originated (e.g., max183).
Called Gatekeeper	This is the Gatekeeper Identifier of the Access Manager or Gatekeeper virtual zone which completed the call routing to the Called Endpoint (e.g., gkNJ, gkNJ.Eatontown).
Called Endpoint	This is the Gateway Name of the MultiVoice Gateway which connected the call to the dialed telephone number (e.g., max183).

Testing call routes

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 Access Manager Number Translator/Call Router tool.

Translator/router tool

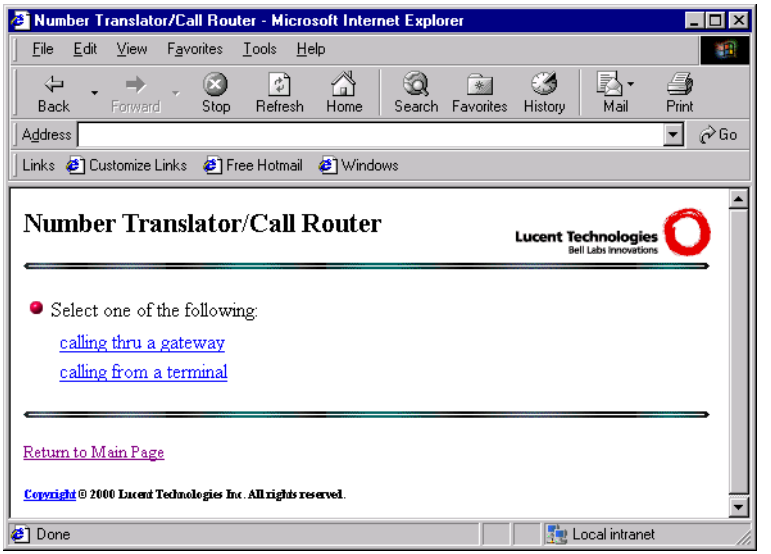
The translator/router tool provides a means for the MultiVoice administrator to test and verify call routes, whether or not number translation is used. With this tool, the MultiVoice administrator can extract and display end-to-end dialing and route information for the telephone number entered on the screen.

Translation information and call routing information is extracted from the databases on the Access Manager, then displayed on the screen as an end-to-end call flow diagram. This includes:

- The entered telephone number, Gateway identification, inbound dial translation, outbound dial translation, destination Gateway, and the dialed number string used to complete the call, for calls initiated through a Gateway.
- The entered telephone number, Gateway identification, inbound dial translation, outbound dial translation and destination Gatekeeper, for calls completed using Multi-zone call routing.
- The entered telephone number, inbound dial translation, outbound dial translation, destination Gateway, and the dialed number string used to complete the call, for calls initiated from a PC terminal.

The translator/router hyperlink opens the Number Translator/Call Router page, as illustrated in Figure 10-4.

Figure 10-4. Number Translator/Call Router page



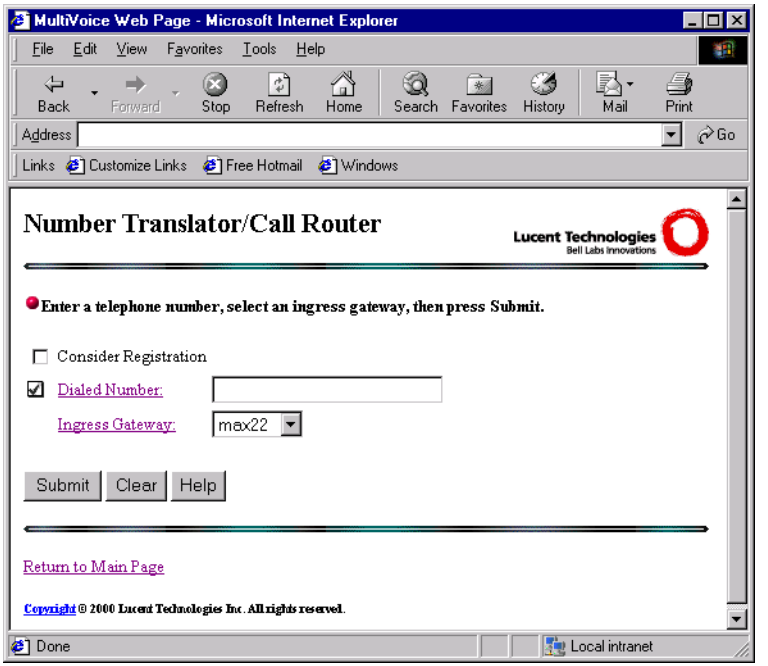
From this page, the MultiVoice administrator may perform route checking for the following:

Option	Description
calling thru a gateway	When tracing a route using this option, you must enter the destination telephone number in the Dialed Number field, and the Gateway where the call originated in the Ingress Gateway field. The results will appear as follows: `43167 --> GW:gw26 --> 43167 --> EP:MAX183 --> 43167` This information includes: • The entered telephone number, • Gateway identification, • inbound dial translation, • destination Gateway, • the dialed number string/outbound dial translation used to complete the call.
calling from a terminal	When tracing a route using this option, you must enter the destination telephone number in the Dialed Number field. The results will appear as follows: `43167 --> 43167 --> GW:MAX183 --> 43167` This information includes: • The entered telephone number, • inbound dial translation, • destination Gateway, • and the dialed number string/outbound dial translation used to complete the call.

Calling thru a Gateway

When this hyperlink is selected, you may test call routing for calls dialed from an ordinary telephone. The Access Manager displays the Number Translator/Call Router page, as illustrated in Figure 10-5.

Figure 10-5. Calling thru a Gateway options



To test call routing, enter or select the following values on this page:

Parameter	Description
Consider Registration	Select this checkbox to consider only registered endpoints as valid to complete a call.

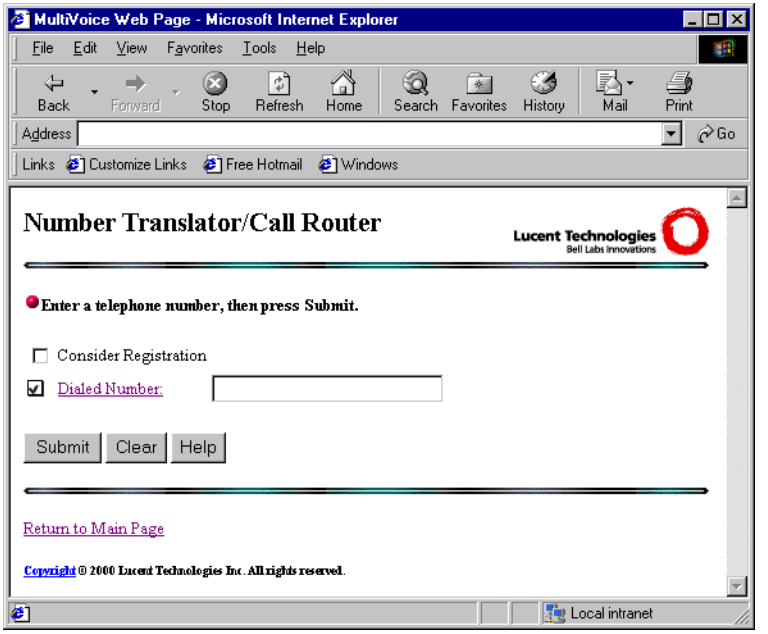
Parameter	Description
Dialed Number	Enter the dialed telephone number. This is the actual dial string entered by the caller and received by the Access Manager.
Ingress Gateway	Enter the Gateway Name of the MultiVoice Gateway where this call originated.

Once this information is entered, click the Submit button to display translation information and call routing information, as extracted from the databases on the Access Manager, as an end-to-end call flow diagram.

Calling from a Terminal

When this hyperlink is selected, you may test call routing for calls dialed from an H.323 compliant terminal attached to the network. The Access Manager displays the Number Translator/Call Router page, as illustrated in Figure 10-6.

Figure 10-6. Calling from a Terminal options



Select the Consider Registration checkbox to consider only registered endpoints as valid to complete a call.

To test call routing, enter the Dialed Number, the actual dial string entered by the caller and received by the Access Manager, then click the Submit button to display translation information and call routing information.

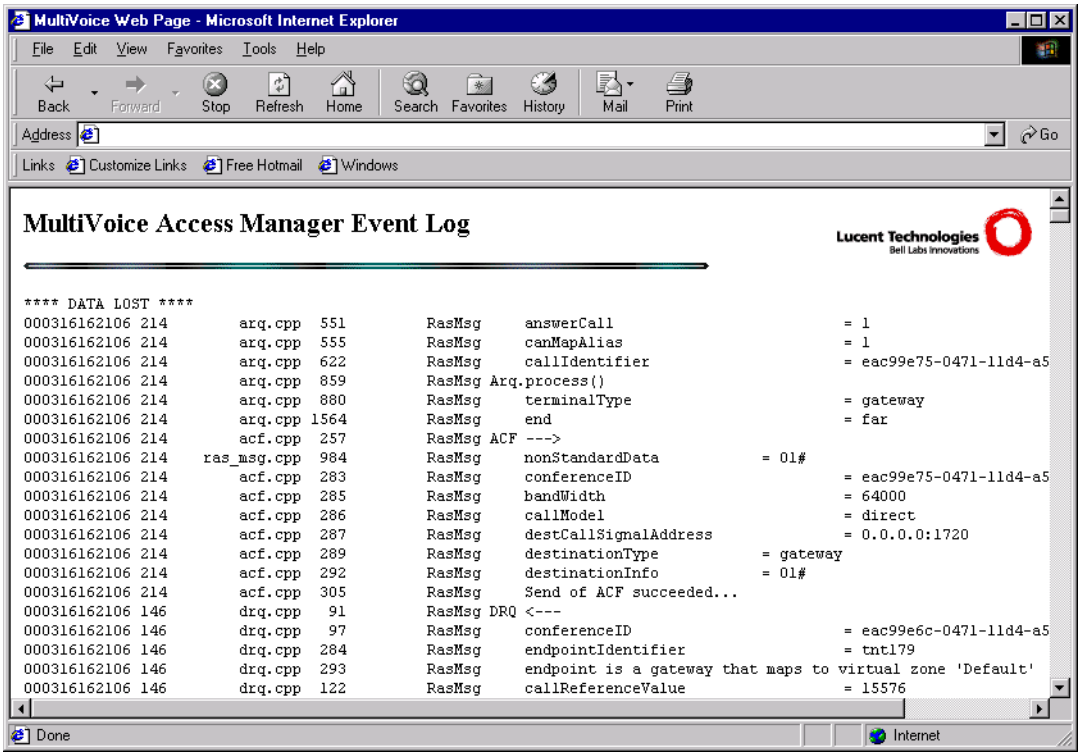
Viewing log files

The Access Manager maintains log files for both calling operations and MVAM events. These log files are viewed by selecting either the `event` or `call` hyperlinks from the MVAM main menu page.

Event log

The Access Manager creates the event log at start up, and writes to the log continuously, until the application is stopped. It records information about Gatekeeper operations, as illustrated in Figure 10-7.

Figure 10-7. MultiVoice Access Manager Event Log



The event log will report on communication between the Gatekeeper and Gateways, communication between peer Gatekeepers, call admission requests, user authentication, and other functions performed by the Access Manager.

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 Solaris or HP-UX 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 extract shows a stop record, a start record, an incomplete reconrd from the file, `02172000.txt`, that was created February 17, 2000:

```
version 1.3.0

start,02/17/2000,11:19:08,eac99d52-ee65-11d3-9fde-00c07b727d
3d,192.168.35.238:mvam238:192.168.35.171:tnt171:gw:0:095:1:1
:2:10,16000,60000:?:?,192.168.35.238:mvam238:192.168.35.171:
tnt171:gw,192.168.35.238:mvam238:192.168.35.172:tnt172:gw,?:
66000:?

stop,02/17/2000,11:19:08,eac99e7f-ee64-11d3-9ee2-00c07b727d3
d,192.168.35.238:mvam238:192.168.35.172:tnt172:gw:1:?:1:1:5:
2,normalDrop,132
```

```
incomplete,02/17/2000,11:21:16,eac99dd9-ee65-11d3-a15e-00c07
b727d3d,192.168.35.238:mvam238:192.168.35.171:tnt171:gw:0:62
5:1:1:26:12,7325781234:41234:dskran,4007:86000:?,normalDrop,
?
```

Start call record format

The start call record is as follows:

Field	Description	Example
start	This field identifies the call record as a start record.	`start`
date	This field contains the date the record was created (mm/dd/yyyy).	`02/17/2000`
time	This field contains the time the record was created (hh:mm:ss).	`11:19:08`
call identifier	This field provides a globally unique call identifier for this call. This is a 32-character hexadecimal string whose content is determined by the endpoint (Gateway or terminal).	`eac99d52-ee65-11d3-9fde-00c07b727d3d`

Field	Description	Example
connecting endpoint	This field identifies the connecting endpoint (Gateway, or the H.323 device), that generated this call record. It includes the following: **gatekeeper IP address** The IP address of the Gatekeeper. **gatekeeper identifier** The globally unique name of the Gatekeeper. **endpoint IP address** The IP address of the endpoint. **endpoint identifier** The gatekeeper assigned identifier (or ?). **endpoint type** This identifies the endpoint as a gateway, gw, or terminal, tm (or ?). **answered** Identifies where the call was answered: 0 (ingress/near end) 1 (egress/far end) **trunk group** The call's trunk group number (or ?). **shelf** The call's shelf number (or ?). **slot** The call's slot number (or ?). **line** The call's line or DS1 number (or ?) **channel** The call's channel or DS0 number (or ?).	`192.168.35.238:mvam238:192.168.35.171:tnt171:gw:0:095:1:1:2:10`
bandwidth	This field specifies the number of 100 bps requested for a bi-directional call, for audio and video bit rates, excluding headers and overhead. It is displayed in bits per second.	`16000`

Field	Description	Example
calling party	This field identifies the calling party, or originator of the call. It includes the following: **real telephone number** The telephone number of the calling party (or ?). Only known if some form of calling party identification is being used (for example, PINs) **translated telephone number** The telephone number the real telephone number has been translated to (or ?). Exists when MVAM's ANI translation feature is used. **user alias** The administered user alias of the calling party (or ?). An alphanumeric string which uniquely identifies a user within a Gatekeeper's zone.	`60000:?:?`
calling endpoint	This field identifies the Gateway, or the H.323 device where the call originated. It includes the following: **gatekeeper IP address** The IP address of the Gatekeeper (or ?). **gatekeeper identifier** The globally unique name of the Gatekeeper (or ?). **endpoint IP address** The IP address of the endpoint. **endpoint identifier** The gatekeeper assigned identifier (or ?). **endpoint type** This identifies the endpoint as a gateway, `gw`, or terminal, `tm` (or ?).	`192.168.35.238:mvam238:192.168.35.171:tnt171:gw,`

Field	Description	Example
called endpoint	This field identifies the Gateway, or the H.323 device which completed the call. It includes the following: **gatekeeper IP address** The IP address of the Gatekeeper. **gatekeeper identifier** The globally unique name of the Gatekeeper. **endpoint IP address** The IP address of the endpoint. **endpoint identifier** The gatekeeper assigned identifier (or `?`). **endpoint type** This identifies the endpoint as a gateway, `gw`, or terminal, `tm` (or `?`).	`192.168.35.238:mvam238:192.168.35.172:tnt172:gw`
called party	This field identifies the called party. It includes the following: **primary DNIS** The first DNIS dialed. **secondary DNIS** The second DNIS dialed. **user alias** The administered user alias of the called party.	`?:66000:?`

Stop call record format

The stop call record is as follows:

Field	Description	Example
stop	This field identifies the call record as a stop record.	`stop`
date	This field contains the date the stop record was created (mm/dd/yyyy).	`02/17/2000`

Field	Description	Example
time	This field contains the time the stop record was created (hh:mm:ss).	`11:19:08`
call identifier	This field provides a globally unique call identifier for this call. This is a 32-character hexadecimal string whose content is determined by the endpoint (Gateway or terminal).	`eac99e7f-ee64-11d3-9ee2-00c07b727d3d`
disconnecting endpoint	This field identifies the Gateway, or H.323 device, which generated the stop record. It includes the following: **gatekeeper IP address** The IP address of the Gatekeeper. **gatekeeper identifier** The globally unique name of the Gatekeeper. **endpoint IP address** The IP address of the endpoint. **endpoint identifier** The gatekeeper assigned identifier (or ?). **endpoint type** This identifies the endpoint as a gateway, `gw`, or terminal, `tm` (or ?). **answered** Identifies where the call was answered: 0 (ingress/near end) 1 (egress/far end) **trunk group** The call's trunk group number (or ?). **shelf** The call's shelf number (or ?). **slot** The call's slot number (or ?). **line** The call's line or DS1 number (or ?) **channel** The call's channel or DS0 number (or ?).	`192.168.35.238:mvam238:192.168.35.172:tnt172:gw:1:?:1:1:5:2`

Field	Description	Example
disconnect reason	This field contains the reason the call was disconnected. This will contain one of four values: • forcedDrop • normalDrop • undefinedReason • gatewayFailure.	`normalDrop`
call duration	This field contains the length of the call measured in seconds (or ?). The call duration value is calculated by subtracting the call stop time recorded, when the first disconnect request is received, from the call start time recorded, when the first connect request is received. The field contains a ? when a duration cannot be calculated.	`132`

Incomplete call record format

The incomplete call record is as follows:

Field	Description	Example
incomplete	This field identifies the call record as a incomplete record.	`incomplete`
date	This field contains the date the stop record was created (mm/dd/yyyy).	`02/17/2000`
time	This field contains the time the stop record was created (hh:mm:ss).	`11:21:16`

Field	Description	Example
call identifier	This field provides a globally unique call identifier for this call. This is a 32-character hexadecimal string whose content is determined by the endpoint (Gateway or terminal).	`eac99dd9-ee65-11d3-a15e-00c07b727d3d`
disconnecting endpoint	This field identifies the Gateway, or H.323 device, which generated the stop record. It includes the following: **gatekeeper IP address** The IP address of the Gatekeeper. **gatekeeper identifier** The globally unique name of the Gatekeeper. **endpoint IP address** The IP address of the endpoint. **endpoint identifier** The gatekeeper assigned identifier (or ?). **endpoint type** This identifies the endpoint as a gateway, `gw`, or terminal, `tm` (or ?). **answered** Identifies where the call was answered: 0 (ingress/near end) 1 (egress/far end) **trunk group** The call's trunk group number (or ?). **shelf** The call's shelf number (or ?). **slot** The call's slot number (or ?). **line** The call's line or DS1 number (or ?). **channel** The call's channel or DS0 number (or ?).	`192.168.35.238:mvam238:192.168.35.171:tnt171:gw:0:625:1:1:26:12`

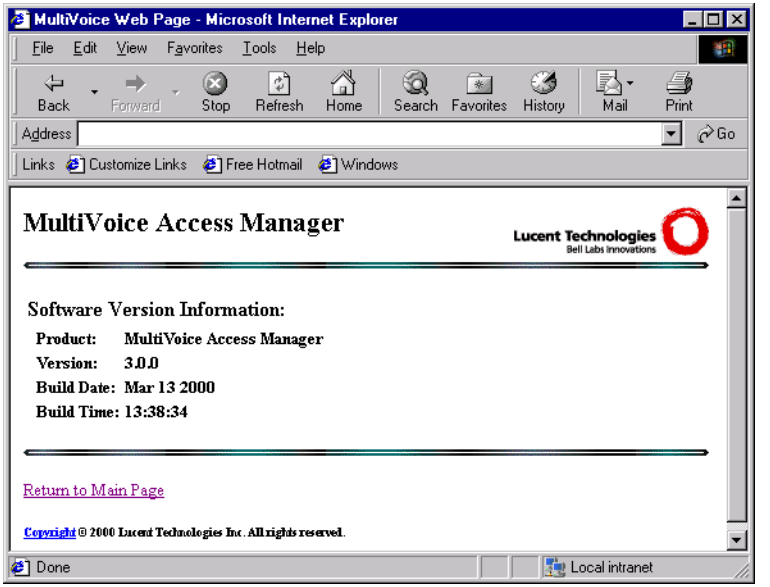
Field	Description	Example
calling party	This field identifies the calling party, or originator of the call. It includes the following: **real telephone number** The telephone number of the calling party (or ?). Only known if some form of calling party identification is being used (for example, PINs) **translated telephone number** The telephone number the real telephone number has been translated to (or ?). Exists when MVAM's ANI translation feature is used. **user alias** The administered user alias of the calling party (or ?). An alphanumeric string which uniquely identifies a user within a Gatekeeper's zone.	`7325781234:41234:dskran`
called party	This field identifies the called party. It includes the following: **primary DNIS** The first DNIS dialed. **secondary DNIS** The second DNIS dialed. **user alias** The administered user alias of the called party.	`4007:86000:?`
disconnect reason	This field contains the reason the call was disconnected. This will contain one of four values: • forcedDrop • normalDrop • undefinedReason • gatewayFailure.	`normalDrop`

Field	Description	Example
call duration	This field contains the length of the call measured in seconds (or ?). The call duration value is calculated by subtracting the call stop time recorded, when the first disconnect request is received, from the call start time recorded, when the first connect request is received. The field contains a ? when a duration cannot be calculated.	?

Displaying MVAM version

To display MVAM software version information, as illustrated in Figure 10-8, click `Misc: version` on the MVAM main page:

Figure 10-8. Software Version Information page



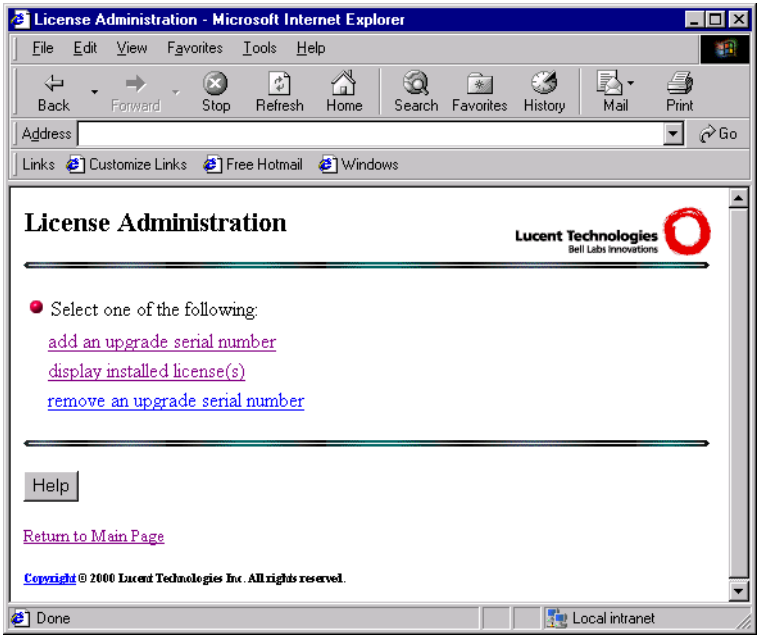
The machine in this example, is running MVAM version 3.0.0. The software was created on March 13, 2000 at 1:38 p.m.

License Administration

Note: For detailed information on MultiVoice Access Manager licenses, see Appendix B, “MVAM Licenses.”

To display the MultiVoice Access Manager License Administration page, as illustrated in Figure 10-9, click `Misc: license` on the MVAM main page:

Figure 10-9. License Administration page



From this page, you may perform the following license administration tasks:

Option	Description
add an upgrade serial number	This option is used to add an upgrade serial number.
display installed license(s)	This option is used to display the MultiVoice Access Manager licenses, implemented by serial numbers, on the current MVAM installation.
remove an upgrade serial number	This option is used to remove an upgrade serial number.

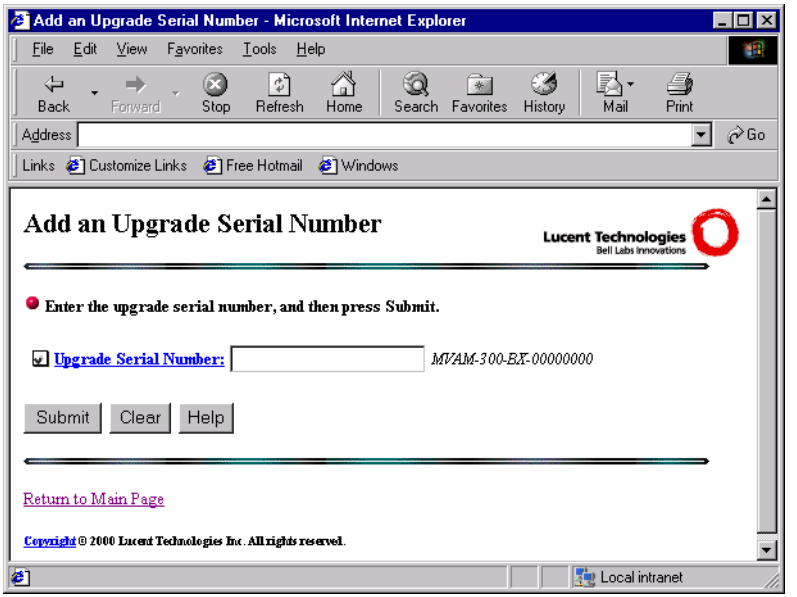
Note: You can get on-line help for any screen by clicking the Help button, or for specific fields by clicking any underlined field name.

Most Access Manager screens display 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.

Adding upgrade serial numbers

To add upgrade serial numbers to the current MVAM installation, click the Add an Upgrade Serial Number link on the License Administration page. The Add an Upgrade Serial Number page, as illustrated in Figure 10-10, appears:

Figure 10-10. Add an Upgrade Serial Number page

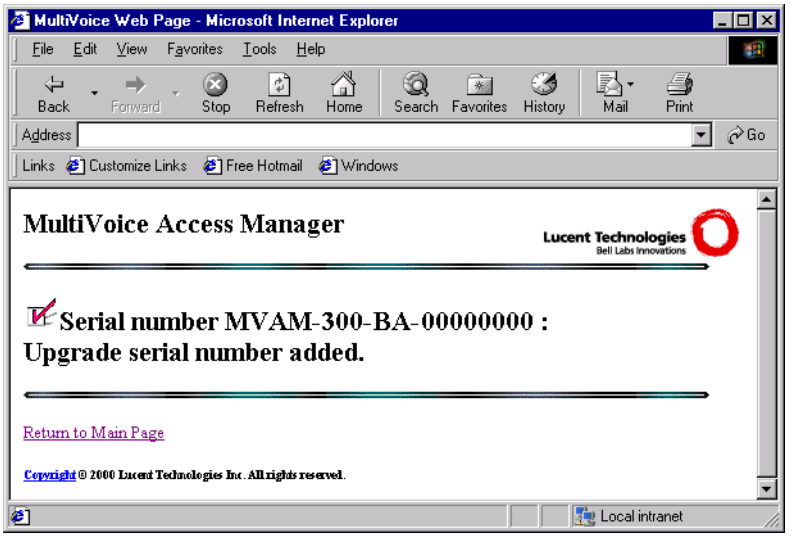


To add an upgrade serial number, enter the following information on this page:

Parameter	Description
Upgrade Serial Number	This is a alpha-numeric string. A unique serial number is provided with each License Pack.

Once you have entered this information, click the Submit button to save it. If the upgrade serial number is valid and was entered correctly, a confirmation message displays, as illustrated in Figure 10-11:

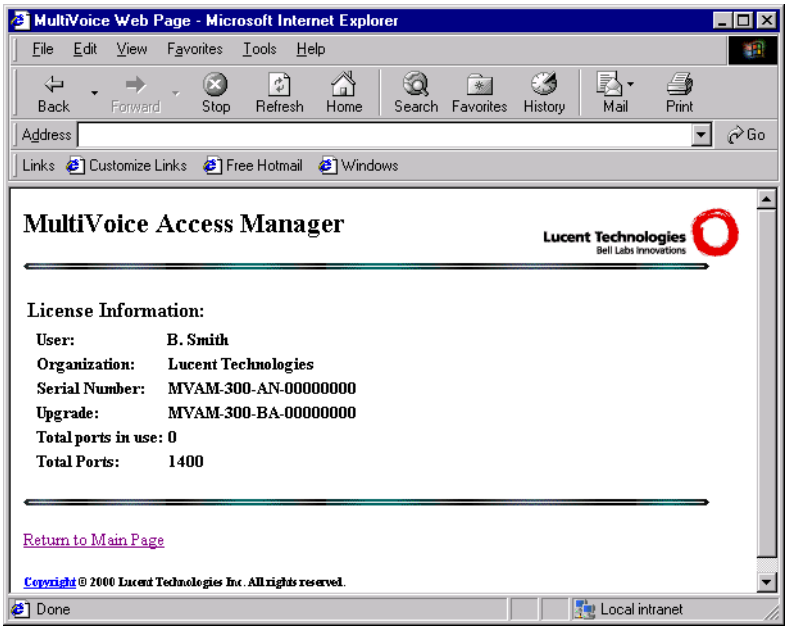
Figure 10-11. Upgrade serial number added



Displaying installed license(s)

Select this option to display the licenses installed on the current MVAM installation. Licenses are implemented by serial numbers. The MultiVoice Access Manager serial number and upgrade serial numbers, if installed, are displayed, as illustrated in

Figure 10-12. Display Installed License(s) page

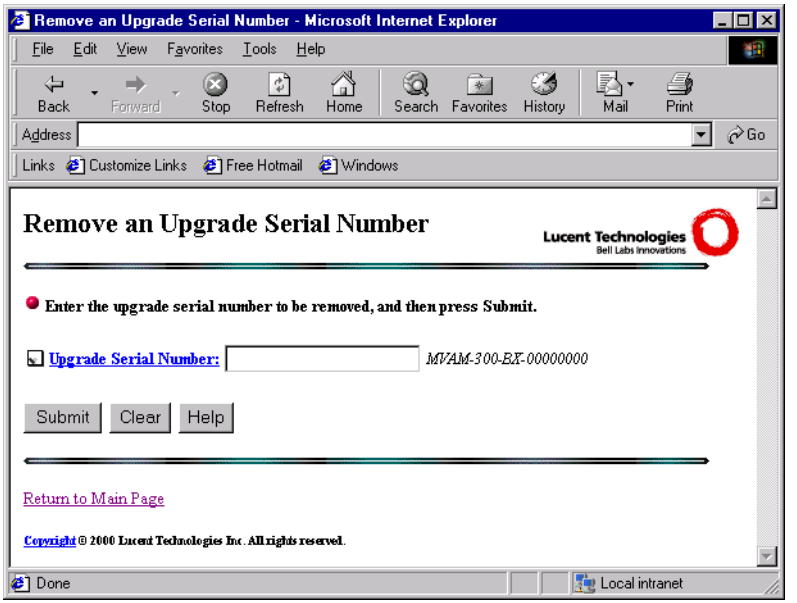


In this example, the MultiVoice Access Manager serial number is MVAM-300-AN-00000000, the upgrade serial number installed is MVAM-300-BA-00000000. There are no ports currently in use. The total number of ports supported on this MVAM installation is 1400.

Removing upgrade serial numbers

To remove upgrade serial numbers from the current MVAM installation, click the Remove an Upgrade Serial Number link on the License Administration page. The Remove an Upgrade Serial Number page, as illustrated in Figure 10-13, appears:

Figure 10-13. Remove an Upgrade Serial Number page

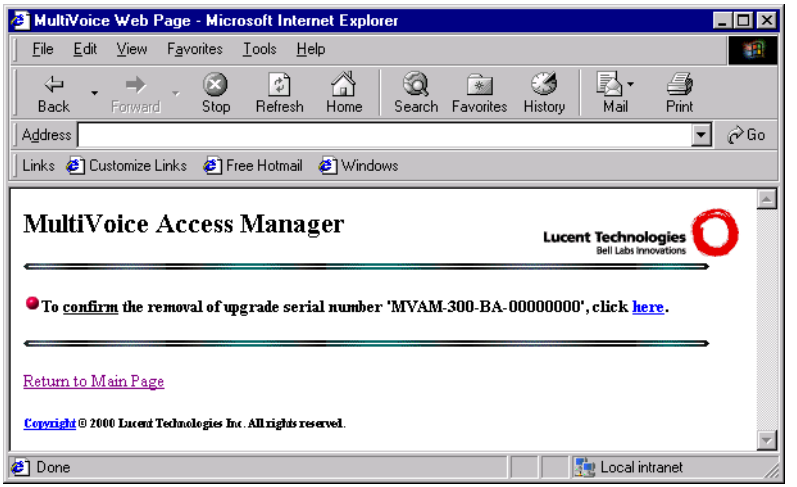


To remove an upgrade serial number, enter the following information on this page:

Parameter	Description
Upgrade Serial Number	This is a alpha-numeric string. A unique serial number is provided with each License Pack.

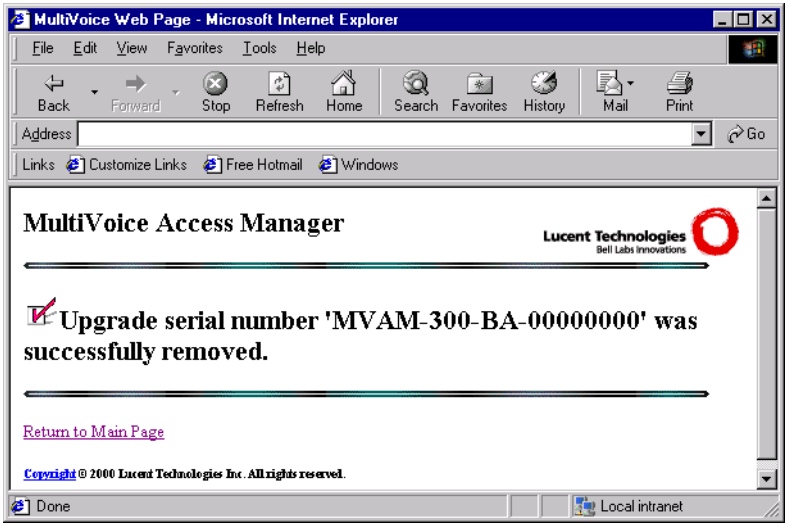
Once you have entered this information, click the Submit button to remove it from the current MVAM installation. You will be prompted to confirm the removal of the upgrade serial number entered, as illustrated in Figure 10-14:

Figure 10-14. Confirm removal of upgrade serial number



If the upgrade serial number is valid and was entered correctly, a confirmation message displays, as illustrated in Figure 10-15:

Figure 10-15. Upgrade serial number removed



Supported Gateways and Terminals

A MultiVoice Access Manager License installed on a Windows NT system supports a maximum of 400 ports. A MultiVoice Access Manager License installed on a SPARC Solaris or HP-UX system supports a maximum of 3000 ports.

License Packs allow you to increase the number of ports supported on your Windows NT, SPARC Solaris, or HP-UX system. License Packs are available in 1000, 5000, 10,000, and 20,000 port licenses. For more details on MultiVoice Access Manager licenses and License Packs, see Appendix B, “MVAM Licenses”.

Troubleshooting

11

Ensure the MultiVoice environment is set up correctly 11-1

Possible problems and solutions. 11-3

Error messages 11-8

Additional troubleshooting resources. 11-11

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.
- 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.
- If the MLG parameter on the Gateway is enabled, verify that a matching ADMA Rule is defined with PIN Authentication set to Yes (overriding authentication set on the MultiVoice Gateway).
- 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.
- If the MLG parameter on the Gateway is enabled, verify that a matching ADMA Rule is defined with ANI Authentication set to Yes (overriding authentication set on the MultiVoice Gateway).
- 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_cgi.exe

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

- Check the URL you're using to access MVAM. Make sure you have not opened a *file://* URL.
- Check your Web server configuration. Make sure it was properly configured to support CGI scripts. If you're using a standard Apache installation and have installed MVAM's CGI script in the existing Apache cgi-bin/ directory (as recommended), try the following URLs to run the Apache test CGI scripts:
  - http://localhost/cgi-gin/test-cgi
  - http://localhost/cgi-bin/printenv

  (or replace localhost as necessary with the name of the host running MVAM and the Web server). These test scripts are not available for Xitami or IIS under Windows NT. If you installed MVAM's HTML and CGI content somewhere other than the original document and CGI roots, these test scripts are not available for Apache under Solaris or HP-UX.

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 to ensure the values

are set correctly. (For a description of the MVAM Interface screen, see “MVAM interface screen” on page 11-24.)

Section	Parameter(s)	Setting
[insertIntoWin]	(all parameters)	The desired parameters must be set to 1 to display information in the Events Log file (on the console) and in the Events Log window. The default value is 0, displaying no information in the Events Log file (on the console) or in the Events Log window.

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 (for example: `c:\mvam\event\log.txt` on Windows NT; `/opt/mvam/event/log.txt` on Solaris or HP-UX), ensure that the event directory exists, and that the disk (Windows NT) or file system (Solaris, HP-UX) has space available.

Note: The event log file grows *very* quickly over time.

Also check the following sections of the mvam.ini file to ensure the values are set correctly.

Section	Parameters	Setting
[supserve]	msgfile	Controls debugging. 0–Events are not sent to the Events Log file (on the console) or to the Events Log window. 1–Events are sent to the Events Log file (on the console) and to the Events Log window. Events are specified in the [insertIntoWin] section.
[insertIntoWin]	(all parameters)	The desired parameters must be set to 1 to display information in the Events Log file (on the console) and in the Events Log window. The default value is 0, displaying no information in the Events Log file (on the console) or in the Events Log window.

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 MultiVoice Gateways register with MVAM. See the troubleshooting entry, “MVAM does not register a correctly configured gateway” on page 11-7.

- 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 your 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. The CLID will be displayed with the ARQ message in the MVAM Interface Screen if you set `[insertIntoWin]Ras=1` in the MVAM initialization file.

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 hear 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 MVAM from a MultiVoice Gateway.
  - From a MAX TNT: Enter the ping command and the numeric IP address of the MVAM on the command line.
  - From a MAX 1800/2000/6000: Press CTRL+D, then press E (E=Termsvr). Enter the ping command and the numeric IP address of the MVAM at the prompt.

  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 the Gateway parameters: Reg Retry and Keepalive Timer are set appropriately for the operating conditions on your 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 you 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, make 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.

Couldn’t read license.

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

Run the MultiVoice Access Manager License Installer (Windows NT) or `mvam_license.sh` (Solaris, HP-UX) to install a MultiVoice license. (See Appendix B, “MVAM Licenses” for instructions.) You will need the serial number from your MultiVoice Access Manager Warranty Registration card.

If you start Windows NT MVAM from the Start menu and the window appears and disappears so quickly that you cannot read the message in the window, there

is startup trouble, most likely, related to the license. Open a Command window and type the following:

```
c:\mvam\bin\mvam
```

(or the appropriate directory in which MVAM was installed). Read the message that appears in the window. If no message appears, increase the number of parameters enabled under the [insertIntoWindow] section of the initialization file. For example set the following: Mvam=1, Gen=1, Ras=1.

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

This message appears in the Web interface. 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) message.

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 no active calls.
- At the end of the call accounting cycle, when one call log is closed and a new call log was opened, but no calls have been initiated.

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 Number Translator/Call Router: calling thru 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 add a user with a name that you have specified for another user.

Users cannot share identical User Alias values.

Additional troubleshooting resources

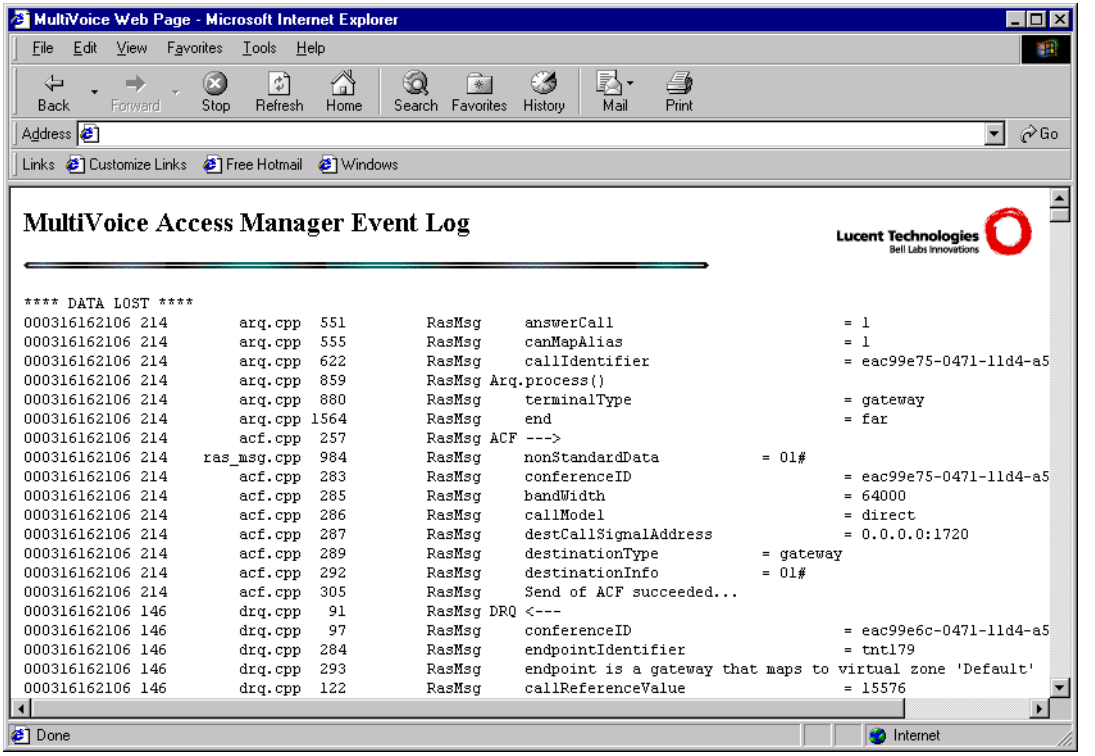
You can use the MVAM event log to troubleshoot problems on the MultiVoice network. You can also use the MVAM interface screen, which appears on the computer running MVAM when MVAM starts.

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 `Logs: event` to display the event log. The event log lists the communications between MultiVoice Gateways and MVAM, similar to Figure 11-1.

Figure 11-1. Access Manager Event Log page



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****`.

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 30.30.30.1).

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.

```
000306183230 5 rrq.cpp 148 RasMsg RRQ <---
000306183230 5 ras_msg.cpp 972 RasMsg nonStandardData =
0001P19=%C0&P17=120&P16=80&P15=9%2F1%2F1%2F1%2Ffffffe00%2C4%2F1%2F1%2F2%2Ffffffe00
%2C4%2F1%2F2%2F1%2Ffffffe00%2C4%2F1%2F2%2F2%2Ffffffe00
000306183230 5 rrq.cpp 319 RasMsg discoveryComplete = 0
000306183230 5 rrq.cpp 331 RasMsg callSignalAddress[1/1] = 10.10.10.1:1720
000306183230 5 rrq.cpp 338 RasMsg using callSignalAddress[1/1] = 10.10.10.1:1720
000306183230 5 rrq.cpp 345 RasMsg rasAddress[1/1] = 10.10.10.1:1025
000306183230 5 rrq.cpp 352 RasMsg using rasAddress[1/1] = 10.10.10.1:1025
000306183230 5 rrq.cpp 359 RasMsg terminalType = gateway
000306183230 5 rrq.cpp 370 RasMsg terminalAliases[1/1] = max101 (h323Id)
000306183230 5 rrq.cpp 408 RasMsg endpoint is a gateway that maps to virtual zone
Default
000306183230 5 rrq.cpp 440 RasMsg endpointVendor:
000306183230 5 rrq.cpp 441 RasMsg T35CountryCode = 0xb5
000306183230 5 rrq.cpp 442 RasMsg T35Extension = 0x0
000306183230 5 rrq.cpp 443 RasMsg manufacturerCode = 0x14
000306183230 5 rrq.cpp 444 RasMsg productID = Lucent Multi-Voice Gateway
000306183230 5 rrq.cpp 445 RasMsg versionID = 8.0-103.0c5
000306183230 5 rrq.cpp 467 RasMsg timeToLive = 120
000306183230 5 rcf.cpp 160 RasMsg RCF --->
000306183230 5 ras_msg.cpp 984 RasMsg nonStandardData = 0001P2=0&P19=%C0
000306183230 5 rcf.cpp 185 RasMsg callSignalAddress = 30.30.30.1:1720
000306183230 5 rcf.cpp 188 RasMsg terminalAlias:
000306183230 5 rcf.cpp 190 RasMsg h323-ID = max101
000306183230 5 rcf.cpp 198 RasMsg endpointIdentifier = max101
```

```
000306183230 5 rcf.cpp 200 RasMsg timeToLive = 120
000306183230 5 rcf.cpp 203 RasMsg Send of RCF succeeded...
```

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. No authentication is performed and the MultiVoice network is setup to support dual-stage dialing.

The originating MultiVoice Gateway sends an H.323 Admission Request (ARQ) packet to MVAM. The MultiVoice Access Manager searches for a terminating MultiVoice Gateway in its database and sends that information in an Admission Confirmation (ACF) packet to the originating MultiVoice Gateway. The originating gateway then communicates with the terminating gateway and the terminating MultiVoice Gateway sends an H.323 Admission Request (ARQ) packet to the MVAM. This is followed by an ACF back from MVAM to that gateway.

```
000306200054 5 arq.cpp 408 RasMsg ARQ <---
000306200054 5 arq.cpp 412 RasMsg conferenceID =
eac99dc6-fcb8-11d3-a7fa-00c07b8d9964
000306200054 5 arq.cpp 416 RasMsg call type = P2P
000306200054 5 arq.cpp 417 RasMsg call model = direct
000306200054 5 arq.cpp 435 RasMsg endpointIdentifier = MAX101
000306200054 5 arq.cpp 441 RasMsg endpointIdentifier is a gateway that maps to vir-
tual zone Default
000306200054 5 arq.cpp 470 RasMsg destinationInfo[1/1] = 919085551212 (e164)
000306200054 5 arq.cpp 479 RasMsg using destinationInfo[1/1] = 919085551212
000306200054 5 arq.cpp 497 RasMsg srcCallSignalAddress = 10.10.10.1:1720
000306200054 5 arq.cpp 520 RasMsg srcInfo[1/1] = 9085551234 (e164)
000306200054 5 arq.cpp 541 RasMsg using srcInfoE164 = 9085551234
000306200054 5 arq.cpp 547 RasMsg bandWidth = 64000
000306200054 5 arq.cpp 551 RasMsg answerCall = 0
000306200054 5 arq.cpp 555 RasMsg canMapAlias = 1
```

```
000306200054 5 ras_msg.cpp 972 RasMsg nonStandardData =
0001P10=9%2F%2D%2F%2D%2F1%2F1

000306200054 5 arq.cpp 622 RasMsg callIdentifier =
eac99dc6-fcb8-11d3-a7fa-00c07b8d9964

000306200054 5 arq.cpp 859 RasMsg Arq.process()

000306200054 5 arq.cpp 880 RasMsg terminalType = gateway

000306200054 5 arq.cpp 1247 RasMsg end = near

000306200054 5 arq.cpp 2285 RasMsg pin = not required

000306200054 5 arq.cpp 2329 RasMsg ani = not required

000306200054 5 acf.cpp 257 RasMsg ACF --->

000306200054 5 ras_msg.cpp 984 RasMsg nonStandardData = 919085551212

000306200054 5 acf.cpp 283 RasMsg conferenceID =
eac99dc6-fcb8-11d3-a7fa-00c07b8d9964

000306200054 5 acf.cpp 285 RasMsg bandWidth = 64000

000306200054 5 acf.cpp 286 RasMsg callModel = direct

000306200054 5 acf.cpp 287 RasMsg destCallSignalAddress = 20.20.20.1:1720

000306200054 5 acf.cpp 289 RasMsg destinationType = gateway

000306200054 5 acf.cpp 292 RasMsg destinationInfo = 919085551212

000306200054 5 acf.cpp 305 RasMsg Send of ACF succeeded...

000306200054 5 arq.cpp 408 RasMsg ARQ <---

000306200054 5 arq.cpp 412 RasMsg conferenceID =
eac99dc6-fcb8-11d3-a7fa-00c07b8d9964

000306200054 5 arq.cpp 416 RasMsg call type = P2P

000306200054 5 arq.cpp 417 RasMsg call model = direct

000306200054 5 arq.cpp 435 RasMsg endpointIdentifier = MAX201

000306200054 5 arq.cpp 441 RasMsg endpointIdentifier is a gateway that maps to vir-
tual zone Default

000306200054 5 arq.cpp 470 RasMsg destinationInfo[1/1] = 919085551212 (e164)

000306200054 5 arq.cpp 479 RasMsg using destinationInfo[1/1] = 919085551212

000306200054 5 arq.cpp 486 RasMsg destCallSignalAddress = 20.20.20.1:1720

000306200054 5 arq.cpp 497 RasMsg srcCallSignalAddress = 10.10.10.1:1720

000306200054 5 arq.cpp 520 RasMsg srcInfo[1/1] = MAX101 (h323Id)

000306200054 5 arq.cpp 537 RasMsg using srcInfoH323Id = MAX101

000306200054 5 arq.cpp 547 RasMsg bandWidth = 64000

000306200054 5 arq.cpp 551 RasMsg answerCall = 1

000306200054 5 arq.cpp 555 RasMsg canMapAlias = 1

000306200054 5 arq.cpp 622 RasMsg callIdentifier =
eac99dc6-fcb8-11d3-a7fa-00c07b8d9964
```

```
000306200054 5 arq.cpp 859 RasMsg Arq.process()
000306200054 5 arq.cpp 880 RasMsg terminalType = gateway
000306200054 5 arq.cpp 1564 RasMsg end = far
000306200054 5 acf.cpp 257 RasMsg ACF --->
000306200054 5 ras_msg.cpp 984 RasMsg nonStandardData = 919085551212
000306200054 5 acf.cpp 283 RasMsg conferenceID =
eac99dc6-fcb8-11d3-a7fa-00c07b8d9964
000306200054 5 acf.cpp 285 RasMsg bandWidth = 64000
000306200054 5 acf.cpp 286 RasMsg callModel = direct
000306200054 5 acf.cpp 287 RasMsg destCallSignalAddress = 0.0.0.0:1720
000306200054 5 acf.cpp 289 RasMsg destinationType = gateway
000306200054 5 acf.cpp 292 RasMsg destinationInfo = 919085551212
000306200054 5 acf.cpp 305 RasMsg Send of ACF succeeded...
000306200056 1 brq.cpp 82 RasMsg BRQ <---
000306200056 1 brq.cpp 88 RasMsg conferenceID =
eac99dc6-fcb8-11d3-a7fa-00c07b8d9964
000306200056 1 brq.cpp 107 RasMsg endpointIdentifier = MAX101
000306200056 1 brq.cpp 118 RasMsg endpoint is a gateway that maps to virtual zone
'Default'
000306200056 1 brq.cpp 142 RasMsg bandWidth = 5300
000306200056 1 brq.cpp 148 RasMsg callIdentifier =
eac99dc6-fcb8-11d3-a7fa-00c07b8d9964
000306200056 1 brq.cpp 157 RasMsg gatekeeperIdentifier = not found
000306200056 1 brq.cpp 163 RasMsg answeredCall = 0
000306200056 1 ras_msg.cpp 972 RasMsg nonStandardData =
0001P10=9%2F%2D%2F%2D%2F1%2F1
000306200056 1 brq.cpp 193 RasMsg Brq.process()
000306200056 1 bcf.cpp 83 RasMsg BCF --->
000306200056 1 bcf.cpp 86 RasMsg conferenceID =
eac99dc6-fcb8-11d3-a7fa-00c07b8d9964
000306200056 1 bcf.cpp 89 RasMsg bandWidth = 5300
000306200056 1 bcf.cpp 92 RasMsg Send of BCF succeeded...
000306200056 1 brq.cpp 82 RasMsg BRQ <---
000306200056 1 brq.cpp 88 RasMsg conferenceID =
eac99dc6-fcb8-11d3-a7fa-00c07b8d9964
000306200056 1 brq.cpp 107 RasMsg endpointIdentifier = MAX201
000306200056 1 brq.cpp 118 RasMsg endpoint is a gateway that maps to virtual zone
'Default'
```

```
000306200056 1 brq.cpp 142 RasMsg bandWidth = 5300
000306200056 1 brq.cpp 148 RasMsg callIdentifier =
eac99dc6-fcb8-11d3-a7fa-00c07b8d9964
000306200056 1 brq.cpp 157 RasMsg gatekeeperIdentifier = not found
000306200056 1 brq.cpp 163 RasMsg answeredCall = 1
000306200056 1 ras_msg.cpp 972 RasMsg nonStandardData =
0001P10=9%2F%2D%2F%2D%2F1%2F1
000306200056 1 brq.cpp 193 RasMsg Brq.process()
000306200056 1 bcf.cpp 83 RasMsg BCF --->
000306200056 1 bcf.cpp 86 RasMsg conferenceID =
eac99dc6-fcb8-11d3-a7fa-00c07b8d9964
000306200056 1 bcf.cpp 89 RasMsg bandWidth = 5300
000306200056 1 bcf.cpp 92 RasMsg Send of BCF succeeded...
```

When single-stage dialing is enabled for a MultiVoice network, destination dial string, `destinationInfo[1/1] = 919085551212 (e164)`, identifies the called telephone number, which the caller dialed together with the Gateway access number.

When MultiVoice is configured to perform ANI authentication, MVAM will verify the Calling Line ID (CLID) sent by the MultiVoice Gateway in the Admission Request (ARQ) packet against the user database. If a matching User Alias is located, MVAM will retrieve the user information and admit the call:

```
000306191013 5 arq.cpp 408 RasMsg ARQ <---
000306191013 5 arq.cpp 412 RasMsg conferenceID =
eac99da0-fcb1-11d3-a7fa-00c07b8d9964
000306191013 5 arq.cpp 416 RasMsg call type = P2P
000306191013 5 arq.cpp 417 RasMsg call model = direct
000306191013 5 arq.cpp 435 RasMsg endpointIdentifier = MAX101
000306191013 5 arq.cpp 441 RasMsg endpointIdentifier is a gateway that maps to vir-
tual zone Default
000306191013 5 arq.cpp 470 RasMsg destinationInfo[1/1] = 919085551212 (e164)
000306191013 5 arq.cpp 479 RasMsg using destinationInfo[1/1] = 919085551212
000306191013 5 arq.cpp 497 RasMsg srcCallSignalAddress = 10.10.10.1:1720
000306191013 5 arq.cpp 520 RasMsg srcInfo[1/1] = 9085551234 (e164)
000306191013 5 arq.cpp 541 RasMsg using srcInfoE164 = 9085551234
000306191013 5 arq.cpp 547 RasMsg bandWidth = 64000
```

```
000306191013 5 arq.cpp 551 RasMsg answerCall = 0
000306191013 5 arq.cpp 555 RasMsg canMapAlias = 1
000306191013 5 ras_msg.cpp 972 RasMsg nonStandardData =
0001P10=9%2F%2D%2F%2D%2F1%2F1
000306191013 5 arq.cpp 622 RasMsg callIdentifier =
eac99da0-fcb1-11d3-a7fa-00c07b8d9964
000306191013 5 arq.cpp 859 RasMsg Arq.process()
000306191013 5 arq.cpp 880 RasMsg terminalType = gateway
000306191013 5 arq.cpp 1247 RasMsg end = near
000306191013 5 arq.cpp 2285 RasMsg pin = not required
000306191013 5 arq.cpp 2313 RasMsg near-end user known by ANI:
000306191013 5 arq.cpp 2314 RasMsg userName = Robert Taylor
000306191013 5 arq.cpp 2315 RasMsg userAlias = 9085551234
000306191013 5 arq.cpp 2316 RasMsg phoneNum = 9085551111
000306191013 5 arq.cpp 2317 RasMsg phoneAlias =
000306191013 5 arq.cpp 2323 RasMsg pin = encrypted
000306191013 5 acf.cpp 257 RasMsg ACF --->
000306191013 5 ras_msg.cpp 984 RasMsg nonStandardData = 919085551212
000306191013 5 acf.cpp 283 RasMsg conferenceID =
eac99da0-fcb1-11d3-a7fa-00c07b8d9964
000306191013 5 acf.cpp 285 RasMsg bandWidth = 64000
000306191013 5 acf.cpp 286 RasMsg callModel = direct
000306191013 5 acf.cpp 287 RasMsg destCallSignalAddress = 20.20.20.1:1720
000306191013 5 acf.cpp 289 RasMsg destinationType = gateway
000306191013 5 acf.cpp 292 RasMsg destinationInfo = 919085551212
```

Note: Whenever the MVAM retrieves a user record, it writes all information from the user record to the event log.

When MultiVoice Gateways are configured to collect DNIS/ANI, `srcInfo[1/1] = 9085551234 (e164)` identifies the source dial string (ANI), which must match the caller's telephone number recorded in the user database.

When MultiVoice is configured to perform PIN authentication, MVAM will verify the PIN collected by the MultiVoice Gateway against the user database. If a matching PIN is located, MVAM will retrieve the user information and admit the call (both PIN and ANI authentication are shown in the following example):

```
000306193700 5 arq.cpp 408 RasMsg ARQ <---
000306193700 5 arq.cpp 412 RasMsg conferenceID =
eac99d33-fcb5-11d3-a7fa-00c07b8d9964
000306193700 5 arq.cpp 416 RasMsg call type = P2P
000306193700 5 arq.cpp 417 RasMsg call model = direct
000306193700 5 arq.cpp 435 RasMsg endpointIdentifier = MAX101
000306193700 5 arq.cpp 441 RasMsg endpointIdentifier is a gateway that maps to vir-
tual zone Default
000306193700 5 arq.cpp 470 RasMsg destinationInfo[1/1] = 919085551212 (e164)
000306193700 5 arq.cpp 479 RasMsg using destinationInfo[1/1] = 919085551212
000306193700 5 arq.cpp 497 RasMsg srcCallSignalAddress = 10.10.10.1:1720
000306193700 5 arq.cpp 520 RasMsg srcInfo[1/1] = 9085551234 (e164)
000306193700 5 arq.cpp 541 RasMsg using srcInfoE164 = 9085551234
000306193700 5 arq.cpp 547 RasMsg bandWidth = 64000
000306193700 5 arq.cpp 551 RasMsg answerCall = 0
000306193700 5 arq.cpp 555 RasMsg canMapAlias = 1
000306193700 5 ras_msg.cpp 972 RasMsg nonStandardData =
0001P9=2%2F%01&P10=9%2F%2D%2F%2D%2F1%2F1
000306193700 5 arq.cpp 608 RasMsg pin = encrypted
000306193700 5 arq.cpp 622 RasMsg callIdentifier =
eac99d33-fcb5-11d3-a7fa-00c07b8d9964
000306193700 5 arq.cpp 859 RasMsg Arq.process()
000306193700 5 arq.cpp 880 RasMsg terminalType = gateway
000306193700 5 arq.cpp 1247 RasMsg end = near
000306193700 5 arq.cpp 2269 RasMsg near-end user known by PIN:
000306193700 5 arq.cpp 2270 RasMsg userName = Robert Taylor
000306193700 5 arq.cpp 2271 RasMsg userAlias = 9085551234
000306193700 5 arq.cpp 2272 RasMsg phoneNum = 9085551111
000306193700 5 arq.cpp 2273 RasMsg phoneAlias =
000306193700 5 arq.cpp 2279 RasMsg pin = encrypted
000306193700 5 arq.cpp 2313 RasMsg near-end user known by ANI:
000306193700 5 arq.cpp 2314 RasMsg userName = Robert Taylor
000306193700 5 arq.cpp 2315 RasMsg userAlias = 9085551234
000306193700 5 arq.cpp 2316 RasMsg phoneNum = 9085551111
000306193700 5 arq.cpp 2317 RasMsg phoneAlias =
000306193700 5 arq.cpp 2323 RasMsg pin = encrypted
```

```
000306193700 5 acf.cpp 257 RasMsg ACF --->
000306193700 5 ras_msg.cpp 984 RasMsg nonStandardData = 919085551212
000306193700 5 acf.cpp 283 RasMsg conferenceID =
eac99d33-fcb5-11d3-a7fa-00c07b8d9964
000306193700 5 acf.cpp 285 RasMsg bandWidth = 64000
000306193700 5 acf.cpp 286 RasMsg callModel = direct
000306193700 5 acf.cpp 287 RasMsg destCallSignalAddress = 20.20.20.1:1720
000306193700 5 acf.cpp 289 RasMsg destinationType = gateway
000306193700 5 acf.cpp 292 RasMsg destinationInfo = 919085551212
000306193700 5 acf.cpp 305 RasMsg Send of ACF succeeded...
```

When a call disconnects, both the originating and terminating Gateways send an H.225 DisengageRequest (DRQ) packet to the MVAM. In turn, MVAM sends a DisengageConfirmation (DCF) packet back to each of the Gateways. This is illustrated in the event log below.

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

```
000306191019 1 drq.cpp 91 RasMsg DRQ <---
000306191019 1 drq.cpp 97 RasMsg conferenceID =
eac99da0-fcb1-11d3-a7fa-00c07b8d9964
000306191019 1 drq.cpp 284 RasMsg endpointIdentifier = MAX101
000306191019 1 drq.cpp 293 RasMsg endpoint is a gateway that maps to virtual zone
'Default'
000306191019 1 drq.cpp 122 RasMsg callReferenceValue = 9389
000306191019 1 drq.cpp 128 RasMsg disengageReason = normal drop
000306191019 1 drq.cpp 134 RasMsg callIdentifier =
eac99da0-fcb1-11d3-a7fa-00c07b8d9964
000306191019 1 drq.cpp 143 RasMsg gatekeeperIdentifier = not found
000306191019 1 drq.cpp 149 RasMsg answeredCall = 0
000306191019 1 ras_msg.cpp 972 RasMsg nonStandardData =
0001P10=9%2F%2D%2F%2D%2F1%2F1
000306191019 1 drq.cpp 180 RasMsg Drq.process()
000306191019 1 dcf.cpp 62 RasMsg DCF --->
000306191019 1 dcf.cpp 65 RasMsg conferenceID =
eac99da0-fcb1-11d3-a7fa-00c07b8d9964
000306191019 1 dcf.cpp 69 RasMsg Send of DCF succeeded...
```

```
000306191019 1 drq.cpp 91 RasMsg DRQ <---
000306191019 1 drq.cpp 97 RasMsg conferenceID =
eac99da0-fcb1-11d3-a7fa-00c07b8d9964
000306191019 1 drq.cpp 284 RasMsg endpointIdentifier = MAX201
000306191019 1 drq.cpp 293 RasMsg endpoint is a gateway that maps to virtual zone
'Default'
000306191019 1 drq.cpp 122 RasMsg callReferenceValue = 9389
000306191019 1 drq.cpp 128 RasMsg disengageReason = normal drop
000306191019 1 drq.cpp 134 RasMsg callIdentifier =
eac99da0-fcb1-11d3-a7fa-00c07b8d9964
000306191019 1 drq.cpp 143 RasMsg gatekeeperIdentifier = not found
000306191019 1 drq.cpp 149 RasMsg answeredCall = 1
000306191019 1 ras_msg.cpp 972 RasMsg nonStandardData =
0001P10=9%2F%2D%2F%2D%2F1%2F1
000306191019 1 drq.cpp 180 RasMsg Drq.process()
000306191019 1 dcf.cpp 62 RasMsg DCF --->
000306191019 1 dcf.cpp 65 RasMsg conferenceID =
eac99da0-fcb1-11d3-a7fa-00c07b8d9964
000306191019 1 dcf.cpp 69 RasMsg Send of DCF succeeded...
```

Example of an unsuccessful call

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

```
000306194435 5 arq.cpp 408 RasMsg ARQ <---
000306194435 5 arq.cpp 412 RasMsg conferenceID =
eac99d4d-fcb6-11d3-a7fa-00c07b8d9964
000306194435 5 arq.cpp 416 RasMsg call type = P2P
000306194435 5 arq.cpp 417 RasMsg call model = direct
000306194435 5 arq.cpp 435 RasMsg endpointIdentifier = MAX101
000306194435 5 arq.cpp 441 RasMsg endpointIdentifier is a gateway that maps to vir-
tual zone Default
000306194435 5 arq.cpp 470 RasMsg destinationInfo[1/1] = 912015551212 (e164)
000306194435 5 arq.cpp 479 RasMsg using destinationInfo[1/1] = 912015551212
000306194435 5 arq.cpp 497 RasMsg srcCallSignalAddress = 10.10.10.1:1720
000306194435 5 arq.cpp 520 RasMsg srcInfo[1/1] = 9085551234 (e164)
000306194435 5 arq.cpp 541 RasMsg using srcInfoE164 = 9085551234
```

```
000306194435 5 arq.cpp 547 RasMsg bandWidth = 64000
000306194435 5 arq.cpp 551 RasMsg answerCall = 0
000306194435 5 arq.cpp 555 RasMsg canMapAlias = 1
000306194435 5 ras_msg.cpp 972 RasMsg nonStandardData =
0001P10=9%2F%2D%2F%2D%2F1%2F1
000306194435 5 arq.cpp 622 RasMsg callIdentifier =
eac99d4d-fcb6-11d3-a7fa-00c07b8d9964
000306194435 5 arq.cpp 859 RasMsg Arq.process()
000306194435 5 arq.cpp 880 RasMsg terminalType = gateway
000306194435 5 arq.cpp 1247 RasMsg end = near
000306194435 5 arq.cpp 2285 RasMsg pin = not required
000306194435 5 arq.cpp 2329 RasMsg ani = not required
000306194435 5 arq.cpp 1430 RasMsg route of call failed
000306194435 5 arj.cpp 83 RasMsg ARJ --->
000306194435 5 arj.cpp 85 RasMsg rejectReason = route of call failed
000306194435 5 arj.cpp 86 RasMsg Attempting to clear call record from active call
table
000306194435 5 arj.cpp 89 RasMsg conferenceID =
eac99d4d-fcb6-11d3-a7fa-00c07b8d9964
000306194435 5 arj.cpp 112 RasMsg Send of ARJ succeeded...
```

In the following example, MVAM could not authenticate a caller, using ANI authentication, and rejects the call:

```
000306194726 5 arq.cpp 408 RasMsg ARQ <---
000306194726 5 arq.cpp 412 RasMsg conferenceID =
eac99df9-fcb6-11d3-a7fa-00c07b8d9964
000306194726 5 arq.cpp 416 RasMsg call type = P2P
000306194726 5 arq.cpp 417 RasMsg call model = direct
000306194726 5 arq.cpp 435 RasMsg endpointIdentifier = MAX101
000306194726 5 arq.cpp 441 RasMsg endpointIdentifier is a gateway that maps to vir-
tual zone Default
000306194726 5 arq.cpp 470 RasMsg destinationInfo[1/1] = 919085551212 (e164)
000306194726 5 arq.cpp 479 RasMsg using destinationInfo[1/1] = 919085551212
000306194726 5 arq.cpp 497 RasMsg srcCallSignalAddress = 10.10.10.1:1720
000306194726 5 arq.cpp 520 RasMsg srcInfo[1/1] = 9085551234 (e164)
000306194726 5 arq.cpp 541 RasMsg using srcInfoE164 = 9085551234
000306194726 5 arq.cpp 547 RasMsg bandWidth = 64000
```

```
000306194726 5 arq.cpp 551 RasMsg answerCall = 0
000306194726 5 arq.cpp 555 RasMsg canMapAlias = 1
000306194726 5 ras_msg.cpp 972 RasMsg nonStandardData =
0001P10=9%2F%2D%2F%2D%2F1%2F1
000306194726 5 arq.cpp 622 RasMsg callIdentifier =
eac99df9-fcb6-11d3-a7fa-00c07b8d9964
000306194726 5 arq.cpp 859 RasMsg Arq.process()
000306194726 5 arq.cpp 880 RasMsg terminalType = gateway
000306194726 5 arq.cpp 1247 RasMsg end = near
000306194726 5 arq.cpp 2285 RasMsg pin = not required
000306194726 5 arq.cpp 2308 RasMsg *** ERROR ***>>> Can't determine calling user --
unknown ANI
000306194726 5 arj.cpp 83 RasMsg ARJ --->
000306194726 5 arj.cpp 85 RasMsg rejectReason = unknown ANI
000306194726 5 arj.cpp 86 RasMsg Attempting to clear call record from active call
table
000306194726 5 arj.cpp 89 RasMsg conferenceID =
eac99df9-fcb6-11d3-a7fa-00c07b8d9964
000306194726 5 arj.cpp 112 RasMsg Send of ARJ succeeded...
```

In the following example, MVAM could not authenticate a caller, using PIN authentication, and rejects the call:

```
000306195035 5 arq.cpp 408 RasMsg ARQ <---
000306195035 5 arq.cpp 412 RasMsg conferenceID =
eac99d08-fcb7-11d3-a7fa-00c07b8d9964
000306195035 5 arq.cpp 416 RasMsg call type = P2P
000306195035 5 arq.cpp 417 RasMsg call model = direct
000306195035 5 arq.cpp 435 RasMsg endpointIdentifier = MAX101
000306195035 5 arq.cpp 441 RasMsg endpointIdentifier is a gateway that maps to vir-
tual zone Default
000306195035 5 arq.cpp 470 RasMsg destinationInfo[1/1] = 919085551212 (e164)
000306195035 5 arq.cpp 479 RasMsg using destinationInfo[1/1] = 919085551212
000306195035 5 arq.cpp 497 RasMsg srcCallSignalAddress = 10.10.10.1:1720
000306195035 5 arq.cpp 520 RasMsg srcInfo[1/1] = 9085551234 (e164)
000306195035 5 arq.cpp 541 RasMsg using srcInfoE164 = 9085551234
000306195035 5 arq.cpp 547 RasMsg bandWidth = 64000
000306195035 5 arq.cpp 551 RasMsg answerCall = 0
```

```
000306195035 5 arq.cpp 555 RasMsg canMapAlias = 1
000306195035 5 ras_msg.cpp 972 RasMsg nonStandardData =
0001P9=2%2F%0A%05&P10=9%2F%2D%2F%2D%2F1%2F1
000306195035 5 arq.cpp 608 RasMsg pin = encrypted
000306195035 5 arq.cpp 622 RasMsg callIdentifier =
eac99d08-fcb7-11d3-a7fa-00c07b8d9964
000306195035 5 arq.cpp 859 RasMsg Arq.process()
000306195035 5 arq.cpp 880 RasMsg terminalType = gateway
000306195035 5 arq.cpp 1247 RasMsg end = near
000306195035 5 arq.cpp 2264 RasMsg *** ERROR ***>>> Can't determine calling user -
unknown PIN
000306195035 5 arj.cpp 83 RasMsg ARJ --->
000306195035 5 arj.cpp 85 RasMsg rejectReason = unknown PIN
000306195035 5 arj.cpp 86 RasMsg Attempting to clear call record from active call
table
000306195035 5 arj.cpp 89 RasMsg conferenceID =
eac99d08-fcb7-11d3-a7fa-00c07b8d9964
000306195035 5 arj.cpp 112 RasMsg Send of ARJ succeeded...
```

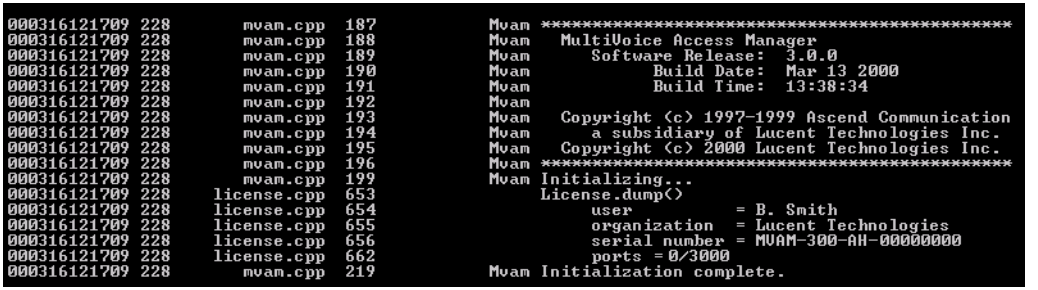
MVAM interface screen

The MVAM Interface screen displays real-time information.

Viewing real-time information

When you launch MVAM, the MVAM interface screen appears, similar to Figure 11-2:

Figure 11-2. Access Manager Interface screen



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.

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

MVAM Initialization File

A

When you install MVAM, the MVAM installer creates the initialization file `mvam.ini`. 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.

Typically, you should not have to change any settings in the file manually. You configure the most common settings in MVAM through the Web browser connection, or during installation. However, changing parameters related to capacity may be necessary over time as call volume increases.



Caution: Before modifying the initialization file, copy the original initialization file to `mvam.ini.old`.



Caution: You do not need to copy the original initialization file prior to upgrading or installing MVAM. During MVAM installation, the mvam.ini file is backed up automatically. On WindowsNT, the initialization file is backed up to mvam.ini.BAK. On Solaris and on HP-UX, the initialization file is backed up to mvam.ini.OLD.

Table A-1 shows the parameters stored in the MVAM initialization file, including the default settings. The sections and parameters shown in this table are listed in

alphabetical order for ease of use. In the actual initializaton file, there is a default order that may be changed by the user.

Note: If parameters are removed, or values are removed or entered incorrectly, MVAM may not produce the results you expect.

Table A-1. MVAM initialization file parameters

Section	Parameter	Description	Default Value
Act	capacity	Maximum number of calls that MVAM can monitor.	20000
Act	enabled	Determines whether MVAM logs calls in the Active Call table. 0 = False 1 = True (default)	1
Act[a]	filePath	Identifies the path to the MVAM call-log file.	c:\mvam\calls\ (WinNT) /opt/mvam/calls (Solaris, HP-UX)
Act[a]	maxAllowableCallLength	Specifies the number of seconds per call length. This feature is disabled if this value is set to 60 seconds or less.	86400
Act[a]	writeStartCdrPerParty	Specifies whether a start call detail record is written for each call endpoint. 0 = disabled 1 = enabled (default)	1

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

Section	Parameter	Description	Default Value
Act[a]	writeStopCdrPerParty	Specifies whether a stop call detail record is written for each call endpoint. 0 = disabled 1 = enabled (default)	1
Act[b]	frequency	Specifies how often MVAM creates a new call-log file. once daily (default) weekly monthly	daily
Adma	rules	Identifies the path and filename of the ADMA Rules database.	c:\mvam\db\rules.txt (WinNT) /opt/mvam/db/rules.txt (Solaris, HP-UX)
Adma	ruleSets	Identifies the path and filename of the ADMA Rule Sets database.	c:\mvam\db\ ruleSets.txt (WinNT) /opt/mvam/db/ ruleSets.txt (Solaris, HP-UX)
Adma	table	Identifies the path and filename of the ADMA Gateway/Trunk Rules database.	c:\mvam\db\table.txt (WinNT) /opt/mvam/db/table.txt (Solaris, HP-UX)

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

Section	Parameter	Description	Default Value
AliasANI	*A Gateway Name.* *This parameter is specified by the user.* *Example: max120*	Specifies a false ANI used by an egress Gateway, if canMapAlias, on the egress Gateway, is set to true. The egress Gateway Name must match the AliasANI parameter name specified. Must be a valid telephone number, up to 24 digits (maximum).	(*No Value assigned*) *Example: 5781234*
Api	configFile	Specifies the path to the configuration file.	amv_gk_table
Api	name	Specifies the MVAM.	default
CallLog	size	Maximum number of lines allowed in the MVAM call log file.	1000
Ept	ageGatewayRegistration	Determines whether MultiVoice Gateways must perform keep-alive registrations. 0 = No 1 = Yes (default)	1
Ept	ageTerminalRegistration	Determines whether terminals must perform keep-alive registrations. (Administered through the Web interface.) 0 = No 1 = Yes (default)	1

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

Section	Parameter	Description	Default Value
Ept	dropsCallOn ExpiredGateways	Determines whether MVAM logs active calls on an unregistered MultiVoice Gateway as dropped calls. 0 = False 1 = True (default)	1
Ept	registrationPeriodMargin	Sets the amount of time, beyond the registration period, after which a registration is considered to be expired. (Administered through the Web interface.)	30
EventLog	frequency	Specifies the frequency [EventLog]file is created Daily, weekly, monthly, once.	daily
EventLog	size	Maximum number of lines allowed in the event log.	1000
EventLog[a]	file	Identifies the path and filename of the event log.	c:\mvam\events\log.txt (WinNT) /opt/mvam/events/ log.txt (Solaris, HP-UX)
Gkcp[a]	webPagePath	Identifies the path to the MVAM Web pages.	c:\mvam\webpages\ (WinNT) /opt/mvam/htdocs/ (Solaris, HP-UX)

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

Section	Parameter	Description	Default Value
Gkct	displayCapacity	Sets the maximum number of inclusion areas which may be displayed through the administration interface for each Gatekeeper.	25
Gkct	file	Identifies the path and filenname of the Gatekeeper Coverage Area database.	c:\mvam\db\gkc.txt (WinNT) /opt/mvam/db/gkc.txt (Solaris, HP-UX)
Gkct	listCapacity	Sets the maximum number of inclusion areas which may be assigned to a single Gatekeeper. Valid values are 1 through 2000.	2000
Gkt	capacity	Identifies the maximum number of Gatekeepers stored in the Gatekeeper database.	32
Gkt	file	Identifies the path and filename of the MultiVoice Gatekeeper database.	c:\mvam\db\gk.txt (WinNT) /opt/mvam/db/gk.txt (Solaris, HP-UX)
Gwct[a]	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 listCapacity.	25

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

Section	Parameter	Description	Default Value
Gwct[a]	file	Identifies the path and filename of the MultiVoice Gateway coverage area database.	c:\mvam\db\gwc.txt (WinNT) /opt/mvam/db/gwc.txt (Solaris, HP-UX)
Gwct[a]	listCapacity	Defines the maximum number of Inclusion Areas allowed per MultiVoice Gateway. Valid values are 1 through 2000.	2000
GwRouting	maxRoutableCapacity	Specifies the percentage of total available ports on the Gateway based on the minimum number of DS0, DSP, or Max VoIP calls.	98
GwRouting	RoutingAlgorithm	Specifies the type of algorithm MVAM will use to route calls. Valid values are: loadBalancing = MVAM uses a port usage ratio to make call routing decisions on the Gateways. useCount = MVAM makes call routing decisions based on the number of calls routed on each Gateway.	loadBalancing
Gwt[a]	file	Identifies the path and filename of the MultiVoice Gateway database.	c:\mvam\db\gwt.txt (WinNT) /opt/mvam/db/gwt.txt (Solaris, HP-UX))

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

Section	Parameter	Description	Default Value
insertInto Win	Act	Determines whether the source information is displayed in the Events Log file (on the console) and in the Events Log window. 0=False 1=True (default)	0
insertInto Win	Ept	Determines whether the source information is displayed in the Events Log file (on the console) and in the Events Log window. 0=False 1=True (default)	0
insertInto Win	Gen	Determines whether the source information is displayed in the Events Log file (on the console) and in the Events Log window. 0=False 1=True (default)	0
insertInto Win	Gkcp	Determines whether the source information is displayed in the Events Log file (on the console) and in the Events Log window. 0=False 1=True (default)	0

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

Section	Parameter	Description	Default Value
insertInto Win	Gkct	Determines whether the source information is displayed in the Events Log file (on the console) and in the Events Log window. 0=False 1=True (default)	0
insertInto Win	Gkt	Determines whether the source information is displayed in the Events Log file (on the console) and in the Events Log window. 0=False 1=True (default)	0
insertInto Win	Gwct	Determines whether the source information is displayed in the Events Log file (on the console) and in the Events Log window. 0=False 1=True (default)	0
insertInto Win	Gwt	Determines whether the source information is displayed in the Events Log file (on the console) and in the Events Log window. 0=False 1=True (default)	0

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

Section	Parameter	Description	Default Value
insertInto Win	Mvam	Determines whether the source information is displayed in the Events Log file (on the console) and in the Events Log window. 0=False 1=True (default)	1
insertInto Win	Nxtl	Determines whether the source information is displayed in the Events Log file (on the console) and in the Events Log window. 0=False 1=True (default)	0
insertInto Win	Odbc	Determines whether the source information is displayed in the Events Log file (on the console) and in the Events Log window. 0=False 1=True (default)	0
insertInto Win	Prefixer	Determines whether the source information is displayed in the Events Log file (on the console) and in the Events Log window. 0=False 1=True (default)	0

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

Section	Parameter	Description	Default Value
insertInto Win	Ras	Determines whether the source information is displayed in the Events Log file (on the console) and in the Events Log window. 0=False 1=True (default)	0
insertInto Win	Router	Determines whether the source information is displayed in the Events Log file (on the console) and in the Events Log window. 0=False 1=True (default)	0
insertInto Win	Sec	Determines whether the source information is displayed in the Events Log file (on the console) and in the Events Log window. 0=False 1=True (default)	0
insertInto Win	Translator	Determines whether the source information is displayed in the Events Log file (on the console) and in the Events Log window. 0=False 1=True (default)	0

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

Section	Parameter	Description	Default Value
insertInto Win	Tt	Determines whether the source information is displayed in the Events Log file (on the console) and in the Events Log window. 0=False 1=True (default)	0
insertInto Win	UtOdbc	Determines whether the source information is displayed in the Events Log file (on the console) and in the Events Log window. 0=False 1=True (default)	0
insertInto Win	UtText	Determines whether the source information is displayed in the Events Log file (on a console) and in the Events Log window. 0=False 1=True (default)	0
Mvam	debugPrinting	Enables/disables application level event logging. 0 = disabled 1 = enabled	1
Mvam	epToEpKeepAlivePeriod	Determines endpoint to endpoint keep-alive period in seconds. 0=No keep alive.	0

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

Section	Parameter	Description	Default Value
Mvam	keepStats	Controls the generation of RAS statistics. Valid values are 0 (false) and 1 (true).	0
Mvam	realMultiZone	Enables/disables real MultiZone call routing (Gatekeeper to Gatekeeper communications.) 0 = disabled 1 = enabled	1
Nxtl	capacity	Sets the maximum number of Number Translation tables which may be created on a Gateway.	512
Nxtl	displayCapacity	Sets the maximum number of translation rules which may be displayed in a single row through the administration interface for a Number Translation table.	5
Nxtl	file	Identifies the path and filename of the Number Translation database.	c:\mvam\db\nxtl.txt (WinNT) /opt/mvam/db/nxtl.txt (Solaris, HP-UX)
Nxtl	nxtCapacity	Sets the maximum number of translation rules which may be created for a single Number Translation table.	100

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

Section	Parameter	Description	Default Value
Nxtl	nxtPath	Identifies the logical directory path to the Number Translation table directory.	c:\mvam\db\nxts\ (WinNT) /opt/mvam/db/nxts/ (Solaris, HP-UX)
Prefixer	aliasPrefix	Specifies the Telephone Alias dialing prefix. Valid entries are *1 through *9. Alias dialing is not supported in a MultiVoice network.	*2
Prefixer	passThruPrefix	Specifies the pass-through dialing prefix. Valid entries are *1 through *9.	(*No Value assigned*)
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	gatekeeperIdentifier	Sets the Gatekeeper identifier of the MVAM. (Administered through the Web interface.)	gkId
Ras	gatewayRegistration Period	Sets the desired Gateway re-registration period. (Administered through the Web interface.)	120

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

Section	Parameter	Description	Default Value
Ras	maxSimulLrq	Specifies the number of parallel LRQs that will be sent.	3
Ras	terminalRegistration Period	Sets the terminal re-registration period. (Administered through the Web interface.)	120
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
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

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

Section	Parameter	Description	Default Value
Sec	allowPcToPhone	Determines whether to process call requests from H.323-compliant terminals. 0 = disabled 1 = enabled (default)	1
Sec	allowPhoneToPC	Determines whether to process call requests to H.323-compliant terminals. 0 = disabled 1 = enabled (default)	1
Sec	allowTerminalsTo Register	Determines whether H.323-compliant terminals are allowed to register. 0 = disabled 1 = enabled (default)	1
Sec	aniRequired	Determines whether or not the MVAM performs ANI authentication: 0 = False (default) 1 = True	0
Sec	displayPinInEventLog	Determines whether or not the user PINs are included in the event log displayed on the screen: 0 = False (default) 1 = True	0

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

Section	Parameter	Description	Default Value
Sec	ignoreTerminalBrqs[c]	Determines whether to ignore bandwidth change request messages (BRQs) from H.323-compliant terminals. 0 = disabled (default) 1 = enabled	0
Sec	ignoreTerminalDrqs[b]	Determines whether to ignore disconnect request messages (DRQs) from H.323-compliant terminals. 0 = disabled (default) 1 = enabled	0
Sec	pinSize	Sets the size (number of digits entered) of user PIN codes. Valid values are 1 through 24. This value defaults to 10 (digits).	10
Sec	proxyPinRequired	Determines whether or not the MVAM performs PIN authentication: 0 = False (default) 1 = True	0

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

Section	Parameter	Description	Default Value
supserve	msgfile	Controls whether the Event Log gets written to the Events Log file ((WinNT – c:\mvam\events\log.txt Solaris, HP-UX – /opt/mvam/events/log.txt) 0–Events are not sent to the Events Log file (on the console) or to the Events Log window. 1–Events are sent to the Events Log file (on the console) and to the Events Log window. Events are specified in the [insertIntoWin] section. **Note:** The events log file can grow very quickly over time.	0
Tt	file	Identifies the path and filename of the Terminal database.	c:\mvam\db\t.txt (WinNT) /opt/mvam/db/t.txt (Solaris, HP-UX)
Tt	MinE164Size	Specifies the minimum digits for a terminal's E164 address.	7
Tt	nxtIn	Identifies the ingress number translation table used for processing calls from PC terminals.	null

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

Section	Parameter	Description	Default Value
UtOdbc[b, c]	dataSourceName	Data source name (DSN) of the ODBC-compliant database.	mvamUser (ODBC) ipvoice (AllBill)
UtOdbc[b, c]	password	Login password for the ODBC-compliant database.	NULL
UtOdbc[b, c]	phoneAliasColumnName	Name of the column containing the Telephone Alias field.	phoneAlias (ODBC) Phonealias (AllBill)
UtOdbc[b, c]	phoneNumColumnName	Name of the column containing the Telephone Number field.	phoneNum (ODBC) Phonenum (AllBill)
UtOdbc[b, c]	pinColumnName	Name of the column containing the PIN field.	pin (ODBC) Pinnum (AllBill)
UtOdbc[c]	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 (default)	No
UtOdbc[b, c]	tableName	Name of the table in the ODBC-compliant database.	mvamUser (ODBC) ipvoice (AllBill)
UtOdbc[b, c]	userAliasColumnName	Name of the column containing the User Alias field.	userAlias (ODBC) Accessno (AllBill)

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

Section	Parameter	Description	Default Value
UtOdbc[b, c]	userName	Login user name for the ODBC-compliant database.	NULL
UtOdbc[b, c]	userNameColumnName	Name of the column containing the User Name field.	userName (ODBC) Ipname (AllBill)
UtOdbc[c]	zoneColumnName	Name of virtual zone associated with user.	zone (ODBC) Zonename (AllBill)
UtText	capacity	Maximum number of records allowed in the user database. Valid entries are 1 through 1,000.	1000
UtText[a]	file	Identifies the path and filename of the user database.	c:\mvam\db\user.txt (WinNT) /opt/mvam/db/user.txt (Solaris, HP-UX)
Zt	capacity	Defines the number of slots available in the zone table.	25
Zt	file	Identifies the path and filename of the Virtual Zone database.	c:\mvam\db\zone.txt (WinNT) /opt/mvam/db/zone.txt (Solaris, HP-UX)
Zt	rootForZones	Identifies the default root directory for all virtual zone databases.	c:\mvam\allzones\ (WinNt) /opt/mvam/allzones/ (Solaris, HP-UX)

a. These parameters are configured through the MVAM installation program.

b. Not all PC telephony software provides this information. By ignoring these requests, the MVAM relies on the MultiVoice Gateway to provide call change state messages, allowing consistent processing of calls to and from PC clients.

c. ODBC database support is currently available only for MVAM running on a Windows NT system. These parameters are not configured for MVAM running on Solaris or HP-UX systems.

MVAM Licenses

B

MultiVoice Access Manager (MVAM) provides per-port licensing implemented by serial numbers. A MultiVoice Access Manager serial number is included with MVAM Release 3.0.0 software and is required for installation. License Packs, implemented by upgrade serial numbers, allow you to increase the number of ports supported on your Windows NT, SPARC Solaris, or HP-UX system.

Per-port licensing

MVAM licensing is provided on a per-port basis. The number of ports, or number of calls an endpoint can handle, vary per endpoint (Gateway or PC terminal). For example, a gateway may have 96 ports (possibly more or less depending on the type of gateway), whereas a PC terminal has only one port.

MVAM allows Gateway and terminal registration as long as the total number of ports for all registered endpoints, is less than or equal to the number of ports supported by the MultiVoice Access Manager license.

For example, if an MVAM installation supports 400 ports, a combination of four Gateways each with 96 ports and sixteen terminals could register simultaneously with that MVAM installation.

MultiVoice Access Manager serial numbers

A standard MVAM license is implemented by a serial number included with the MultiVoice Access Manager Release 3.0.0 software and located on the product packaging as well as on the Warranty Registration Card. The serial number provided is required when installing MVAM Release 3.0.0. This software, MVAM Release 3.0.0, will not run without a valid serial number.

The serial number included with the software is valid only on the platform (Windows NT, SPARC Solaris, or HP-UX) with which it was provided. This MultiVoice Access Manager serial number supports the following number of ports, depending on the platform:

Hardware Platform	Ports Supported
Windows NT	400
SPARC Solaris	3000
HP-UX	3000

Serial numbers can be upgraded to support more ports by adding one or more upgrade serial numbers which are included with each License Pack.

License Packs/Upgrade serial numbers

License Packs are used to increase the number of ports supported by a MVAM license on an existing MVAM Release 3.0.0 installation. License Packs are available in several port quantities and implemented by upgrade serial numbers. An upgrade serial numbers is included with each License Pack. A maximum of 20 upgrade serial numbers can be added to an MVAM installation.

Upgrade serial numbers are located on the packaging of the License Pack, as well as on the Warranty Registration Card provided in the packaging. These serial numbers are added to and removed from an MVAM installation through web-based administration while the MVAM is running. These upgrade serial numbers can only be used with an existing MVAM Release 3.0.0 installation that has a MultiVoice Access Manager serial number already in use.

Upgrade serial numbers are platform independent and available in the following quantities:

- 1,000 port licenses
- 5,000 port licenses
- 10,000 port licenses

- 20,000 port licenses

Note: We recommend that no more than 30,000 ports be configured on a single MVAM.

During the MultiVoice Access Manager installation process, the MultiVoice License Installer is installed on your Windows NT, Solaris, or HP-UX system. This utility is used to increase the number of ports your MVAM installation supports.

Before you upgrade a MultiVoice Access Manger license, make sure that you have the upgrade serial number for the License Pack purchased. See

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

Window NT license installation

The MVAM License Installer displays a single data entry window, where users will enter updated license information.

1 From the Start Menu, select MVAM License Installer.

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 MultiVoice Access Manager serial number printed on the MVAM Warranty Registration card.

4 Click the Install button. (Be patient. This operation may take a minute.) The MVAM License Installer should display a message similar to the following:



Click OK. The MultiVoice Access Manager license is installed.

Solaris and HP-UX license installation

The Solaris and HP-UX license utility for MultiVoice Access Manager is located in the `bin` subdirectory of the MVAM top level directory. This script is run from the shell prompt.

Note: The `mvam_license.sh` script should be executed by the MVAM user specified at installation.

To perform the installation, use the following procedure:

1 At the shell prompt, execute `mvam_license.sh`

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

2 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.sh` updates MVAM with the new User name. Press Return to continue.

3 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, `mvam_license.sh` updates the MVAM with the new Organization name. Press Return to continue.

4 Enter the serial number that appears on the MVAM Warranty Registration card:

`Serial number:`**`MVAM-300-BX-00000000`**

5 Press Return to continue. `mvam_license.sh` continues, displaying the following message:

`Please Wait...`

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

`MVAM license installed successfully.`

Gatekeeper-to-gatekeeper communications and MVAM licenses

If two installations of MVAM (peer Gatekeepers) work with each other (see "Gatekeeper-to-Gatekeeper communications" in Chapter 6, "Peer Gatekeeper Administration"), each will need its own MultiVoice Access Manager serial number and upgrade serial numbers. If the same serial number has been used in two MVAM installations, communication between those two gatekeepers will fail. Error messages reflecting the use of duplicate serial numbers will be recorded in the event log.

Legal Notices

C

This appendix provides the End User License Agreement as well as the Warranty for the MultiVoice Access Manager software.

End User License Agreement

The following states the End User License Agreement between Ascend Communications, Inc., including its parent and subsidiary companies (“Ascend”) and end user.

ASCEND COMMUNICATIONS, INC. (“ASCEND”) IS WILLING TO LICENSE THE ENCLOSED SOFTWARE AND ACCOMPANYING USER DOCUMENTATION (COLLECTIVELY, THE “PROGRAM”) TO YOU ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. PLEASE READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE INSTALLING THE PROGRAM, AND BEFORE USING THE ACCOMPANYING USER DOCUMENTATION. INSTALLING THE PROGRAM WILL INDICATE YOUR ACCEPTANCE OF THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT, ASCEND IS UNWILLING TO LICENSE THE PROGRAM TO YOU, IN WHICH EVENT YOU SHOULD RETURN THE PROGRAM WITHIN TEN (10) DAYS FROM SHIPMENT TO THE PLACE FROM WHICH IT WAS ACQUIRED, AND YOUR LICENSE FEE WILL BE REFUNDED. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AGREEMENT CONCERNING THE PROGRAM BETWEEN YOU AND ASCEND, AND IT SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION OR UNDERSTANDING BETWEEN THE PARTIES.

License

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, (c) 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, NON-INFRINGEMENT 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, ITS PARENT OR SUBSIDIARY COMPANIES 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 New York as applied to transactions taking place wholly within New York between New York 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., a wholly-owned subsidiary of Lucent Technologies, One Ascend Plaza, 1701 Harbor Bay Parkway, Alameda, CA 94502.

Lucent Technologies InterNetworking Systems Global Warranty

Unless otherwise stated in the product purchase agreement between you and Lucent, Lucent warrants that during the warranty period the Products will operate in accordance with Lucent's standard published documentation accompanying

the Product. If a Product does not operate in accordance therewith during the warranty period, you must promptly notify Lucent. Lucent, at its option, will either repair or replace the Product without charge. You have the right, as your exclusive remedy, to return the Product for a refund of the purchase price or license fee if Lucent is unable to repair or replace it. The warranty period is twelve (12) months for hardware, ninety (90) days for software and thirty (30) days for media. The warranty period shall begin on the shipping date for Customer-installed Products or on the installation date for Lucent-installed Products.

Support Services Available during Warranty Period

- 90-day advance replacement of field replaceable units, remaining 9 months of service will be field replaceable unit return to factory process.
- 90-day, 7 X 24 access to eSight Live, providing diagnostic support via private chat with a Lucent technician.
- 90-day, 7 X 24 access to software maintenance releases for products that have remote download capabilities.
- 12-month, 7 X 24 access to enabling self-help.
- 12-month, 7 X 24 access to extensive technical database providing product information, frequently asked questions and technical advice through the WEB page providing self help information.
- 12-month, 7 X 24 access to International Return Materials Authorization Policy (RMA), including forms & RMA number issuance.

How to register your products to obtain Warranty Services

1. Write down the product name, serial number and product code of the chassis or base unit for each product purchased.
2. Check to see if someone has been designated to register all products and provide them with this information.
3. Or using this information, register at Lucent's eSight™ Service Center at **http://netcare-esight.com**. Select "Log In/Register" from the home page,

then select “Warranty Registration.” (If you already have a login ID to the site, go to “My NetCare” and choose “Register Products Under Warranty”).

Note: For your convenience, only one person needs to register products for warranty. This person will then receive a Warranty confirmation number that can be used by others to request a login for access to the same information (individual logins are required to access the NetCare eSight Service Center). This Warranty number will encompass all products registered, and all associated users will be updated to include new serial numbers that are registered at a later date by anyone associated with that number. We strongly encourage customers to follow this process for their convenience.

The NetCare® Global Sales Helpdesk is available to answer your questions on this and any other sales-related issue. Call 1800 4NETCARE within the U.S. and (727) 217-2303 outside the U.S., or contact the Helpdesk via e-mail at netcarehelp@lucent.com.

Index

Numerics

2nd GK IP parameter, 10-2, 11-6
800 service, example, 1-24
800 service, local, 1-23

A

Access Manager
  definition, 1-5
ACD, 1-24
Act parameter, A-8
ADMA, 5-2
  ANI authentication, 5-7
  API authentication, 5-8
  gateway/trunk rules, 5-2, 5-24, 5-27
    defining, 5-27
  PIN Authentication, 5-8
  rule sets, 5-3
    defining, 5-17
  rules, 5-3
    defining, 5-7
ADMA rule sets, 5-15
ADMA rules, 5-6
ageGatewayRegistration parameter, A-4
ageTerminalRegistration parameter, A-4
Alias Dialing field, 3-27
aliasPrefix parameter, A-14
AllBill database setup type, 3-3
AllBill user database, 2-12, 9-1
allowPcToPhone parameter, A-16
allowPhoneToPc parameter, A-16
allowTerminalsToRegister parameter, A-16
amv_gk_table, file definition, 2-27
ANI, 3-10
  ANI Required check box, 3-11
  authentication, 11-2, 11-6
    behind PBXs, 3-16
    behind WANs, 3-16
    check box, 11-2
    configure, 3-13
    in ADMA rules, 5-3
    with PIN, 3-16
aniRequired parameter, A-16
announcements, 5-8
API configuration file, 2-27
architecture
  packet-switched, 1-2
Audio Codecs
  G.711, 1-4
  G.723.1, 1-4
  G.728, 1-4
  G.729(A), 1-4
  RT-24, 1-4
Automatic Call Distributor (ACD), 1-24
Automatic Number Identifier (ANI), 3-10

B

bin subdirectory, 2-26
browser software, supported, 2-3
busy signals, and non-ISDN signalling, 3-12

C

call establishment
  troubleshooting, 11-11, 11-14
call log files, 10-16
  incomplete call record, 10-22
  start call record, 10-17
  stop call record, 10-20
call logs, 3-25
call process
  MultiVoice network, 1-5
    using a secondary Gatekeeper, 1-7
    using overlapping coverage areas, 1-13
call record
  call record file creation frequency field, 3-25
  calls.txt file, 10-16
  file creation, 10-16
call record files subdirectory, 2-26
call status
  monitoring, 10-7
Calling Line ID (CLID), 3-10, 3-11, 11-2, 11-6
calls subdirectory, 2-26
calls.txt file, 10-16
capacity parameter, A-2, A-6, A-13, A-20
CD-ROM, MVAM, 2-1
CGI. *See* Common Gateway Interface
cgi-bin subdirectory, 2-5, 2-26
check box
  ANI required, 3-11
  PIN required, 3-10
  to the left of any field, 4-3, 5-5, 5-16, 5-26, 6-4, 8-4, 9-3, 10-27
circuit-switched technology, 1-1
CLEC. *See* Competitive Local Exchange Carrier
Common Gateway Interface (CGI), 2-4, 2-26
Competitive Local Exchange Carrier, 1-22
configFileparameter, A-4
Configure
  PC-to-phone operation
    Allow Terminals to Call Gateways, 3-10
coverage area, 11-2
Coverage areas
  definition, 1-6
coverage areas
  configuration, 4-19
  gatekeeper, 6-8
  gateway, 4-18
  inclusion areas, 4-19, 6-8
  overlapping, 4-19

D

database subdirectory, 2-26
databases
  Gatekeeper, 6-6, 6-7
  Gatekeeper Coverage Area, 6-6, 6-8
  Gatekeeper Virtual Zone, 3-30
  Gateway, 4-5, 4-8, 4-11
  Gateway Coverage Area, 4-21, 4-24
  Gateway/Trunk Rules, 5-2
  Number Translation, 8-7
  Rule Sets, 5-3
  Rules, 5-3
  User, 9-5
dataSourceName parameter, A-19
db subdirectory, 2-26
debugPrinting parameter, A-12, A-13, A-20
Definitions
  amv_gk_table, 2-27
  bin directory, 2-26
  calls directory, 2-26

cgi-bin directory, 2-26
db directory, 2-26
events directory, 2-26
htdocs directory (Solaris, HP-UX), 2-26
MVAM initialization file, 2-27
mvam.dat, 2-27
webpages directory (NT), 2-26
destination phone numbers
determining, 4-18
dial mode, 5-8
dual-stage, 5-3
single-stage, 5-3
dialing prefix
configuration, 3-26
configuration screen, 3-27
default, 3-28
displayCapacity parameter, A-6, A-13
displayPinInEventLog parameter, A-16
DNIS prefix, 5-3, 5-6, 5-7, 5-11
dropsCallOnExpiredGateways parameter, A-5
dual-stage dialing, 5-3

E

E.164 address
terminals, 7-1
Egress Number Translation Table
definition, 4-15
egress translation table, 8-4
enabled parameter, A-2
Ept parameter, A-8
Event File Options screen, 3-18
event log, 11-11
displaying, 11-12
event logs, 10-14
events subdirectory, 2-26
executable file subdirectory, 2-26

F

file parameter, A-5, A-6, A-7, A-13, A-18, A-20
filePath parameter, A-2, A-3
forceDialStringInAcfNonStd parameter, 3-17, A-14, A-15
frequency parameter, A-3, A-5

G

G.711 codec, 1-4
G.723.1 codec, 1-4
G.728 codec, 1-4
G.729(A) codec, 1-4
Gatekeeper, 1-5
gatekeeper, 1-5, 6-8
coverage areas, 6-8
inclusion area, 6-13, 6-16
IP address, 6-4, 6-7
virtual zone, 6-7
gatekeeper coverage area, 6-6
Gatekeeper database, 6-6, 6-7
gatekeeper identifier, 6-4, 6-7
Gatekeeper registration parameters
gatekeeper-ip-sec, 1-12
gatekeeper-keepalive, 1-12
primary-retries, 1-13
registration-retries, 1-13
registration-retry-timer, 1-13
gatekeeper virtual zone, 1-19
call processing, 1-19
definition, 1-19
Gatekeeper Virtual Zone database, 3-30
gatekeeper-ip-sec parameter, 1-11, 1-12
gatekeeper-keepalive parameter, 1-12
Gateway
coverage areas
configuration, 4-19

inclusion areas, 4-19
overlapping, 4-19
database, 4-5, 4-8, 4-11
Gateway Locator feature, 10-9
number translation table, 4-12
Gateway Administration screen, 4-2
Gateway Coverage Area
database, 4-24
Gateway Coverage Area database, 4-21
gateway coverage areas, 4-18
Gateway database, 4-5
Gateway Name field, 5-27, 10-6
Gateway/Trunk Rules, 5-24
Gateway/Trunk Rules database, 5-2
gateways, 1-5
Gen parameter, A-8
GK IP Adrs parameter, 11-1
Gk parameter, A-10
Gkcp parameter, A-8
Gkct parameter, A-9
Gkt parameter, A-9
Gwct parameter, A-9
Gwt parameter, A-9

H

H.323, 1-2
gatekeeper, 1-5
gateways, 1-5
implementation, 1-5
International Telecommunications Union Telephone Recommendation, 1-28
terminal
compliant terminals, 1-27
H.323 compliant terminal, 1-27
H.323 Id
terminals, 7-1
help, online, 3-4, 4-3, 5-5, 5-16, 5-26, 6-4, 8-4, 9-2, 10-27
HP-UX
license installation, B-4
license installer script, B-4, B-5
MVAM installation, 2-22
MVAM startup, 2-30
stopping MVAM, 2-32
System Requirements, 2-3
uninstalling the MVAM, 2-35
Web servers, 2-4
HTML files subdirectory, 2-26

I

ignoreTerminalBrqs parameter, A-17
ignoreTerminalDrqs parameter, A-17
IIS. *See* Microsoft's Internet Information Server
Imatix, 2-4
Web site, 2-4
inclusion area
gatekeeper, 6-13, 6-16
Inclusion areas
definition, 1-6
inclusion areas, 1-13, 4-19, 6-8, 10-9
inclusionListCapacity parameter, A-7
inclusionListDisplayCapacity parameter, A-6
incomplete call record, 10-22
Ingress Number Translation Table
definition, 4-15
ingress translation table, 8-4
installation
Windows NT, 2-6
interface screen, MVAM, 11-24
International Telecommunications Union, 1-2
International Telecommunications Union (ITU), 7-1
Internet Information Server, 2-4
Internet Service Provider, 1-22
IP Device Control IPDC

IPDC
definition
IP-network congestion, 11-6
IP-networking software, 2-3
ISP. *See* Internet Service Provider
ITU-T. *See* International Telecommunications Union

K

Keepalive Timer parameter, 3-24, 11-6, 11-7

L

License installation
HP-UX, 2-24, B-4
Solaris, 2-20, B-4
Windows NT, 2-13, B-3
License Packs, B-2
quantities, 10-33, B-2
upgrade serial numbers, B-2
adding, 10-27
removing, 10-30
Licenses, 2-4
and GK-to-GK communications, B-2
MVAM License Application (Windows NT), B-3
mvam_license.sh script (Solaris, HP-UX), B-4, B-5
listCapacity parameter, A-6
local 800 service, 1-23
log files subdirectory, 2-26
long-distance service
basic public, 1-22

M

manual, MVAM, 2-1
maxRoutableCapacity parameter, A-7
maxSimulLrq parameter, A-15
Microsoft's Internet Information Server (IIS), 2-4
Microsoft's Open Database Connectivity, 2-12
Microsoft's Personal Web Server, 2-4
MinE164Size parameter, A-18
MLG gateway parameter, 5-2
MLG. *See* Multiple Logical Gateways
Modifying Dialing Prefixes screen, 3-27
modifying user PINs, 9-10
msgfile parameter, A-18
Multiple Logical Gateways (MLG), 5-1
MultiVoice Access Manager (MVAM)
definition, 1-5
MultiVoice Access Manager *See* MVAM
MultiVoice applications
Basic public long-distance service, 1-22
Local 800 service, 1-23
PBX trunk intraflow, 1-26
Point-to-point PBX trunk extension, 1-25
MultiVoice Gateway
2nd GK IP, 10-2
Name parameter, 10-2
overlapping coverage areas, 1-13
registered Gateways, 3-23
registration, 3-23
troubleshooting, 11-1
MultiVoice Gateway for the MAX—User's Guide, 4-12, 11-3, 11-7
MultiVoice Gateway registration
keep-alive registration, 1-11, 3-23
registration policy, 1-12
re-registration policy, 1-12
troublshooting, 11-11, 11-13
MultiVoice Gateways
identical naming of, 11-10
MultiVoice network
coverage areas, 1-6

H.323 implementation, 1-5
inclusion areas, 1-6
overlapping coverage areas, 1-13
step-by-step call process, 1-5
step-by-step call processing
overlapping coverage areas, 1-13
secondary gatekeeper, 1-7
using a secondary MVAM, 1-7
multi-zone call routing, 6-6
MVAM
accessing, 3-1
cgi-bin directory
Windows NT, 2-5
configuration files, 2-27
control files, 2-27
directory structure, 2-26
Gatekeeper application
troubleshooting, 11-9
initialization file, A-1
definition, 2-27
parameters
Act, A-8
ageGatewayRegistration, A-4
ageTerminalRegistration, A-4
aliasPrefix, A-14
allowPcToPhone, A-16
allowPhoneToPc, A-16
allowTerminalsToRegister, A-16
aniRequired, A-16
capacity, A-2, A-6, A-13, A-20
configFile, A-4
dataSourceName, A-19
debugPrinting, A-12, A-13, A-20
displayCapacity, A-6, A-13
displayPinInEventLog, A-16
dropsCallOnExpiredGateways, A-5
enabled, A-2
Ept, A-8
file, A-5, A-6, A-7, A-13, A-18, A-20
filePath, A-2, A-3
forceDialStringInAcfNonStd, A-14, A-15
frequency, A-3, A-5
Gen, A-8
Gk, A-10
Gkcp, A-8
Gkct, A-9
Gkt, A-9
Gwct, A-9
Gwt, A-9
ignoreTerminalBrqs, A-17
ignoreTerminalDrqs, A-17
inclusionListCapacity, A-7
inclusionListDisplayCapacity, A-6
listCapacity, A-6
maxRoutableCapacity, A-7
maxSimulLrq, A-15
MinE164Size, A-18
msgfile, A-18
name, A-4
nxtCapacity, A-13
nxtIn, A-18
Nxtl, A-10
nxtPath, A-14
Odbc, A-10
passThruPrefix, A-14
password, A-19
phoneAliasColumnName, A-19
phoneNumColumnName, A-19
pinColumnName, A-19
pinSize, A-17
Prefixer, A-10
prompt, A-19
proxyPinRequired, A-17
Ras, A-11
registrationPeriodMargin, A-5
Router, A-11
RoutingAlgorithm, A-7
rules, A-3
ruleSets, A-3
Sec, A-11
size, A-5, A-15

synchronous, A-15
table, A-3
tableName, A-19
Translator, A-11
Tt, A-12
useArqToStart, A-15
userAliasColumnName, A-19
userName, A-20
userNameColumnName, A-20
UtOdbc, A-12
UtText, A-12
webPagePath, A-5
zoneNameColumnName, A-20
sections
Act, A-2
Adma, A-3
AliasAni, A-4
Api, A-4
CallLog, A-4
Ept, A-4
EventLog, A-5
Gkcp, A-5
Gkct, A-6
Gkt, A-6
Gwct, A-6
GwRouting, A-7
Gwt, A-7
insertIntoWin, A-8
Mvam, A-12
Nxtl, A-13
Prefixer, A-14
Ras, A-14
RtEventLog, A-15
Sec, A-16
supserve, A-18
Tt, A-18
UtOdbc, A-19
UtText, A-20
Zt, A-20
installation
HP-UX, 2-22
Solaris, 2-16
Windows NT, 2-27
installing a Webserver, 2-5
installing the, 2-4
installing, before, 2-6
keep-alive registration, 1-11, 3-23
launching (HP-UX), 2-30
launching (NT), 2-27
launching (Solaris), 2-29
License, 2-4
Main Menu
Options, 3-5
Menu
Control buttons, 3-5
Main
default, 3-2
virtual zones, 3-3
On-line help, 3-4
network requirements, 2-3
opening the user interface, 2-31
registration policy, 1-12
re-registration policy, 1-12
security
user access, 2-6
stopping
HP-UX, 2-32
Solaris, 2-32
Windows NT, 2-32
System requirements, 2-2
HP-UX, 2-3
SPARC Solaris, 2-2
Windows NT, 2-2
uninstalling
Windows NT, 2-33
uninstalling from
HP-UX, 2-35
Solaris, 2-34
Windows NT, 2-33
URL, 2-32
user database management tools
AllBill user database, 2-12
ODBC user database, 2-12
text file user database, 2-12

user interface
Call accounting options screen, 3-25
Display call logs, 3-25
Display event logs, 10-14
Display the status of all active calls, 10-7
Display the status of all administered Gateways, 10-5
Gateway Status screen, 10-4
MVAM Interface screen, 11-24
remote startup, 3-2
startup, 3-1
startup from 127.n.n.n, 3-1, 3-2
startup from localhost, 3-1, 3-2
startupusing host IP address, 3-2
URL, 2-32
verifying successful loading of, 2-28, 2-30, 2-31
version, 2-28, 2-30, 2-31
Web browsers
Microsoft's Internet Explorer, 2-3
Netscape Navigator, 2-3
web browsers, 2-3
webpages directory
Windows NT, 2-5
MVAM initialization file, A-1
MVAM license application, B-3, B-4, B-5
mvam.dat, file definition, 2-27

N

Name parameter, 10-2, 11-2
name parameter, A-4
network congestion, 11-6
Network Requirements, 2-3
networking software, required, 2-3
non-ISDN signalling, and busy signals, 3-12
number translation
inbound, 8-19
Number Translation database, 8-7
number translation replace string, 8-9
number translation rules, 4-17
number translation search string, 8-8
number translation table, 8-4, 8-7
removing active tables, 8-15
number translation tables
egress, 4-15, 8-4
Gateway, 4-12
ingress, 4-15, 8-4
translation rules, 4-17
nxtCapacity parameter, A-13
nxtIn parameter, A-18
Nxtl parameter, A-10
nxtPath parameter, A-14

O

Odbc parameter, A-10
ODBC user database, 2-12, 9-1
ODBC. *See* Microsoft's Open Database Connectivity
online help, 3-4, 4-3, 5-5, 5-16, 5-26, 6-4, 8-4, 9-2, 10-27
Open DataBase Connectivity, 2-12
Options form, 3-5
Options menu
call accounting, 3-7
dialing prefixes, 3-7
event file, 3-7
msicellaneous, 3-8
registration, 3-7
security, 3-7
overlapping coverage area, 1-13
overlapping coverage areas, 1-13, 4-19
call processing, 1-13

P

packet-switched architecture, 1-2

Pass-Thru Dialing field, 3-27
passThruPrefix parameter, A-14
password parameter, A-19
PBX, 1-24
PBX trunk extension, point-to-point, 1-25
PC terminals, 7-1
PC-to-phone
  authentication, 3-11
per-port licensing, 2-4, B-1
  ports supported, 10-33, B-2
Personal Identification Number (PIN), 9-6
Personal Identification Number *See also* PIN
phone numbers
  carrier assigning of, 4-8
  matching, 4-19
phoneAliasColumnName parameter, A-19
phoneNumColumnName parameter, A-19
PIN, 3-12
  authentication
    check box, 11-2
    configure, 3-12
    in ADMA rules, 5-3
    with ANI, 3-16
  creation, 3-13
  modifying, 9-10
  PIN Required check box, 3-10
  prompting, 9-5
  using, 3-8
pinColumnName parameter, A-19
pinSize parameter, A-17
pkgrm command, 2-34
Pkt Audio Mode parameter, 11-1
Point of Presence (PoP), 1-22
point-to-point PBX trunk extension, 1-25
PoP. *See* Point of Presence
pound sign, 3-12, 3-13
Prefixer parameter, A-10
Pri GK Retries parameter, 11-6
primary-retries parameter, 1-13
Private Branch Exchange, 1-24
prompt parameter, A-19
proxyPinRequired parameter, A-17
PSTN
  example of, 1-1
PSTN. *See* Public Switched Telephone Network
public long-distance service
  basic, 1-22
Public Switched Telephone Network, 1-1
publications, related, xxvii

Q

QoS. *See* Quality of Service
Quality of Service (QoS), 1-22

R

RAS, 1-28
Ras parameter, A-11
real-time information, displaying, 11-25
Reg Retry parameter, 11-7
Reg Retry Timer parameter, 11-6
registration
  troubleshooting, 11-11, 11-13
Registration Confirmation, 11-10
Registration Options screen, 3-20, 3-22, 3-23, 3-24, 3-25
Registration Request, 11-10
Registration Request packet, 11-7
Registration, Admission and Status signaling. *See* RAS
registrationDuration parameter, 1-12, 11-7
registrationPeriodMargin parameter, A-5
registration-retries parameter, 1-13
registration-retry-timer parameter, 1-13

related publications, xxvii
Router parameter, A-11
RoutingAlgorithm parameter, A-7
RT-24 codec, 1-4
Rule Set Name, 5-28
Rule Sets database, 5-3
Rules database, 5-3
rules parameter, A-3
ruleSets parameter, A-3

S

Sec parameter, A-11
secondary MVAM, 1-7
security
  configuring PIN, 3-8
  MVAM, 9-6
  restricting access to MVAM, 2-6
Security Options
  Allow Gateways to Call Terminals, 3-10
  Allow Terminals to Call Gateways, 3-10
  Require ANI from Gateways, 3-9
  Require PINs from Gateways, 3-9
  Security Options form, 3-8
Security Options form, 3-8
Security Options screen, 3-10, 3-11, 3-17, 3-19
serial number, 2-14, 2-16, 2-22
serial number, MVAM, 2-1
serial numbers, B-1
servers, Web, 2-3
single-dial enable gateway parameter, 5-2
single-stage dialing, 5-3
size parameter, A-5, A-15
Solaris
  license installation, B-4
  license installer script, B-4, B-5
  MVAM installation, 2-16
  MVAM startup, 2-29
  stopping MVAM, 2-32
  System Requirements, 2-2
  uninstalling the MVAM, 2-34
  Web servers, 2-4
SPARC Solaris
  System Requirements, 2-2
SPARC Solaris. *See* Solaris
start call record, 10-17
Starting, 2-25
status
  call log, 3-25
  event log, 10-14
  monitoring call, 10-7
stop call record, 10-20
Submit button, 4-3, 5-5, 5-16, 5-26, 6-4, 8-4, 9-3, 10-27
synchronous parameter, A-15
System, 2-2
system requirements, 2-2

T

table parameter, A-3
tableName parameter, A-19
TCP/IP, 2-3
Telephone Alias field, 9-6
Telephone number field, 9-6
telephone numbers
  carrier assigning of, 4-8
  matching, 4-19
terminal
  status, 10-7
terminal ingress translation table, 8-19
terminal name, 7-4
terminal phone number, 7-4
terminals
  E.164 address, 7-1
  H.323 Id, 7-1
text file user database, 2-12

tick-tock sound, 3-12, 11-6
translation rules, 8-9
  removing, 8-14
  re-ordering, 8-14
translation table
  terminal ingress, 8-19
Translator parameter, A-11
Trunk ID, 5-28
Tt parameter, A-12

U

upgrade serial numbers, B-2
upgrading MVAM, 2-34
  HP-UX, 2-35
  Solaris, 2-34
useArqToStart parameter, 3-17, 3-18, A-15
User Administration screen, 9-1
User database, 9-5
User interface
  display call logs, 3-25
  display event logs, 10-14
  display the status of all active calls, 10-7
  display the status of all administered Gateways, 10-5
  Gateway call accounting options screen, 3-25
  Gateway status, 10-4
  MVAM Interface screen, 11-24
  remote startup, 3-2
  startup, 2-31, 3-1
  startup from 127.n.n.n, 3-1, 3-2
  startup from localhost, 3-1, 3-2
  startup using host IP address, 3-2
userAliasColumnName parameter, A-19
userName parameter, A-20
userNameColumnName parameter, A-20
UtOdbc parameter, A-12
UtText parameter, A-12

V

version, 2-28, 2-30, 2-31
virtual zone
  zone-specific database, 3-30
Virtual zones
  main menu, 3-3
Voice over IP networks, 1-5
VoIP networks. *See* Voice over IP networks *and* MultiVoice network
VOIP Options menu, 3-24, 10-2, 11-2
VOIP Options menu item, 11-9
VPN Mode, 3-13
VPN mode gateway parameter, 5-2
VPN Mode option, 11-2
VPN Mode parameter, 11-1

W

Web browser
  troubleshooting, 11-8
Web browser access, 3-1
Web browser software, supported, 2-3
Web browsers, 2-3
  Microsoft's Internet Explore, 2-3
  Netscape Navigator, 2-3
Web servers
  supported, 2-3
    HP-UX, 2-4
    Solaris, 2-4
    Windows NT, 2-4
webPagePath parameter, A-5
webpages subdirectory, 2-5, 2-26
Wildcard searches, 10-6
Windows NT
  installing MVAM, 2-6
  license installation, B-3
  license installer screen, B-3
  MVAM cgi-bin directory, 2-5

MVAM installation, 2-27
MVAM startup, 2-27
MVAM webpages directory, 2-5
stopping MVAM, 2-32
System requirements, 2-2
uninstalling MVAM, 2-33
uninstalling the MVAM, 2-33
Web servers, 2-4
World Wide Web sites, related, xxvii
WWW sites, related, xxvii

X

Xitami Webserver, 2-4

Z

zoneNameColumnName parameter, A-20