Wave
Global Administrator Guide

Last Updated 9/7/07

Vertical Communications, Inc. Software License Agreement

NOTICE: Please carefully read this Software License Agreement (this "Agreement") before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which, along with associated media, printed materials and "online" or electronic documentation, is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH Vertical Communications WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price. Written approval is NOT a prerequisite to the validity or enforceability of this Agreement and no solicitation of any such written approval by or on behalf of Vertical Communications shall be construed as an inference to the contrary.
You have acquired a device ("DEVICE") which includes Software licensed by Vertical from one or more software licensors ("Vertical's Software Suppliers"). Such Software products are protected by international intellectual property laws and treaties. The Software is licensed, not sold.

IF YOU DO NOT AGREE TO THIS SOFTWARE LICENSE AGREEMENT, DO NOT USE THE DEVICE OR COPY THE SOFTWARE. INSTEAD, PROMPTLY CONTACT VERTICAL FOR INSTRUCTIONS ON RETURN OF THE UNUSED DEVICE(S) FOR A REFUND. ANY USE OF THE SOFTWARE, INCLUDING BUT NOT LIMITED TO USE ON THE DEVICE, WILL CONSTITUTE YOUR AGREEMENT TO THIS SOFTWARE LICENSE AGREEMENT (OR RATIFICATION OF ANY PREVIOUS CONSENT).

License Grant. Vertical Communications, Inc. ("Vertical") grants the end-user of the Software ("Licensee") a personal, nonsublicensable, nonexclusive, nontransferable license (the "License"): a) to use the Software only on the DEVICE or, if applicable, on a single computer identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the documentation related to the Software solely in support of authorized use of the Software by Licensee. The License applies to the Software only and does not extend to other Vertical software or hardware products. Licensee has no right to receive any source code or design documentation relating to the Software. Licensee may permanently transfer rights under this Software License only as part of a permanent sale or transfer of the Device, and only if the recipient agrees to the Software License Agreement. If the Software is an upgrade, any transfer must also include all prior versions of the Software.

The Software is not fault tolerant. Vertical has independently determined how to use the software in the DEVICE, and Vertical's Software Suppliers have relied upon Vertical to conduct sufficient testing to determine that the software is suitable for such use.

Note on Java Support. The Software may contain support for programs written in Java. Java technology is not fault tolerant and is not designed, manufactured, or intended for use or resale as online control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or

weapons systems, in which the failure of Java technology could lead directly to death, personal injury, or severe physical or environmental damage. Sun Microsystems, Inc., has contractually obligated Vertical's Software Suppliers to make this disclaimer.

Restrictions on Use; Reservation of Rights. The Software and related documentation are protected under copyright laws. Vertical and/or Vertical's Software Suppliers retain all title and ownership in both the Software and related documentation, including any revisions made by Vertical. The copyright notice must be reproduced and included with any copy of any portion of the Software or related documentation. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, or reverse engineer the Software or related documentation or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or related documentation, in whole or in part. The Software and related documentation embody Vertical's confidential and proprietary intellectual property. Licensee shall not disclose to any third party the Software, or any information about the operation, design, performance or implementation of the Software and related documentation which is confidential to Vertical.

Export Restrictions. Licensee acknowledges that Software is of U.S. origin. Licensee agrees to comply with all applicable international and national laws that apply to the Software, including the U.S. Export Administration Regulations, as well as end-user, end-use and country destination restrictions issued by U.S. and other governments.

Limited Media Warranty. Vertical warrants that any media on which the Software is recorded will be free from defects in materials and workmanship under normal use for a period of 90 days from the date the program is shipped to reseller. If a defect in any such media should occur during this 90-day period, the media may be returned to Vertical and Vertical will replace the media without charge. Vertical shall have no responsibility to replace media if the failure of the media results from accident, abuse or misapplication of the media.

EXCEPT AS PROVIDED ABOVE, THE SOFTWARE IS PROVIDED "AS IS" AND VERTICAL AND VERTICAL'S SOFTWARE SUPPLIERS MAKE NO WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO THE SOFWARE AND DOCUMENTATION. VERTICAL AND VERTICAL'S SOFTWARE SUPPLIERS DISCLAIM ALL OTHER WARRANTIES, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OR MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. FURTHER, VERTICAL DOES NOT WARRANT, GUARANTEE, OR MAKE ANY REPRESENTAIONS REGARDING THE USE, OR THE RESULTS OF THE USE, OF THE SOFTWARE OR RELATED WRITTEN DOCUMENTATION IN TERMS OF CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE.

Limitation of Liability. IN NO EVENT SHALL VERTICAL BE LIABLE TO LICENSEE OR ANY THIRD PARTY FOR (A) ANY MATTER BEYOND ITS REASONABLE CONTROL OR (B) ANY CONSEQUENTIAL, SPECIAL, INDIRECT OR INCIDENTAL DAMAGES ARISING OUT OF THIS LICENSE OR USE OF THE SOFTWARE, EVEN IF VERTICAL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. VERTICAL WILL NOT BE LIABLE FOR THE LOSS OF, OR DAMAGE TO, YOUR RECORDS OF DATA, THE RECORDS OF DATA OF ANY THIRD PARTY, OR ANY DAMAGES CLAIMED BY YOU BASED ON A THIRD PARTY CLAIM. IN NO EVENT SHALL THE LIABILITY OF VERTICAL RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO VERTICAL FOR THE LICENSE. ALTHOUGH IBM XML PARSER FOR JAVA EDITION IS INCORPORATED IN THE SOFTWARE, INTERNATIONAL BUSINESS MACHINES, INC. ("IBM") ASSUMES NO LIABILITY FOR ANY CLAIM THAT MAY ARISE REGARDING THE SOFTWARE OR ANY MODIFICATION TO THE SOFTWARE. IBM

DISCLAIMS ALL WARRANTIES, BOTH EXPRESS AND IMPLIED, REGARDING THE SOFTWARE AND ANY MODIFICATION OF THE SOFTWARE.

Government Licensees. This provision applies to all Software and related documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and related documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U. S. Government is granted only with restricted rights and use, and duplication or disclosure by the U. S. Government is subject to the restrictions set forth in subparagraph (c) (1) of the Commercial Computer Software Restricted Rights clause of FAR 52.227-19 or subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013 or their successors, whichever is applicable.

Term and Termination. The License is effective until terminated; however, all of the restrictions with respect to Vertical's copyright in the Software and related documentation will cease being effective at the date of expiration of the Vertical copyright; those restrictions relating to use and disclosure of Vertical's confidential information shall continue in effect. Licensee may terminate the License at any time. The License will automatically terminate if Licensee fails to comply with any of the terms and conditions of the Agreement. Upon termination for any reason, Licensee will immediately destroy or return to Vertical the Software, related documentation and all copies of each.

General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the State of California without respect to any conflict of laws principles. Neither the License nor this Agreement are assignable or transferable by Licensee without Vertical's prior written consent, and any attempt to do so shall be void. Any notice, report, approval or consent required or permitted hereunder shall be in writing. No failure to exercise, and no delay in exercising, on the part of either party hereto, any privilege, any power or any rights hereunder will operate as a waiver thereof, nor will any single or partial exercise of any power hereunder preclude further exercise of any other right hereunder. The parties hereto agree that a material breach of this Agreement by Licensee would cause irreparable injury to Vertical for which monetary damages would not be an adequate remedy and that Vertical shall be entitled to equitable relief in addition to any remedies it may have hereunder or at law.

Should you have any questions concerning this Agreement, contact Vertical Communications, Inc., 1 Cambridge Center, Cambridge, MA 02142.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN VERTICAL AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST VERTICAL UNLESS VERTICAL GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Chapter 12. Managing Workgroups

Chapter 13. Configuring Auto Attendants

Chapter 24. Continuing System Administration

Chapter 25. Client-Side Applications

Part 3 Key Vertical Wave Concepts

Chapter 26. Understanding Vertical Wave Trunks

Chapter 27. Understanding Wave IP Telephony

Chapter 29. Understanding Vertical Wave Data Networking

Chapter 32. System locale settings

About This Guide

CHAPTER CONTENTS

Welcome to the *Vertical Wave Administrator's Guide*. This guide provides detailed information about configuring the Wave Integrated Services Manager (ISM) and Vertical Wave system software.

This guide is intended for network administrators, telephone system administrators, and office personnel who are responsible for configuring and maintaining the Wave system.

This guide provides information about all parts of the remote administration interface used to perform the configuration and system administration steps to set up the Wave system. An extensive online Help system provides detailed information about additional functionality not described in this guide.

Where to start

This guide includes information for readers at a variety of levels. To get the most out of the documentation, start by reading the parts that are most relevant to your level of experience.

For new Wave system administrators

1. Begin by reading Part 3, “Key Vertical Wave Concepts”
2. Next, work through the procedures in Part 1, “Initial Configuration and Administration” to configure the basic Wave system settings.
3. Then choose the advanced features you wish to configure from Part 2, “Advanced Configuration and Administration”.
4. Refer to Part 4, “Reference”, as necessary.

That’s all you need to begin configuring most typical Wave system installations.

For experienced Wave system administrators

1. Begin by working through the procedures in Part 1, “Initial Configuration and Administration”, to configure the basic Wave system settings.
2. Then choose the advanced features you wish to configure from Part 2, “Advanced Configuration and Administration”.
3. Refer to Part 3, “Key Vertical Wave Concepts”, and Part 4, “Reference”, as necessary.

Using the Help system

The Wave Help system provides context-sensitive Help. To access Help, use the following methods:

- From the Wave Global Administrator Management Console, click the Help icon located at the top right corner, then select a topic from either the Contents tab or the Index tab. Use the Search tab to locate topics that include specific text.
- From each Management Console applet, click the Help button to directly access the relevant Help topic.

Conventions used in this guide

In the course of describing Wave system features and functions, this guide uses the conventions described in this section.

Special messages

Note: A note relays information that is important or of special interest.

Hint: A hint relays information to help you perform a task.

Caution: *A caution highlights information that helps you prevent damage to the equipment or to data. It tells you how to avoid the problem.*

Warning: *A warning alerts you to a situation that could cause you physical harm.*

Type conventions

Type Convention	Used to Indicate
Bold	User interface elements (buttons, field labels, and tab labels)
Italics	Book titles, glossary words, and word emphasis
`Courier font`	Screen text and user-typed command line entries
Initial Caps	Product names, menu titles, window titles, application titles, dialog titles, hypertext links, file names, and directories

Terms used

Term	How to Interact
Click	Click the left mouse button.
Right-click	Click the right mouse button.
Shift-click	Hold the Shift key while clicking the left mouse button.
Ctrl-click	Hold the Ctrl key while clicking the left mouse button.
Ctrl+Q	Hold the Ctrl key while pressing one or more additional keys.
Enter	Press the Enter key or select OK.

Term	How to Interact
Type	Type the indicated text, but *do not* press the Enter key or select OK.
Press	Press only the key or keys referred to.
Check	Place a check mark in the check box.
Select	Choose an option from a menu, drop-down list, or list of radio buttons.

Related reading

The following documents are included with Vertical Wave in Acrobat format, and can be found on the Vertical Wave Documentation CD.

For information about this version of Vertical Wave, including new features, known issues, and other late-breaking information, see the Release Notes included on the Documentation CD.

Manuals

Vertical Wave Installation Guide. Provides detailed instructions for physically installing a Vertical Wave system and performing initial system configuration..

Vertical Wave System Recovery Guide. Describes how to use the Vertical Wave System Recovery Disk to restore your Wave ISM to its original factory settings for emergency recovery.

Vertical Wave Administrator's Guide (this manual). Provides task-based instructions on how to use all aspects of the Vertical Wave Administration Console.

Vertical Wave User's Guide. Provides task-based instructions on how to use Vertical Wave, including the telephone commands, ViewPoint, working from remote locations, participating in a contact center, and so forth.

Vertical Edge Digital Phone User's Guide. Describes how to use Vertical Edge digital phones.

Vertical Wave SIP Phone User's Guide. Describes how to use Vertical Wave SIP phones.

Quick Reference Guides

<italics>Vertical Wave Analog Phone Quick Reference Guide. Provides instructions for using analog telephones with Vertical Wave.

Vertical Edge Digital Phone Quick Reference Guide. Provides instructions for using Vertical Edge digital telephones.

Vertical Wave SIP Phone Quick Reference Guide. Provides instructions for using Vertical Wave SIP telephones.

Vertical Wave Voice Mail Quick Reference Guide. Provides instructions for using Vertical Wave Voice Mail features.

Support services

Vertical Communications has worked diligently to produce the highest quality communications system possible. In the course of installing or customizing a system customers may require personal attention.

For technical support contact your reseller.

For more information about Vertical and its products, contact your reseller or call 1-877-VERTICAL.

Web site

The Vertical Communications Web site provides information about Vertical Communications and the Vertical Wave product line.

http://www.vertical.com

System security

You are responsible for the security of your Wave system. Unauthorized use of the Wave system could result in toll fraud. Your system administrator must read all system administration documentation to understand which configuration options can introduce the risk of toll fraud and which configuration options can be activated or deactivated to prevent it.

Vertical Communications, Inc. does not warrant that the configuration software is immune from or will prevent unauthorized use of common-carrier telecommunications facilities and services accessed through or connected to the Wave

ISM. Vertical Communications, Inc. is not responsible for any charges resulting from unauthorized use.

Part 1

Initial Configuration and Administration

Navigating the Management Console

CHAPTER CONTENTS

This chapter provides general navigation information, as well as descriptions of applets and dialog boxes that you might use frequently to configure various Vertical Wave settings.

Before Logging On

Before logging on to the Wave Global Administrator, make sure you have configured your browser as follows:

- Enable your browser security settings to allow installation of ActiveX controls.
- Enter the Wave ISM IP address in the list of trusted sites.

Initial logon

During installation, you should have connected a client workstation to Wave using a modem or an Ethernet port on the Integrated Services Card (ISC). If you have not yet made an initial connection, see the *Vertical Wave Installation Guide* for instructions.

The first time you log on to the Vertical Wave Management Console, you will use a default user name and password. You will change the default name and password later.

To log on for the first time:

1 On the client workstation, launch Microsoft Internet Explorer.

2 Enter the default host name or IP address on the address line of your browser.

The default host name is io-default. The default IP address is 192.168.205.1.

Note: When you launch the Vertical Wave Management Console, a dialog box may appear asking you to install the Java 2 runtime environment (Java 1.5.0_06 plug-in). Click **Yes** in this dialog box to perform the installation.

The Wave Global Adminitrator Log On screen appears.

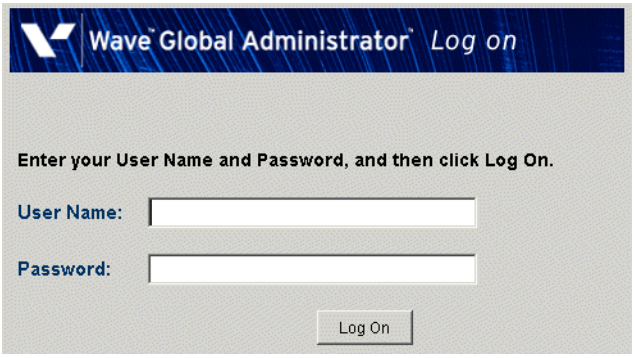


Figure 2-1 Wave Global Administrator Log On screen

3 Enter your user name and password. The initial default logon is:

User Name: GlobalAdministrator

Password: Vertical4VoIP!

Note: The password is case-sensitive.

4 Click **Log On**.

If other users are logged on to the Management Console, a list of logged on users will appear. Click OK to close the dialog box.

When your logon is successful, the Vertical Wave Global Administrator Management Console screen appears. Throughout this document, this screen will be called the Management Console.

Figure 2-2 Vertical Wave Global Administrator Management Console screen

Management Console basics

The Management Console is a portal to the applets and their associated dialog boxes used to configure Wave. You open each of those applets using the same method. Likewise, you return to the Management Console from those applets and their associated dialog boxes using the same method. The following sections describe these methods.

Note: With Microsoft Windows XP Service Pack 2, Microsoft has, by default, enhanced the browser security of Internet Explorer which will affect the functionality of the Management Console, such as preventing some applets from being displayed. To ensure that you do not encounter any problems when using the Management Console, you should perform the following procedure.

If you are accessing Wave from a Windows XP SP2 client, perform the following to avoid potential problems:

a Open Internet Options in Internet Explorer.

b Select "Privacy Options".

c Click on "settings" for the popup-blocker.

d Add the url for the Wave Integrated Services Manager (ISM) to which you need access.

E.g. http://192.168.210.1 or http://yourservername

If you are accessing Wave ISM by IP address, then perform the additional steps that follow. Otherwise skip them.

e Open Internet Options in Internet Explorer.

f Select Secuity.

g Select Trusted Sites.

h Click Sites....

i Uncheck Require server verification (https:).

j Add the IP Address to the Web Sites list.

Opening and closing applets

To open any applet, click its icon in the Wave Global Administrator Management Console. You may need to select the appropriate tab at the top to find the icon you need.

There are two types of applets accessible from the Management Console, dialog boxes and remote access applications. Each type has a different method of exiting and returning to the Management Console.

Dialog box applets

These applets open master dialog boxes. After editing data in a dialog box, click one of the following:

- **Done.** Exits the dialog box, prompting you to save any changes.
- **Restore.** Returns the dialog box data to its previous (unmodified) state.
- **Apply.** Saves your changes without closing the dialog box.
- **Help.** Opens a Help topic describing how to configure the settings in the applet.

You may open subsequent dialog boxes from a master dialog box. If you do, when finished click **Done** or **OK** to close each dialog box until you return to the Management Console.

Remote Access Application applets

These applets open a remote desktop access session to an application. When finished, exit the application as you normally would, for example, by choosing **File > Exit** or by clicking the **X** in the upper-right-hand corner. This returns you to the Management Console.

Note: If you have clicked the Wave Desktop icon in the Management Console for remote access, you will need to log off the Windows desktop inside the remote access session to return to the Management Console.

The following Management Console applets are launched through remote access:

Administration tab

- User / Workgroup Management (see “Using the User / Workgroup Management applet” on page 2-9)
- Date and Time
- RAID-1 Configuration
- Local TAPI Configuration
- Microsoft RRAS
- Network Connections

Diagnostics tab

- Event Viewer
- Network Monitor
- Performance Monitor
- Task Manager
- System Information

Having trouble making a remote connection?

If you have trouble making a remote connection, check your browser proxy settings.

To check the proxy settings:

1. From the Tools menu of Internet Explorer, choose Internet Options.
2. Click the Security tab.
3. If necessary, click the Local intranet icon to select it.
4. Click the Sites button.
5. If necessary, select the Include all sites that bypass the proxy server option.
6. Click the Advanced button.
7. Enter the specific Wave host name in the Add this Web site to the zone field.
8. Click Add.
9. Click OK to save your changes and close each of the three dialog boxes.

Navigating applet tree structures

Several of the Management Console applets employ tree structures to represent the items you are configuring. For example, the Trunk Configuration applet uses a tree structure to represent cards or modules and the trunks and channels you are configuring.

Navigating applet tree structures typically includes the following:

- Displaying and hiding items in a tree (for example, the channels of a card or module in the Trunk Configuration applet)
- Selecting items in a tree

Displaying and hiding items in a tree

To display items in a tree:

1 Open the appropriate applet, if it is not already open.

Figure 2-3 uses the Trunk Configuration applet as an example.

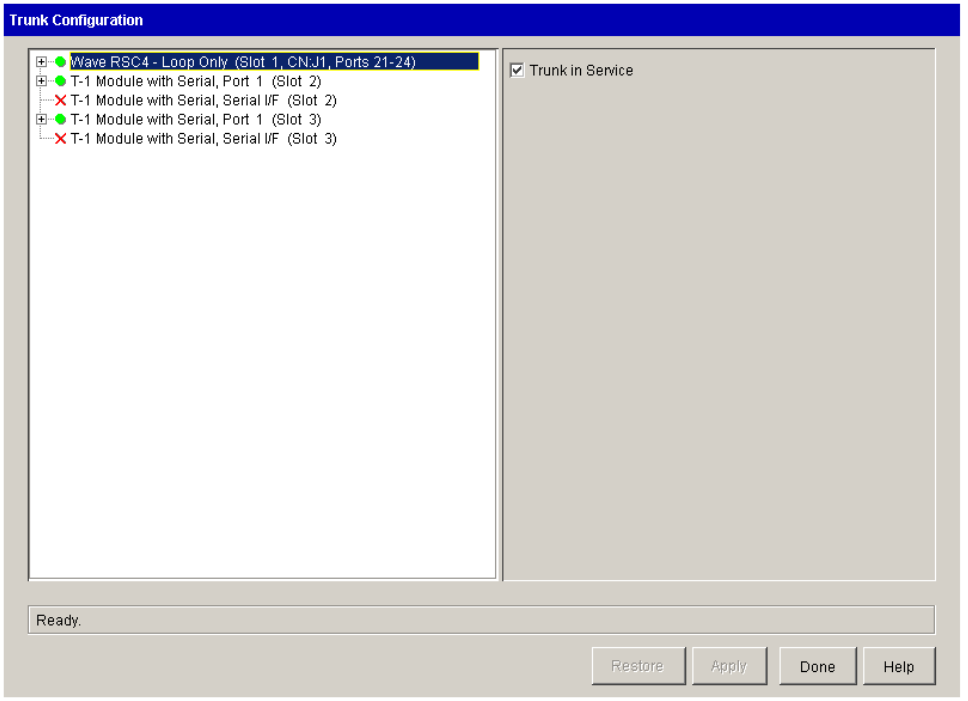


Figure 2-3 Trunk Configuration applet

Note: A green dot next to a trunk, channel, port, module, or card indicates that it is in service. A red X indicates that the item is not in service.

2 Click the plus (+) sign next to the appropriate module or card to display the items within it.

To hide items in a tree:

1 Complete any configuration changes you are making in dialog boxes opened from an applet, and return to that applet.

Figure 2-4 uses the Station Ports applet as an example.

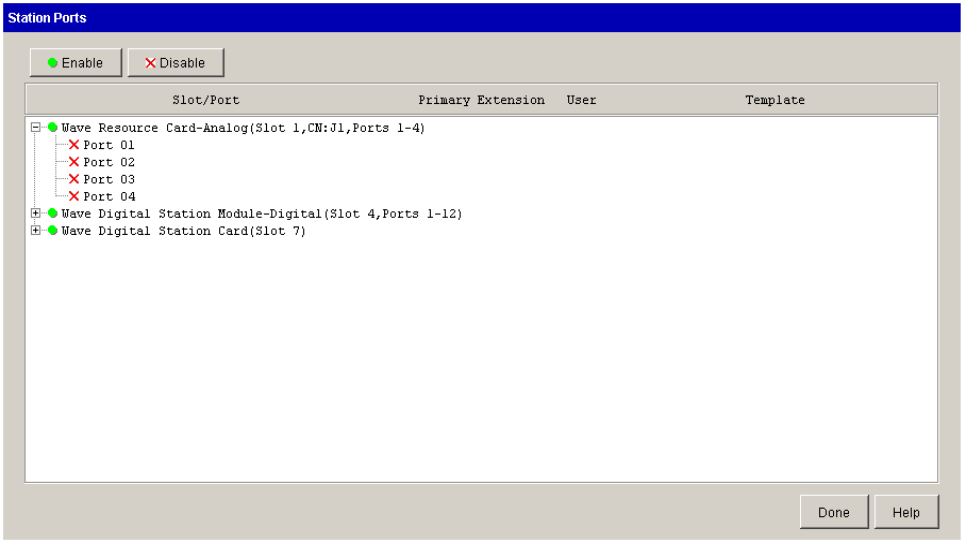


Figure 2-4 Station Ports applet

2 Click the minus (-) sign next to the appropriate trunk, module, or card to hide the items within it.

Selecting items in a tree

To select items in a tree:

1 Open the appropriate applet, if it is not already open, and display the items within a trunk, module, or card.

2 Select the items you want to configure.

- To select a contiguous range of items, select the first item in the range, then hold down the Shift key while you select the last item in the range.
- To select a noncontiguous range of items, hold down the Ctrl key while you select each item.

When you access dialog boxes containing values that apply to the selected channels, what you see depends on which channels are selected:

- If all channels selected have the same values, those values are displayed
- If all channels selected have the same values, and those values are the default values, the word Default is displayed
- If the channels selected have different values, the expression No Common Value is displayed. In the case of check boxes with different values, the check boxes are deselected and (No Common Value) is appended to their labels

Using the User/Workgroup Management applet

The User / Workgroup Management applet is a remote access applet that lets you configure users as well as access many other Wave configuration and monitoring tools.

Accessing the User/Workgroup Management applet

To access the User / Workgroup Management applet, do the following:

1 From the Wave Global Administrator Management Console, click the **User/Workgroup Management** icon, located in the PBX Administration section.

2 A remote access session opens, connecting you to the Global Administrator Log On dialog box, with your Wave username and password already entered.

If your name and password don't appear, enter them.

A username called "Admin" exists by default, with a password of 100. To create other administrators, you must add users to whom you give Global Administrator permissions (see "The Security \ Permissions tab" on page 11-39).

Leave **Station ID** set to 0.

3 Click **OK**. The User / Workgroup Management applet opens.

Note: Leaving the Admin user password as 100 is a security risk that can cost your company money due to toll fraud. For more information about system security, see Appendix A.

The User/Workgroup Management applet interface

The User / Workgroup Management applet interface is composed of *views* (see "Working in views" on page 2-12). Each view enables you to configure, manage, or monitor an aspect of the Wave system.

View	Description	See
Users 	Manage Wave users. Includes changing passwords and allocating disk space to users for voicemail messages and greetings.	"The Users view" on page 11-3
Workgroups 	Manage workgroups (groups of related extensions or contacts).	"The Workgroups view" on page 12-3
Pickup Groups 	Manage Pickup Groups (groups of extensions that can be answered by all the users in the group).	"Call pickup groups" on page 18-4
Dialing Services 	View external first digits and configure how they appear in ViewPoint	"Configuring how first digit extensions appear in ViewPoint" on page 9-3

View	Description	See
Auto Attendants 	Manage auto attendants that handle and route inbound calls with voice menus.	"Creating a new auto attendant" on page 13-3
Queues 	Manage groups of agents in Wave call center queues.	*Vertical Wave Contact Center Administrator's Guide*
Maintenance Log 	View a log recording Global Administrator actions.	"Using the Maintenance Log view" on page 23-4
Dial Plan 	View and edit a complete list of internally dialable numbers.	"Managing your dial plan with the Dial Plan view" on page 23-3
System Prompts 	Listen to and change recordings used for standard system prompts and auto attendants.	"The System Prompts view" on page 19-2
Call Log 	View a record of all the calls made on the system.	"Using the Call Log view" on page 23-5
IVR Plug-Ins 	Manage Wave IVR Plug-ins, which are custom interactive voice response applications that you or third parties can create.	

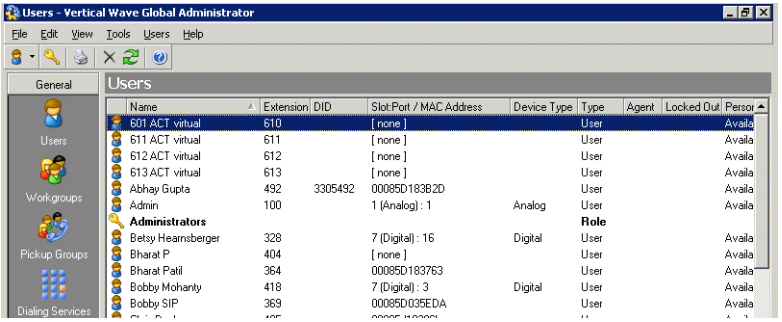
Using the Tools menu

The **Tools** menu of the User/Workgroup Management applet offers additional Wave features not available from the views:

Command	Description	See
Update Access Codes	Lets you change the access code used for a particular dialing service.	"Changing an access code in users' saved numbers" (page 9-33)
Adjust Station IDs		
Columns	Lets you customize the columns that appear in each view.	"Customizing columns" (page 2-14)
Options	Lets you customize the appearance of names, Call Log size, and defaults for station and extension numbers.	"Assigning an extension" (page 11-11) "Displaying a specific number of Call Log entries" (page 23-10)
System Settings	Lets you configure and customize several aspects of your Wave system.	Chapter 4

Working in views

To open a view, click its button in the vertical *view bar* on the left side of the User / Workgroup Management applet window.



You can also open a view by clicking the **View** menu and choosing a view.

Note: If a view is not available to you, you might not have permission to view it. Check with your system administrator, or see "The Security \ Permissions tab" on page 11-39.

The main part of a view contains rows of the *items* that pertain to that view. For example, in the Users view, each Wave user appears as an item on a row. Double-click an item to edit it.

Using commands in a view

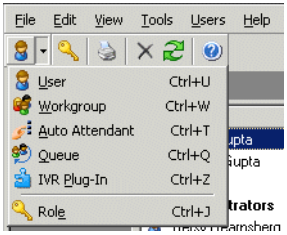
A command always affects the item or items that are selected. To select multiple items, hold down the CRTL key as you click the items. You can perform a command using any of the following methods:

- Choose a command from the view's menu. For example, in the Users view, click the **Users** menu and choose a command.
- Click a toolbar button (see the next table).
- Right-click an item and choose a command from the shortcut menu that appears. This is often the fastest way to perform an command.

Using the User/Workgroup Management applet toolbar

The User / Workgroup Management applet toolbar is located on the main menu bar in each view. It gives you quick access to several User / Workgroup Management applet commands that are also available through the User / Workgroup Management applet menus.

To create a new item when you are working in any Wave view, click the arrow next to the first button on the toolbar and select an item.



See the next section for information about creating new items that are based on existing items.

Customizing columns

Click a column header to sort by that column. Click again to sort in the reverse order. The arrow in the column header shows by which column and in what direction the display is currently sorted.

You can resize column widths by dragging the sides of the column headers.

For each view in the User / Workgroup Management applet, you can choose the columns that you want to see and the columns that you want to hide. Some views do not show all the available columns by default.

To show or hide columns in a view:

1. Choose **Tools > Columns,** or right-click a column header.The Columns dialog box opens.
2. From the **View** dropdown list, choose the view you want to change.
3. Check a column to show it. Uncheck a column to hide it. For an explanation of the various columns, click **Help**.
4. Click **OK**.

Working with voice files

A voice file is an audio recording that is stored as a file. Wave stores system prompts, greetings, voice messages, and recorded conversations in voice files that you can play over your computer speakers or on the telephone. You can record voice files using the telephone.

Wave voice files are in .WAV format, but you can import files of other formats.

Note: When archiving voice messages or call recordings you can specify .MP3 as the file format. See “Archiving call recordings and voice mail” on page 23-34.

Using the audio controls

Wave's audio controls make it easy to create and modify recordings of all types. The following controls appear in Wave wherever you can create and listen to recordings.

To create and play recordings, use the buttons on the audio controls as shown in the following table and speak into your phone.

Record	When you are ready to record, pick up your phone, and then click this button. A beep signals that recording has begun.
Play	To hear the recording, click this button.
Stop	When you are done recording, you can either hang up or click this button.
Fast Forward	To skip ahead in the playback, click this button.
Rewind	To skip back in the playback, click this button.

To move forward and backward within the recording, drag the slider bar.

Importing and exporting voice files

To import or export a voice file, use the import or export buttons on the recording control, as shown in the next table.

Import	You can import a voice file in .WAV or .VOX format to use for any Wave recording (greetings, voice titles, and so on). Wave can import .WAV files with a frequency of 8Khz, 11.025 Khz, 22.05 Khz, or 44.1 Khz. You can also import an 8 kHz PCM .VOX file (MuLaw format for North America and Japan, ALaw format for other countries).

Export You can export any of your recordings, including system prompts and voice titles, to a .WAV file or an .MP3 file.

Initial System Configuration

CHAPTER CONTENTS

This chapter guides you through the tasks required for initial Vertical Wave system configuration.

Before you begin

Before you configure Wave, make sure the following installations and records are complete:

- Cabling and hardware installations

  See the *Vertical Wave Installation Guide*.
- Trunk (or service) confirmation letter from your telephone network provider
- Your Configuration and Design Worksheets (from your Vertical Communications reseller) on trunking, extensions, incoming and outgoing call flow, voice mail access, and your dialing plan

To manage Wave, you need a client workstation with the following minimum configuration:

- A PC running Microsoft Windows 2000, Windows XP, or Windows Server 2003 and at least 256MB of RAM
- LAN or WAN connectivity through an Ethernet card or modem
- Microsoft Internet Explorer 6.0 Service Pack 1

Note: Some of the Management Console applets display dialog boxes, warnings, and panels automatically. If you have installed a browser pop-up blocker on your client PC, these pop-ups may not appear. You can usually configure blocker software to allow pop-ups from specific domains or IP addresses.

Identifying your Wave ISM on the LAN

To identify your Wave ISM and enable it to communicate using Transmission Control Protocol / Internet Protocol (TCP / IP) on your LAN, perform the procedures in the following sections:

- Assigning a new host name
- Changing network interface static IP addresses
- Setting the dial-in default address pool
- Verifying that the Wave ISM is connected to your LAN

Assigning a new host name

In this procedure, you will change the default host name to one that identifies your Wave ISM on your network.

The IP Network Settings applet ensures that the host name is the same as the DNS or IP name, and the WINS or computer name. Use a unique name with up to 15 alphanumeric characters and dashes (-).

To change the host name of your Wave Integrated Services Manager (ISM):

Click

1 If necessary, click the Administration tab of the Management Console.

2 Click the IP Network Settings icon, located in the Data Administration section.

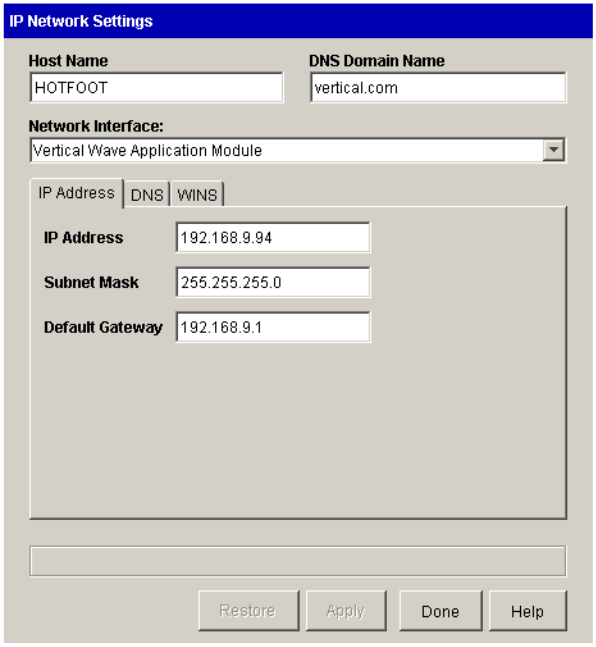


Figure 3-1 IP Network Settings applet

3 Click OK in the dialog box indicating that any changes you make in the applet may require you to restart the Wave ISM.

4 Select the default host name in the Host Name field and type a new name (15 characters or less) for your Wave ISM.

5 Enter a domain name in the DNS Domain Name field.

You must use a period (.) in the domain name, as in vertical.com.

Changing network interface static IP addresses

In this procedure, you will change the default IP addresses for installed cards and modules to static IP addresses that identify the Wave ISM on your network. Your particular configuration reflects only the cards and modules you have installed on your Wave ISM.

To change network interface static IP addresses:

1. In the IP Network Settings applet, choose an interface from the Network Interface drop-down list.
2. If necessary, click the IP Address tab to bring it forward.
3. Select the default value in the IP Address field and type the network IP address you want to assign.
4. Select the default value in the Subnet Mask field and type the subnet mask number you want to assign.

   The default subnet mask number 255.255.255.0 enables up to 254 host computers to be connected to the LAN. On a small network, it is fine to use the default.
5. Enter a value in the Default Gateway field.

   The default gateway is the router that the Wave ISM contacts to locate a machine (a client or any other machine) that is not on the same subnet. The default gateway should be part of the same subnet as the interface you selected in step 1 of this procedure.

   Use the router closest to the Internet or network backbone as the default gateway address that connects your Wave ISM to a larger network; if you have a small network, use the IP address of the Internet router.

   > **Note:** Typically a system has either one default gateway or none. In networks which have loops (multiple paths to the same location), it is possible to have more than one default gateway.
6. Repeat steps 1 through 5 to set the IP address, subnet mask, and default gateway for each network interface listed.

   Note: If you have one or more Media Resource Modules installed in your system, you will need to configure each device as described above.
7. Click Apply.

   Wave saves your changes and automatically restarts if you have made a change to the Windows adapters. A restart is not required if you have only added IP addresses to your MRMs.

   Caution: *Do not click **Done** after clicking **Apply**. Doing so may prevent the Wave ISM from restarting, which will prevent your changes from taking effect.*
8. Close the Web browser.

Setting the dial-in default address pool

Before Wave will allow dial-in connections, you must set the IP address pool for those connections. Because this is an internal pool of addresses, you'll get the appropriate settings from your company's system administration group.

Note: All Wave ISMs ship with the same default IP address pool. Enabling a routing protocol such as RIP or OSPF on the Wave ISM causes it to advertise a route to that address pool. If you choose not to change the default IP address pool, each system will advertise a route to the same IP address pool, which may result in network problems.

To set the dial-in default address pool:

1. If necessary, click the Administration tab of the Management Console.
2. Click the Microsoft RRAS icon, located in the Data Administration section.

   Click

   When you launch certain Microsoft Windows tools from the Vertical Wave Management Console, they start up in a remote control window that allows tools or applications running on the server (Wave in this case) to appear on the client (your workstation). Each time you use one of these tools, you will perform a remote control log on. See "Remote Access Application applets" on page 2-5 for detailed information and an example.
3. In the Routing and Remote Access dialog box, select the Wave ISM in the tree on the left.
4. Select **Action > Properties**.
5. Click the IP tab.
6. Define the IP address pool in the Static address pool section of the RAS Server TCP/IP Configuration dialog box.

   The IP address pool is defined with a range of IP addresses.

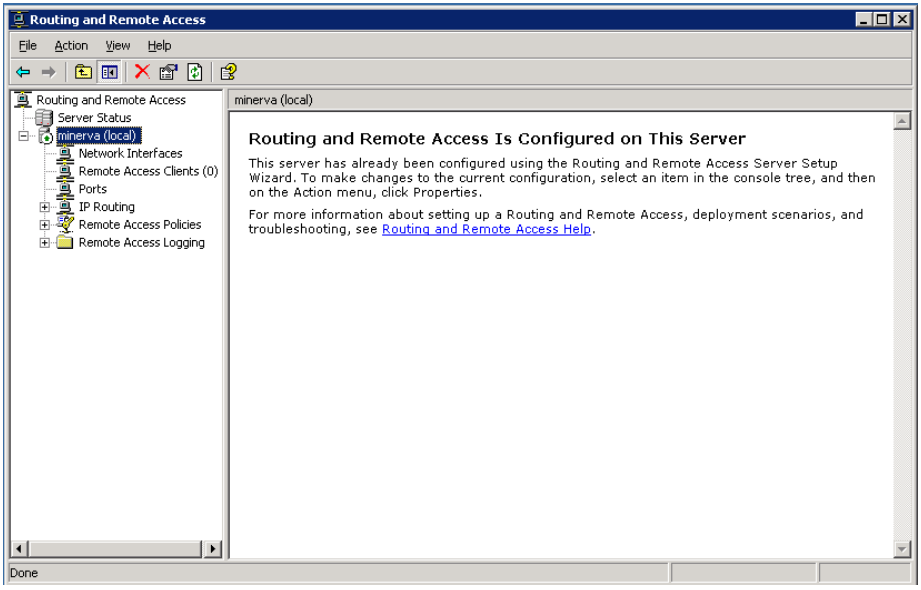


Figure 3-2 RAS Server TCP/IP Configuration dialog

Note: The lowest two addresses and the broadcast address (the highest address) in the range are reserved and will not be assigned.

7 Click OK to save your changes.

8 Close the Routing and Remote Access dialog box to return to the Management Console.

Verifying that the Wave ISM is connected to your LAN

When you can successfully reach the Wave ISM across your network, you know it is configured to operate on your LAN.

To verify the Wave/LAN connection:

1 Open a Command Prompt window on your client workstation.

2 Ping the Wave ISM using either the host name or the IP address you assigned to the Integrated Services Card. When entering the command using the IP address, use the form:

ping *x.x.x.x*

where *x.x.x.x* is the IP address of the Wave ISM.

If you need additional help using ping, enter the following command:

ping -h

A successful ping will look like the one shown in Figure 3-3.

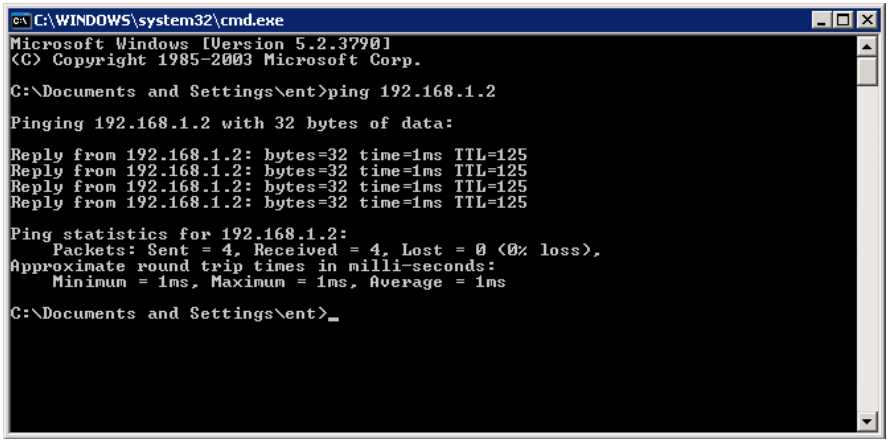


Figure 3-3 Successful Wave LAN connection

Logging on to the Wave ISM

To log on:

1 Connect your client workstation to the Wave ISM.

- If you connect a workstation to an Ethernet port on the Integrated Services Card, change the IP address of the workstation to any IP address *on the same subnet as the Wave ISM except the address of the Wave ISM isself.* For example, if the Wave ISM is configured as 192.168.205.1 with a subnet mask of

255.255.255.0, you should choose an address between 192.168.205.2 and 192.168.205.254. Restart the workstation after changing the IP address.

- If you connect over a modem, use your initial connection dial-up networking settings. For more information, see the *Vertical Wave Installation Guide.*

2 Open Microsoft Internet Explorer and enter the Wave host name (or IP address) in the address line.

The Log On Vertical Wave screen appears.

3 Enter the default user name and password.

The default user name is GlobalAdministrator and the default password is Vertical4VoIP!.

4 Click Log On.

When you have successfully logged on, the Vertical Wave Management Console appears.

Verifying installed components

You can verify that all of your installed cards and modules are recognized by the Wave system and functioning properly by using the Chassis View applet. Chassis View shows all cards and modules installed in the Wave ISM chassis; connectors and LEDs display status dynamically.

To verify installed components:

1 If necessary, click the Administration tab of the Remote Management Console.

Click

2 Click the Chassis View icon, located in the General Administration section.

3 Make sure all the cards and modules you have installed are visible in the graphical representation of your Wave ISM chassis.

Positioning the cursor on a card or module displays an expanded version of it, along with statistics for that card or module, to the right of the representation of the entire chassis. Clicking a card or module takes you to the appropriate configuration applet.

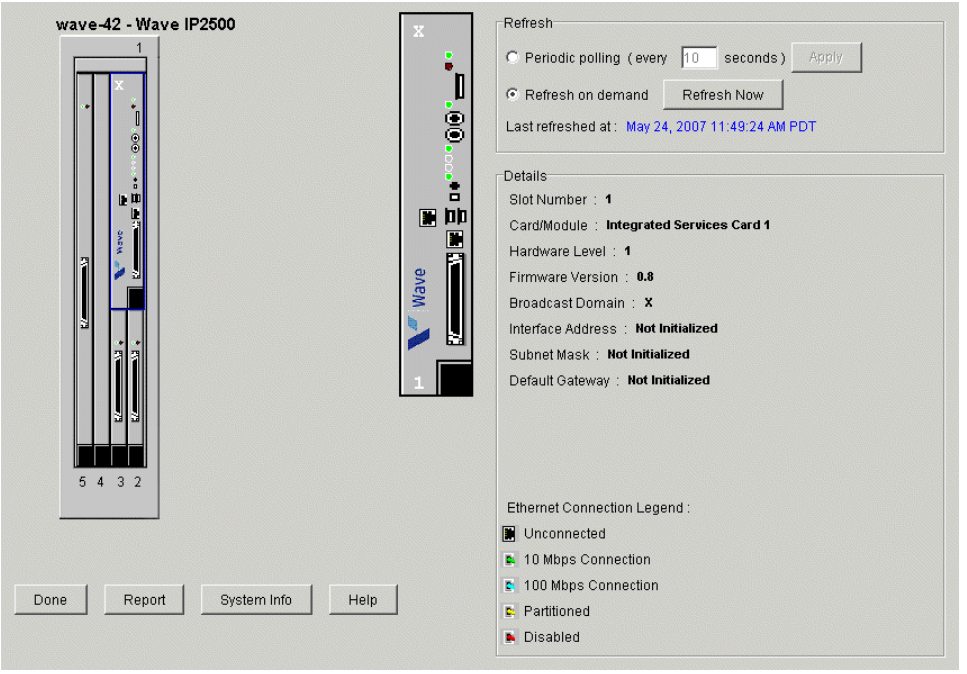
4 If a card is not visible in Chassis View, check the physical LEDs to make sure they are green (on and operational).

If the physical LEDs are red (nonoperational):

a Shut down and then power off the Wave system.

b Reseat the card.

c Restart the system, reopen your browser window, and check Chassis View again.



Chassis View applet showing installed cards and modules

d Verify that the Wave components that were not visible now show as functioning in Chassis View.

5 Click **Done** to return to the Management Console.

Setting the system date and time

Use the instructions that follow to verify or change your Wave date, time, and time zone.

To set the date, time, and time zone:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Date and Time icon, located in the General Administration section.

When you launch certain Microsoft Windows tools from the Vertical Wave Management Console, they start up in a remote control window that allows tools or applications running on the server (Wave in this case) to appear on the client (your workstation). Each time you use one of these tools, you will perform a remote control log on. See “Remote Access Application applets” on page 2-5 for detailed information and an example.

3 Log on to Windows.

The default user name is GlobalAdministrator and the default password is Vertical4VoIP!.

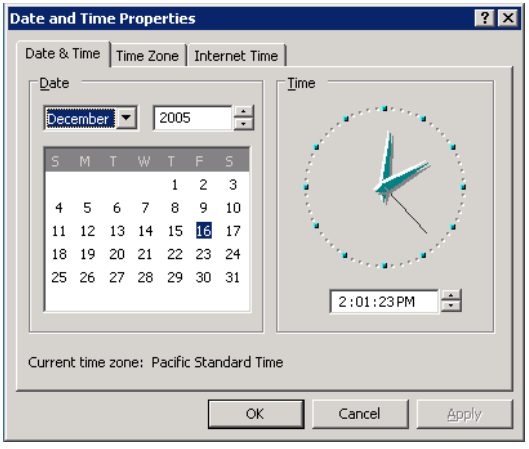


Figure 3-4 Date / Time Properties dialog

4 In the Date / Time Properties dialog box, click the Time Zone tab, and verify that the time zone is correct for your Wave ISM location.

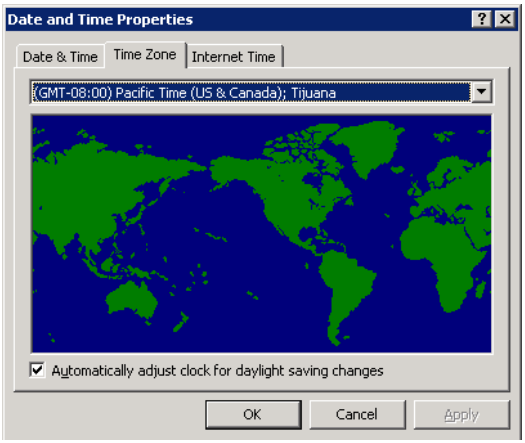


Figure 3-5 Date/Time Properties dialog showing Time Zone tab

If you need to make changes:

- **a** Change the time zone by selecting a zone from the drop-down list.
- **b** If you do not want Wave to adjust automatically for daylight savings time, deselect the check box.

5 Click the Date & Time tab (see Figure 3-4), and verify that the date and time are correct for your Wave location.

If you need to make changes to the date and time:

- **a** To change the month, choose a new value from the drop-down list.
- **b** To change the year, click the up or down arrow to the right of the year field.
- **c** To change the day of the month, click the desired date.
- **d** To change the time, select the hours, minutes, seconds, or A.M./P.M. field, then either type a new value or use the up or down arrow to adjust the value. Repeat this process for each field that needs to be changed.

6 Click OK to save the changes.

7 Click Done (Return to Console).

Entering basic system information

You should enter your company name and the Wave Integrated Services Manager (ISM) serial number so that the information is easy to locate when it is requested by your technical support provider. The company name is used in your external caller ID. The Wave ISM serial number is used by the Software Licenses applet to verify that a Vertical Communications software license is applied to the correct Wave ISM, and by Global Manager to identify each Wave ISM uniquely.

To enter basic system information:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

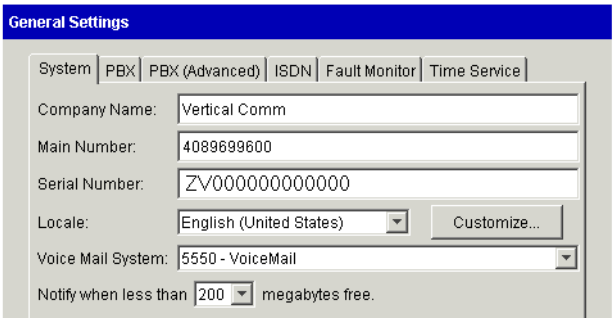


Figure 3-6 General Settings applet, showing the System tab

3 Enter a name in the **Company Name** field.

4 Enter the serial number of the Wave Integrated Services Manager (ISM) in the **Serial Number** field.

The serial number is located on the side of the Wave ISM. It has the following format: ZVnnnnnnnnnn. Enter the whole number.

5 Select your locale from the **Locale** drop-down list.

6 The **Voice Mail System** field defines the voice mail pilot number for the system. The default is 550, but you can map it to a different pilot.

7 Click Apply to save your changes.

8 Click Done to return to the Management Console.

Configuring the time service

The time service polls a specified time server to keep accurate time for Wave components.

To configure the time service settings:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 Click the Time Service tab.

4 Enter the domain names of the desired time servers in the Primary Time Server and Secondary Time Server fields.

Enter the full name of the time server. Two commonly used time servers are *time.nist.gov* and *tick.usno.navy.mil*.

5 Enter the interval (in hours) between each time server poll in the Synchronize Period (hours) field.

6 Click Synchronize Time Service.

This polls the time server immediately.

7 To verify that Wave was resynchronized, refresh your browser window and click the Time Service tab again. If the Last synchronized on field has been updated, resynchronization was successful.

8 To restore the defaults in each of the Time Service fields, click Restore System Defaults

9 Click Apply to save your changes.

10 Click Done to return to the Management Console.

Installing client-side caching

Client-side caching for Wave increases the performance of the Management Console, especially for slow modem connections. The following are important notes about client-side caching:

- It is necessary to install client-side caching on each client every time you upgrade Wave, including Service Pack updates.
- Client-side caching remains active until the next upgrade.

- The caching mechanism will not prevent the client machine from administering previous releases.
- Installing client-side caching requires you to reboot your PC.

To install client-side caching:

Click

1 Click the Client Caching icon in the upper-right corner of the Management Console screen.

   The Remote Management Client-Side Caching page appears.

2 Click the download link on the Web page.

3 Click Save.

4 In the Save As dialog box, navigate to the location on your client workstation hard drive where you want to save the installation program, then click Save.

5 Close all open programs.

6 Double-click the installation program icon to launch the program.

7 Follow the instructions in the installation wizard.

8 When installation is complete, reboot your PC to enable client-side caching.

   Note: If you do not want to reboot at this time, you can return to the Management Console and reboot later.

Adding accounts and passwords

To secure your Wave ISM from unauthorized configuration, you must remove the GlobalAdministrator account and replace it with a new account.

By default, only individuals with enterprise-level access can configure the Wave ISM using the Vertical Wave Management Console.

The Access Permissions applet contains a list of all the Management Console applets and the access level required to use them. You can use the Access Permissions applet to change the level of access granted to manager- and user-level accounts. For instructions on using the Access Permissions applet, refer to the Management Console Help.

The accounts you create in the Password Administration applet are local accounts and are not controlled by your primary domain controller (PDC). For information about adding Wave to your PDC and adding administrator accounts to the PDC, see "Creating Wave user accounts on the primary domain controller" on page 3-16.

To replace the default Wave accounts:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Password Administration icon, located in the General Administration section. The Password Administration applet opens.

3 Click New to open the Add New User dialog box.

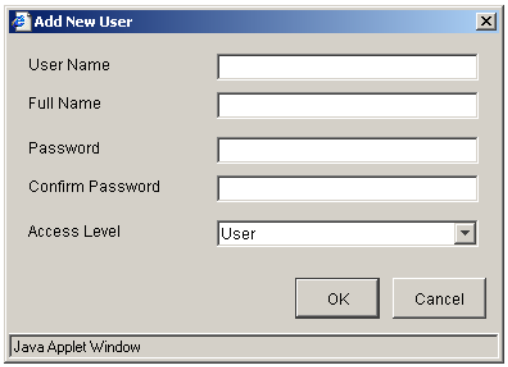


Figure 3-7 Add New User dialog box

The first user you create will be an enterprise-level user. Enterprise-level access is the most comprehensive. It allows an administrator to perform all of the Wave administrative functions, including changing and configuring access permissions. You will need at least one account with enterprise-level access to configure everything in your Wave ISM.

4 Enter a user name for the account in the User Name field.

The user name can up to 20 characters and can use any combination of alphanumeric characters and exclamation points (!), underscores (_), and dashes (-). However, the first character may not be a numeral.

5 Enter the user's full name in the Full Name field.

The full name can be up to 32 characters and can use any combination of characters, including spaces.

6 Enter a password and confirm it in the appropriate fields.

The password can be up to 14 characters and can use any combination of characters except spaces.

7 Choose Enterprise from the Access Level drop-down list.

8 Click OK to close the dialog box.

The information you have specified will appear in the account list in the Password Administration applet.

9 Repeat steps 3 through 8 to create additional accounts. (For accounts with lower access levels, choose Manager or User instead of Enterprise in step 7.)

10 Click Done to return to the Management Console.

11 To secure your Wave ISM, you must log off and log on again with your new enterprise-level user name and password, then return to the Password Administration applet and delete the default GlobalAdministrator accounts.

Caution: *Be sure to keep a record of the new account passwords. Once you remove the default accounts, the only access will be through the new accounts. If you lose your enterprise-level password, you must reinstall and reconfigure your system to gain access.*

Creating Wave user accounts on the primary domain controller

If your Wave installation includes multiple systems, and you have multiple administrators, you might find it convenient to add your Wave ISMs to your Microsoft Windows primary domain controller (PDC). You can then create Wave system administrator accounts on the PDC, allowing centralized login authentication and Wave system administrator account maintenance.

To create Wave accounts on the PDC:

1 On the primary domain controller, create global groups called VNI-Enterprise, VNI-System, and VNI-Users.

2 Add accounts for your Wave administrators to these groups.

Click

To add Wave to your PDC domain:

1 If necessary, click the Administration tab of the Management Console.

2 Click the Network Connections icon, located in the Data Administration section.

When you launch certain Microsoft Windows tools from the Vertical Wave Management Console, they start up in a remote control window that allows tools or applications running on the server (Wave in this case) to appear on the client (your workstation). Each time you use one of these tools, you will perform a remote control log on. See “Remote Access Application applets” on page 2-5 for detailed information and an example.

3 Log on to Windows.

The default user name is GlobalAdministrator and the default password is Vertical4VoIP!.

4 Select **Start > Control Panel > System**.

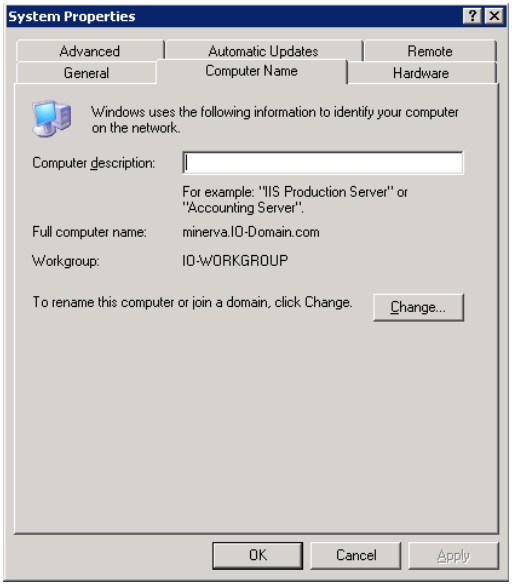


Figure 3-8 Network properties dialog box

5 Click Change on the Computer Name tab.

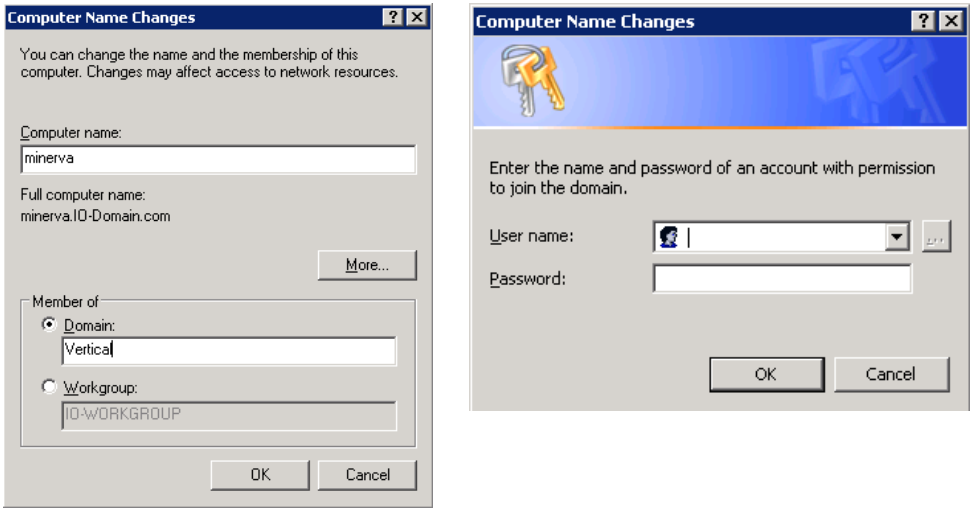


Figure 3-9 Identification Changes dialog box with joining domain login prompt

6 Select the Domain radio button from the Member of group box.

7 Enter the PDC domain name and click **OK**.

A login prompt will then appear.

8 Enter the user name and password of a user on the PDC who has privileges to add workstations to the PDC.

9 Click **OK** to clear the message that appears.

10 Follow the prompts to close the System dialog box. When a message appears asking if you want to restart Wave, click No.

11 Run Create Packages from Wave Utilities.

You can access Create Packages by choosing Start > All Programs > Wave > Utils > CreatePkg.

12 Click Yes in the dialog box that appears.

13 When a message appears indicating that the Create Packages utility has run successfully, click OK.

14 Open the User Manager, located in the Administrative Tools suite.

You can access this tool by choosing **Start > Administrative Tools > Computer Management**, then choosing **Local Users and Groups**.

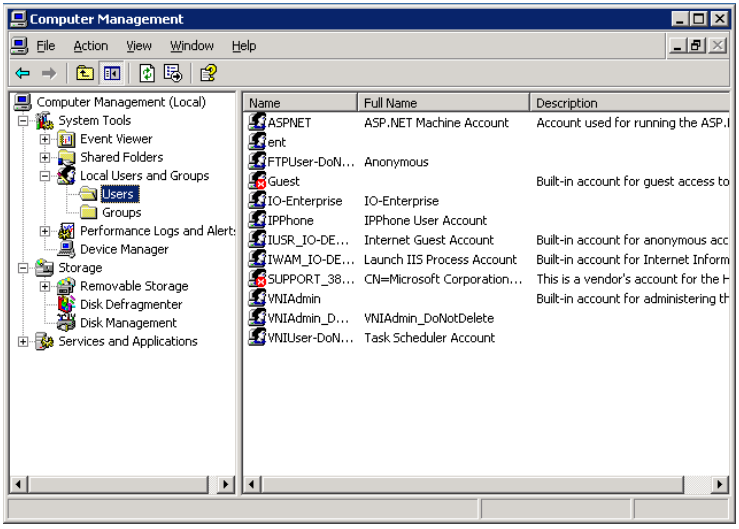


Figure 3-10 User Manager

15 Add the VNI-Enterprise, VNI-System, and VNI-Users groups to the Administrators group.

16 Restart Wave by choosing **Start > Shut Down > Restart**.

Now, whenever you log on to Wave, enter the PDC domain name followed by a backslash (\), then enter your PDC domain user name and password.

For example:

User name: Domain\Username
Password: Password

Note: When logging on to the Wave desktop using Windows Remote Desktop, use your PDC domain user name and password for the Windows login prompt.

Using accounts from a trusted domain

Some customers may want to allow access to the Wave domain by users that do not have accounts in the Wave domain, but have accounts in other trusted domains (user

domains) within their intranet. The easiest way to allow this access is to create a one-way trust relationship.

To create a one-way trust relationship:

1. Export the trust from your user domain:
   a. Log on to the primary domain controller (PDC) of the user domain.
   b. Open the User Manager for Domains tool, located in the Administrative tools suite.
   c. Run User > Select Domain and select the user domain in the list.
   d. Use the User Manager to run Policies > Trust Relationships.
   e. Click the Add button next to the Trusting (not Trusted) Domains group box.
   f. Enter the Wave domain in the Domain Name field.
   g. Assign a password.
      This password is not related to any other password on your system.
   h. Confirm the password.
   i. Click OK in the Trusting Domain dialog box to save the changes.
   j. Click Close to close the Trust Relationships dialog box.
2. Add the global groups VNI-Enterprise, VNI-System, and VNI-Users to the user domain:
   a. In the User Manager for Domains tool, select User > New Global Group.
   b. Enter VNI-Enterprise in the Group Name field.
   c. Add the appropriate users to the VNI-Enterprise group.
   d. Click OK.
   e. Repeat steps 2a through 2d to add VNI-System and VNI-Users groups and users to the user domain.
3. Add the user domain to the list of Trusted Domains in the Wave domain PDC.
   a. Log onto the Wave domain PDC.
   b. Use the User Manager to run Policies > Trust Relationships again.
   c. Click the Add button, next to the Trusted (not Trusting) Domains group box.
   d. Enter the name of the user domain in the Domain Name field.

e Enter the same password you used in step 1g above.

f Confirm the password.

g Click OK in the Trusted Domain dialog box to save the changes.

h Click Close to close the Trust Relationships dialog box.

4 Synchronize the domains.

a Run the Server Manager from Programs > Administrative Tools.

b Select your PDC if it is not already selected.

c Choose Computer > Synchronize Entire Domain.

d Click Yes to confirm and OK to confirm again.

You now have a one-way trust relationship, and can log into the Wave ISMs (members of the IODomain).

System Settings in the User/Workgroup Management applet

CHAPTER CONTENTS

About system settings

The system settings available through the User / Workgroup Management applet control overall Wave behavior. Before adding Wave users, you should define your system settings.

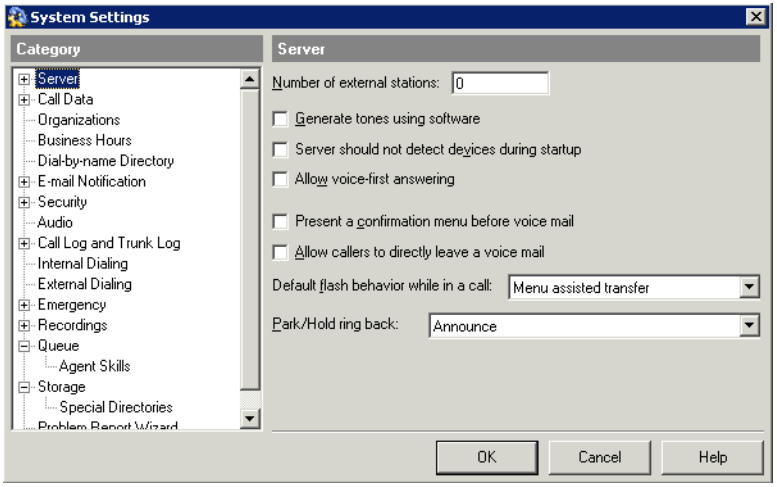
Opening the System Settings dialog box

To access system settings in the User / Workgroup Management applet:

From the Management Console, click the icon for **User/Workgroup Management**, located in the PBX Administration section. The User / Workgroup Management

applet opens. See “Navigating applet tree structures” on page 2-6 for information about navigating in the User / Workgroup Management applet.

5 Choose **Tools > System Settings**. The System Settings dialog box opens.



Documentation for the System Settings dialog box

The following table shows where to find documentation for the various tabs of the System Settings dialog box:

Tab	See…
Server	page 3
Server \ Network Capture	page 50
Call Data \ Account Codes	page 6
Call Data \ Custom Data	page 14
Organizations	page 2
Business Hours	page 6
Dial-by-name Directory	page 5
E-mail Notification	page 10
E-mail Notification \ Event Log	page 13
Security	page 11

Tab	See…
Security \ Permitted Passwords	page 11, page 12
Security \ Workstation Firewall	*Vertical Wave Installation Guide*
Audio	page 1
Call Log and Trunk Log	page 12
Call Log and Trunk Log \ Archive	page 48
Internal Dialing	Dial-by-name directory: page 6 Internal dialing timeouts: page 35
External Dialing	page 34
Emergency	page 35
Recordings \ Archive	page 34
Recordings \ System Call Recording	page 6
Recordings \ Reminder Beeps	page 7
Queue	*Vertical Wave Contact Center Administrator's Guide*
Queue \ Agent Skills	*Vertical Wave Contact Center Administrator's Guide*
Storage	page 46
Storage \ Special Directories	page 49
Problem Report Wizard	page 52

Setting general Wave options

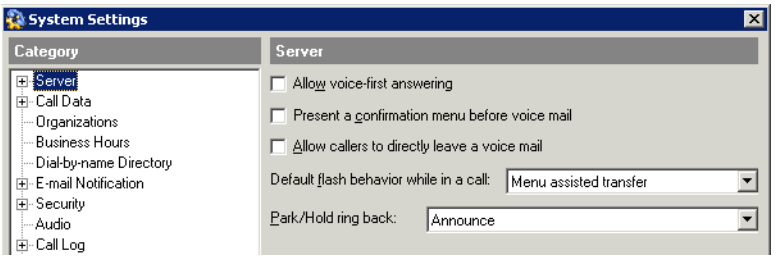
General Wave options include the following:

- **Setting general ISM settings.** See the next section.
- **Configuring the dial-by-name directory.** See page 5.

Setting general ISM settings

To set general ISM settings, do the following:

1 Choose the Server tab.



2 Define the following settings:

- **Allow voice-first answering.** If checked, users with Toshiba digital phones as well as Cybiolink or Aastra Powertouch analog phones can use the voice-first answering feature. With voice-first answering, internal calls are connected to the user's speakerphone automatically without the phone ringing or needing to be picked up. A beep indicates an incoming internal call. (External callers ring as normal.)

  To use voice-first answering, a user must turn it on using ViewPoint or the telephone commands. See *Vertical Wave User's Guide* for details.

- **Present a confirmation menu before voicemail.** Check to have callers hear the confirmation prompt, "To leave a message press 1, or press * to return to the menu" after they hear a user's voicemail greeting. If unchecked (the default), callers go directly to recording their message after hearing the greeting.

- **Allow callers to directly leave a voicemail.** Check to enable callers to dial a user's voice mailbox directly by dialing the extension followed by * from internal dial tone or from an auto attendant.

  If checked, the system adds a 3-second delay after dialing an extension before the call is connected, to wait for the *. Callers can skip the delay by pressing # after the extension. To change the delay, see "Avoiding the auto attendant ambiguous dialing delay" on page 13-10.

- **Default Flash behavior while in a call.** Select what happens when users press **Flash** (or quickly press the hook) while on a call.

  Choose **Menu assisted transfer** to take users to the Wave call handling menu (for details, see Appendix A of *Vertical Wave User's Guide*).

Choose **Direct transfer** to immediately prompt users for an extension to transfer the call. Use this option to create faster, simplified telephone transferring for users who answer and transfer many calls. Note that with direct transfer, users cannot access the other commands on the call handling menu unless they have Wave ViewPoint or a Toshiba digital phone.

- **Park/Hold ringback.** Select what happens when a user answers an automatic ringback call after leaving a call on hold or parked for too long.

  Choose **Announce** to have Wave announce the caller, as with normal call announcing.

  Choose **Direct connect** to have the user connected immediately with the caller.

  Note: By default ringback occurs once, and if the ringback call is unanswered the call is sent to the user's voicemail. You can increase the number of ringback attempts before the call goes to voicemail using the `RingbackRetries` advanced setting. See Appendix J of *Vertical Wave Installation Guide.*

  For instructions on setting ringback, see *Vertical Wave User's Guide.*

3 Click **OK**.

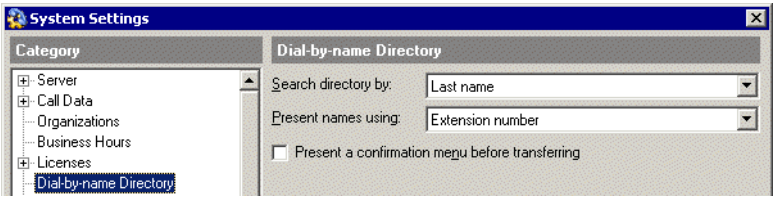
Configuring the dial-by-name directory

The dial-by-name directory enables callers to dial Wave users by name, which is helpful when the extension is not known.

To configure the dial-by-name directory:

1 Choose **Tools > System Settings**.

2 Choose the Dial-by-name Directory tab.



3 In **Search directory by**, select one of the following methods by which callers can search for users:

- **Last name.** Callers enter the first few letters of the last name. This is the default.

- **First name.** Callers enter the first few letters of the first name.
- **Last name or First name.** Callers enter the first few letters of either the first or last name.

4 In **Present names using,** select one of the following methods for presenting the names of users to callers:

- **Extension number.** Callers hear an extension number after each name, for example, “For John Sargent, press 175.” This is the default.
- **Numbered list.** Callers hear a sequence number after each name, as in “For John Smith, press 1”.

5 Use the **Present a confirmation menu before transferring** field to choose what happens when a dial-by-name entry results in a single match. If unchecked, the caller is connected immediately. Check the field to have the caller to confirm his or her choice. For example, a caller would hear, “For John Sargent, press 1. To try again, press *.”

6 Click **OK**.

Changing the internal dial-by-name extension

By default, users can dial 411 to access the dial-by-name directory. To change the number, do the following:

1 Choose **Tools > System Settings**. The System Settings dialog box opens.

2 Choose the Internal Dialing tab.

3 Enter the number in **Dial-by-name directory.**

Note: When you change 411 to another number, the system prompts that refer to it automatically update to use the new number.

Setting business hours

Wave uses your business hours settings in schedules that you create for the following:

- **After hours greetings.** See “Scheduling transfers and greetings” on page 13-11.
- **Automatic transfers.** See “Scheduling transfers and greetings” on page 13-11.
- **Notification of new voice messages.** See “Scheduling notifications” on page 11-24.

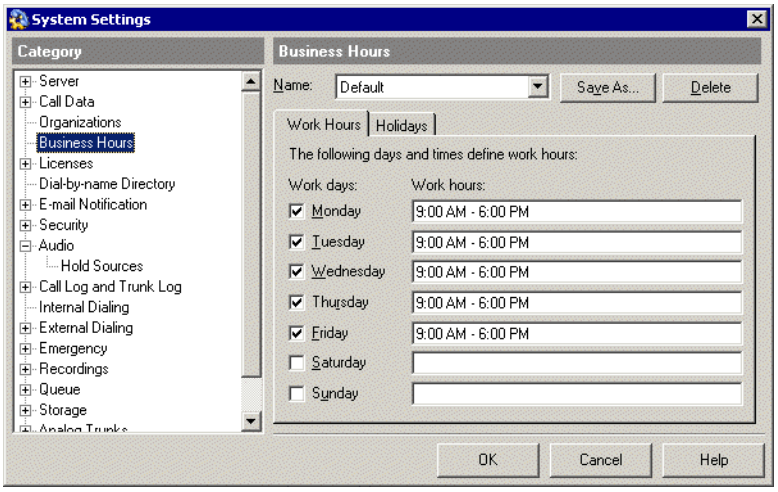
You can create as many sets of business hours as you need. For example, you can create a set of business hours for the company as a whole (the default), and then create additional sets of business hours for individual Organizations, shifts, and so forth.

Defining business hours

To define your business hours, you define your daily work hours, work days and holidays, as follows:

1 Choose **Tools > System Settings**. The System Settings dialog box opens.

2 Choose the Business Hours tab.



From the Business Hours tab you can do the following:

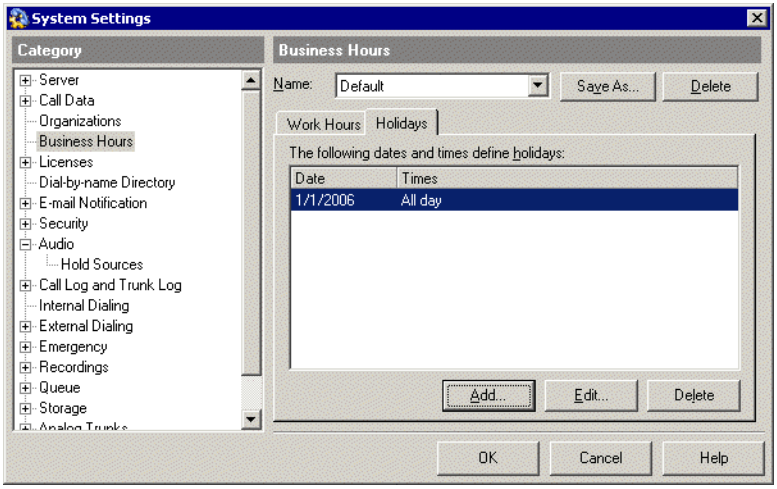
- To create a new set of business hours, fill in the fields, then click **Save As**.
- To edit an existing set of business hours, select its **Name** from the dropdown list.
- To delete a set of business hours, select its **Name** from the dropdown list, then click **Delete**.

1 On the Work Hours tab, under **Work days**, check each day that is a work day, and under **Work hours**, enter the starting and ending times for each work day.

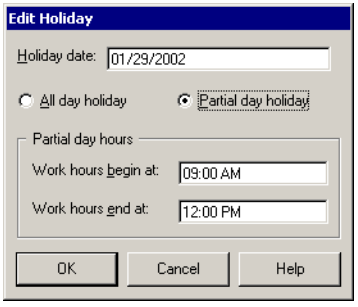
Note: When you define business hours and holidays, you can type dates and times in most formats. Your entries are converted to a standard format that is based on your Windows regional settings.

You can enter more than one time range for a day, separated by commas, for example, “9:00 AM - 12:00 PM, 3:00 PM - 6:00 PM.” Use this format to express business hour shifts that overlap midnight. For example, to express a shift that runs from 5:00 PM to 2:00 AM the next morning, enter “12:00 AM - 2:00 AM, 5:00 PM - 12:00 AM” for each work day.

1 To define holidays, click the Holidays tab.



1 Click **Add** to add a new holiday. Click **Edit** to edit an existing one.



1 Enter the **Holiday date**.

1 Choose if this is an **All day holiday** or **Partial day holiday**. For a partial day holiday, enter:

- **Work hours begin at.** Starting time for work on the holiday.
- **Work hours end at.** Ending time for work on the holiday.

2 Click **OK**.

3 Click **OK** to close the System Settings dialog box.

Setting up e-mail notification

Wave can automatically send an e-mail to a user whenever he or she receives a new voice message, and send the voice message audio file as an attachment to the e-mail.

Once you enable e-mail notification for the system, you must configure each user appropriately.

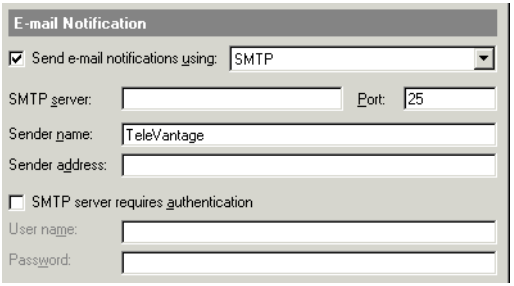
Enabling e-mail notification

To enable e-mail notification for the system, do the following:

1 Choose **Tools > System Settings**, then choose the E-mail Notification tab.

2 To enable e-mail notification, check **Send e-mail notifications using**. Select SMTP from the dropdown list.

Fill in the SMTP settings fields with information provided by your e-mail administrator or Internet Service Provider.



3 Click **OK**.

E-mail notification of voice messages will be available the next time the Wave ISM is started.

Configuring users for e-mail notification

For information on setting up e-mail notification for a user, see “Setting e-mail notification” on page 11-22.

Enforcing strong password security

Password security is crucial in preventing your company from being victimized by toll fraud. Unauthorized users who gain privileged access to your telephone system can place outbound long distance or international calls that get charged to you. In 99.9% of cases, access is gained through insecure (easy-to-guess) passwords. By making your passwords more secure, you can dramatically increase the security of your Wave system against toll fraud. For more information about making your system secure, see Appendix A.

To enforce strong password security on your system:

1. Choose **Tools > System Settings**. The System Settings dialog box opens.
2. Choose the Security tab.
3. Use the following options to safeguard your Wave system against unauthorized access:
   - **Passwords automatically expire after __ days.** Checking this option forces users to regularly change their passwords. Enter the number of days that each user may keep a password before the system requires them to change it to something new.

     You can override this setting for individual users, to permit passwords that never expire. You can also manually force a user to change his or her password whenever you want. See “The Security tab” on page 11-38.
   - **Automatically lock out accounts after __ failed logon attempts.** If checked, the system *locks out* an account after the number of consecutive failed logon attempts that you enter. A locked-out account cannot log on to the system, even with the correct username and password, until the administrator unlocks it.

     To have the system automatically reopen locked-out accounts after a certain time has elapsed, check **Automatically clear lockout after __ minutes**, and enter the number of minutes.

     You can also manually reopen a locked-out account, as follows:
     - **User.** In the Users view, double-click the user to open the Users dialog box, click the Other tab, uncheck **User is locked out**, and click **OK**.
     - **Queue.** In the Queues view, double-click the queue to open the Queue dialog box, click the Account tab, uncheck **Queue is locked out**, and click **OK**.

- **Hang up trunks after __ failed logon attempts.** If checked, the system hangs up on any incoming caller who tries to log on to a Wave account with an invalid password after the number of consecutive attempts that you enter.

4 Choose the Security \ Permitted Passwords tab.

By forbidding easy-to-guess passwords, you can make your system much more secure from unauthorized access. Vertical highly recommends checking all the options on this tab to prevent toll fraud.

When you change any of the options on this tab, users whose passwords are now prohibited will be prompted to change them the next time they log on, and will show up in the Security Analysis report (see Appendix A).

5 Use the following options to restrict the passwords that users can choose:

- **Minimum password length.** Enter the minimum number of digits for a password. For secure passwords, the minimum should be at least five, and preferably seven or more digits.
- **Prevent passwords that contain an account's extension.** Passwords that contain the extension number are especially easy to guess. Check this option to prevent the extension from being any part of the password. For example, a user at extension 337 could not have a password of 337, 33755, or 13378080.
- **Prevent passwords that contain entries from the following list.** Check to prevent passwords from containing any of the digit strings in the list. Wave provides by default a list of easy-to-guess digit strings.

  To add a new digit string to the list, click **Add**. To edit a digit string in the list, select it and click **Edit**. To remove a digit string from the list, select it and click **Delete**.

6 Click **OK**.

Setting up personal call supervision defaults

You can set system defaults for whether users' personal calls can be Monitored, Coached, or Joined using the Supervise commands. When you create a new user, these defaults are used to define if users' personal calls can be supervised, and you can override the defaults for individual users (see "Configuring whether the user's calls can be supervised" on page 11-39.

Notes

- When you change a system default, users who have that Supervise permission set to "System Default" change to reflect the new default.
- Whether or not a user can *use* the Supervise commands is controlled by permissions. See "Assigning a user's permissions" on page 11-40.

To change personal call supervision defaults

1 Choose **Tools > System Settings.** The System Settings dialog box opens.

2 Choose the Security tab.

3 In each of the following fields choose "Yes" or "No":

- **Personal calls can be monitored.** Users with the "Allow monitoring user calls" permission can listen to users' personal (not queue) calls without the monitored user knowing.
- **Personal calls can be coached.** Users with the "Allow coaching user calls" permission can add themselves to users' personal (not queue) calls and be heard by the coached user, but not by the caller.
- **Personal calls can be joined.** Users with the "Allow joining user calls" permission can add themselves to users' personal (not queue) calls as full participants.

4 Click **OK**.

For instructions on using the Monitor, Coach, and Join features, see Chapter 12 of *Vertical Wave User's Guide*. For information on configuring a user for the permissions needed to Coach, Monitor or Join another user's personal calls, see "Assigning a user's permissions" on page 11-40. For information on supervising queue calls, see the *Vertical Wave Contact Center Administrator's Guide*.

Configuring Analog and Digital Trunks

CHAPTER CONTENTS

This chapter provides information about configuring analog and digital trunks. Before you can configure Vertical Wave to process calls, connect to the Internet, or connect your LAN, you must complete the following tasks:

- Creating new trunk groups, if the default groups do not meet your needs
- Configuring trunks and channels

Note: Before you configure trunk groups, trunks, and channels, be sure you understand the concepts presented in Chapter 26, Understanding Vertical Wave Trunks.

Creating new trunk groups

Before you can configure analog and digital trunks and put them in trunk groups, those trunk groups must exist. Wave provides default trunk groups (see Table 26-2, on page 6) that you can use to quickly group a set of analog or digital channels for most call routing scenarios.(You will configure these trunk groups later, in Chapter 8, Configuring Inbound Call Routing.) If necessary, you can create additional trunk groups using the procedure in this section.

The following procedure specifies how to create, name, and set the direction and hunt order for a new trunk group. Later in the configuration process, you will configure Caller ID settings on the Out tab (see Chapter 18, PBX Feature Configuration) and configure the In tab (see Chapter 8, Configuring Inbound Call Routing).

Note: The Wave system has a maximum of 20 groups, including hunt groups, trunk groups, and zone paging groups.

Hint: You might wish to rename the default trunk groups to be more meaningful to your business or call-routing scenarios, for example, Connect to PBX, Long Distance Calls, or ISDN.

To create, name, and specify a direction for a new trunk group:

1 If necessary, click the Administration tab of the Management Console.

Click 

2 Click the Trunk Groups icon, located in the Trunk Administration section.

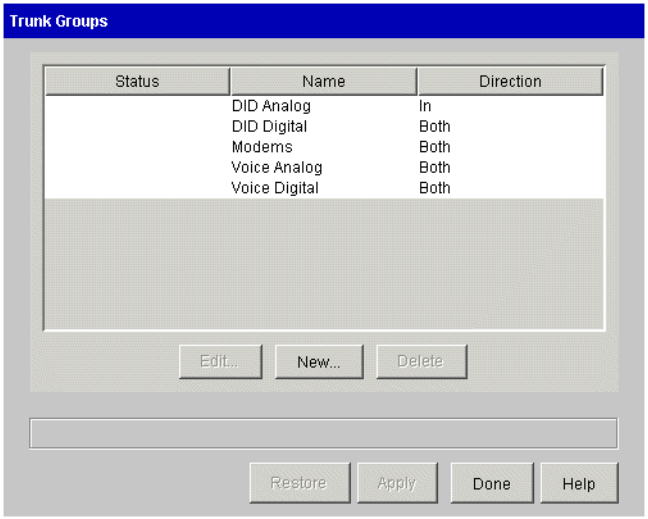


Figure 5-1 Trunk Groups applet

3 Click New to open the Trunk Group dialog box.

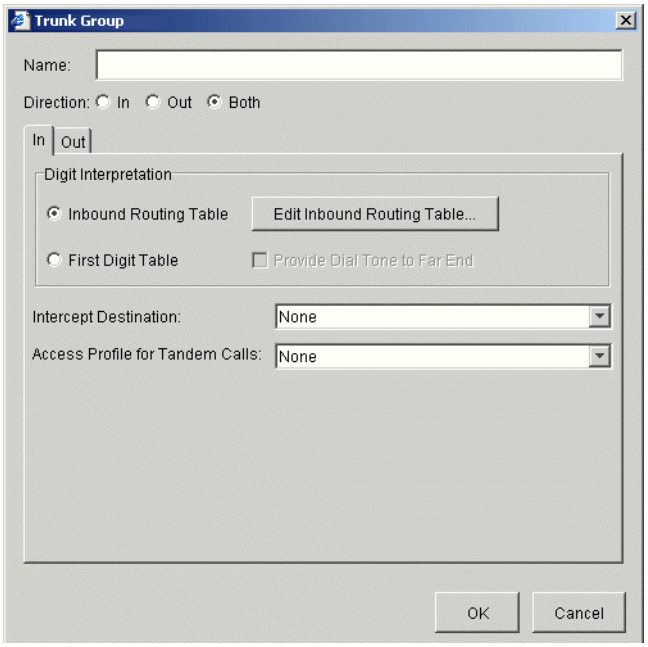


Figure 5-2 Trunk Group dialog, showing In tab

4 In the Name field, enter a name or phrase for the new trunk group, using up to 16 alphanumeric characters.

The name for your new trunk group must be unique. This trunk group name will appear on caller ID telephones when a caller receives calls through this trunk group and no caller ID was received.

5 Select In, Out, or Both to specify the direction of the trunk group.

Your Service Confirmation Letter should detail the direction of the trunks you have installed. Refer to it to determine which direction to select.

Note: Different service providers may use varying terminology for trunk direction for voice circuits. The following terms are synonymous:

- In, inbound (with respect to Wave)
- Out, outbound (with respect to Wave)
- Both, bidirectional, two-way, 2-way, in and out

6 Click the Out radio button to bring the Out tab forward.

7 Select Linear or Circular in the Hunt Group group box.

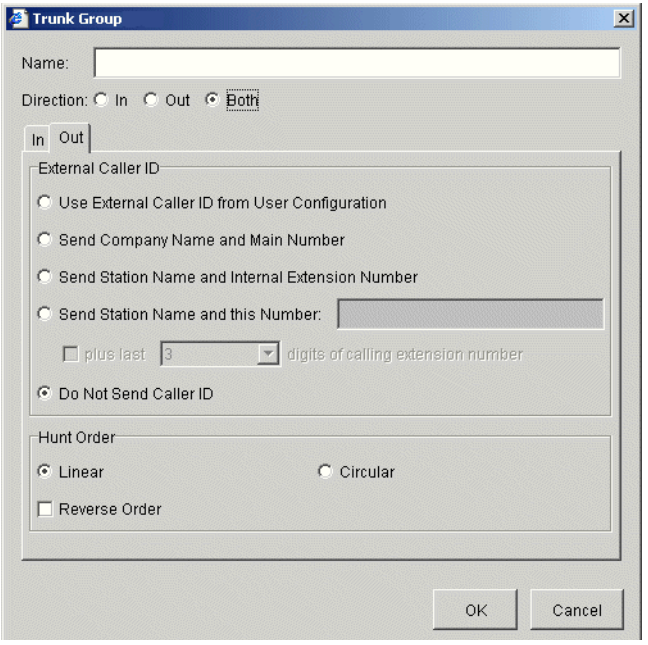


Figure 5-3 Trunk Group dialog, showing Out tab

- Linear—Looks for a free channel, always starting at the beginning of the list of trunk groups and searching to the end, or—for reverse-order hunting—always starting at the end of the list and searching to the beginning.
- Circular—Looks for a free channel, starting where the last search left off. From this point (where the last search left off), forward-order hunting works forward through the list of available channels, and reverse-order hunting works backward through the list.

For more information about hunt types, see “Trunk group hunt types” on page 7.

8 Select Reverse Order if appropriate.

9 Click OK to save your changes and close the Trunk Group dialog box.

10 Click Done to close the Trunk Groups applet and return to the Management Console.

Configuring trunks and channels

You use the Trunk Configuration applet to set up the handshake and signaling between the Wave ISM and the equipment on the service provider end of the trunk. Using this applet, you can set the configuration options to match the settings your trunk service provider has provisioned on your trunks.

Hint: Locate your service confirmation letters or provisioning information forms before starting the following procedures (see Chapter 35, Service Confirmation Letters and Provisioning Information Forms, for more information about these forms).

Caution: *The trunk options and the channel/trunk signaling options must be set identically to the settings shown on your trunk Service Confirmation Letter.*

Caution: *Never mix trunk types within a trunk group. If necessary, create a new trunk group (see "Creating new trunk groups" on page 1).*

Trunk and channel settings

Both digital channels and analog trunks have three major configuration parameters. These parameters are described in Table 5-1.

Table 5-1 Digital channel and analog trunk parameters

Parameter Name	Description
Enabled	Places a T-1 or analog channel or trunk into service or removes it from service.
Signaling	Sets the signaling method for the channel or trunk.
Trunk group (for voice or modem channels)	Sets the trunk group membership for the analog trunks or digital channels. For example, you can assign a trunk group called Voice Analog to eight separate analog trunks.

Configuring analog trunks

You use the Trunk Configuration applet to configure analog trunk settings for the analog trunk ports on the Integrated Services Card, or for the additional ports on the Integrated Services Card with expansion board or any eight-port analog trunk module (e.g., the Analog DID Trunk Module or the Analog Universal Module). Refer to your

Service Confirmation Letter, provided by your service provider, for the appropriate values to set.

The Integrated Services Card (ISC) in slot 6 provides 3 loop start analog trunks. If your Wave ISM has a Integrated Services Card with expansion board occupying slots 5 and 6, it has an additional 11 analog trunks, 3 of which are loop start only and 8 of which are loop / ground start.

Note: Before configuring the trunks, configure the trunk groups you want to assign to the analog trunks. For information about configuring trunk groups, see "Creating new trunk groups" on page 1.

Caution: *If you need to remove an analog trunk module from your Wave ISM, you must first assign all ports of the module to* ***None*** *in the* ***Trunk Group*** *drop-down list in the Trunk Configuration applet. For details about this drop-down list, see step 4 of "Configuring analog channels" on page 8.*

Complete the following tasks to configure analog trunks:

- Configuring analog trunk card or module settings
- Configuring analog channels

Configuring analog trunk card or module settings

To configure the analog trunk card or module settings:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Trunk Configuration icon, located in the Trunk Administration section.

3 Select the card or module you want to configure, then select the Trunk in Service check box.

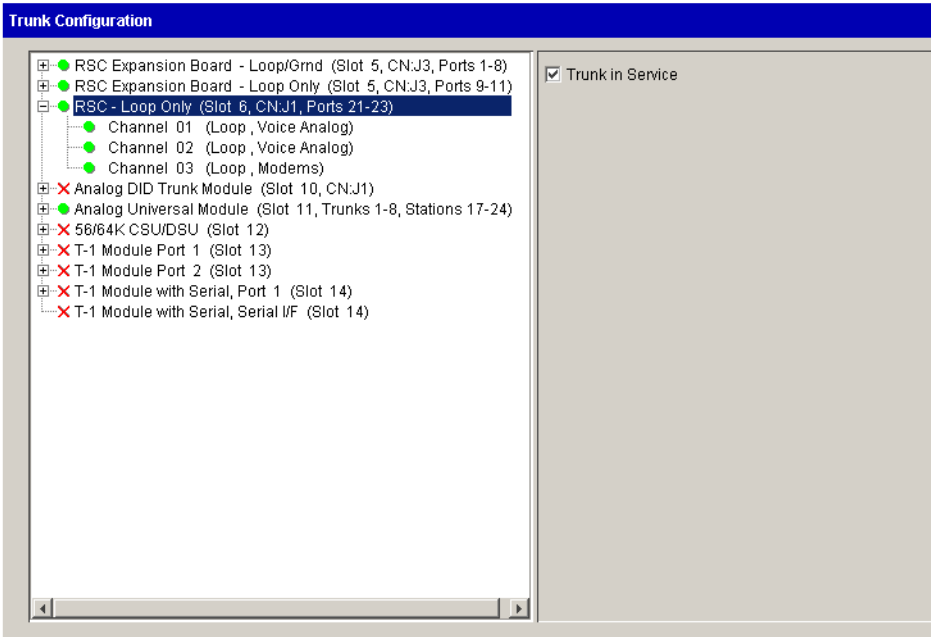


Figure 5-4 Trunk Configuration applet, showing analog module settings

If your Wave ISM only has a Integrated Services Card and no other analog trunk modules, there is only one entry in the list: Integrated Services Card - Loop Only (Slot 6).

Refer to the *Vertical Wave IP 2500 Hardware Reference Guide* for information about each card and module installed in your Wave ISM.

4 Configure the card or module's analog trunks or ports, which are labeled channels (see "Configuring analog channels" on page 8).

5 Click Apply to save your changes.

6 Click Done to return to the Management Console.

Configuring analog channels

To configure a card or module's analog channels:

1 Click the + next to a card or module to display the channels, and select the channels you want to configure.

- To select a contiguous range of channels, select the first channel in the range, then hold down the Shift key while you select the last channel in the range.
- To select a noncontiguous range of channels, hold down the Ctrl key while you select each channel.

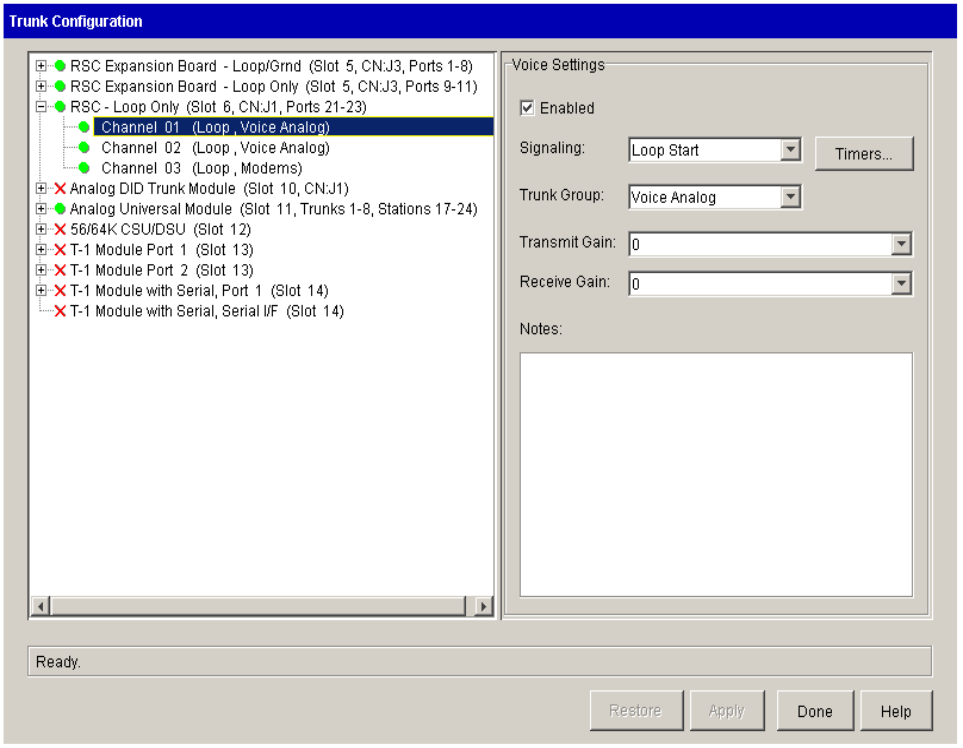


Figure 5-5 Trunk Configuration applet, showing analog channel settings

2 Be sure that the channels are enabled; the Enabled check box should be selected.

3 Select the signaling method from the Signaling drop-down list.

The signaling method is indicated on your service confirmation letter. See Chapter 35, Service Confirmation Letters and Provisioning Information Forms, for more information.

The signaling methods are as follows:

- Loop Start—If you are configuring the analog trunks on the Integrated Services Card (ISC), you must choose Loop Start. If you have an RS3A-C, the three analog trunks in Slot 6 are Loop Start and the other eight analog trunks in Slot 5 can be configured as Loop Start or Ground Start.
- Ground Start—This option is available only for the analog universal module, the analog trunk module, and the eight analog trunks on the RS3A-C (which can also be configured for Loop Start).
- Wink Start—If you are configuring the analog DID or AUM module, you must choose Wink Start.

Caution: *Do not adjust the **Timers** settings unless you are an expert.*

4 Select the trunk group you want to assign to the selected trunks from the Trunk Group drop-down list.

Note: When you configure analog DID trunk modules, only trunk groups configured for the inbound direction will appear in the Trunk Group drop-down list; trunk groups set for both directions will not appear.

5 Adjust the Transmit Gain and Receive Gain values if necessary.

- Transmit Gain—If the voice level of outgoing calls is too low, increase the value; if the voice level is too high, decrease the value.
- Receive Gain—If the voice level of incoming calls is too low, increase the receive gain; if the voice level is too high, decrease the value.

Caution: *Feedback can result if you set the gain level too high. In most cases, the default value of 0 should be fine.*

6 Record information in the Notes field.

This information could include circuit-specific information or other information from the Trunk Configuration property sheet. Circuit number and carrier information or brief notes regarding issues encountered can be entered in this comment field. Field personnel can use this data to locate and identify the physical circuit connected to the Wave ISM.

7 Click Apply to save your changes.

8 Click Done to return to the Management Console.

Configuring digital trunks and channels

Use the Trunk Configuration applet to assign voice, data, or ISDN traffic to digital channels; to configure connection settings for a digital channel on WAN modules or cards (for example, the two-port T-1 module); and to assign each channel to a connection.

Caution: *If you need to remove a T-1 module from the Wave ISM, you must first assign all channels of the module to* ***None*** *in the* ***Connection*** *drop-down list in the Trunk Configuration applet. For details about this drop-down list, see "Configuring digital trunk card or module settings," step 3.*

Complete the following tasks to configure digital trunks:

- Configuring digital trunk card or module settings
- Configuring digital channels
- Configuring digital channels for voice
- Configuring digital channels for data
- Configuring digital channels for ISDN
- Assigning digital channels to a serial interface

Configuring digital trunk card or module settings

To configure the digital trunk card or module settings:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Trunk Configuration icon, located in the Trunk Administration section.

3 Select the card or module you want to configure, and check the Trunk In Service check box.

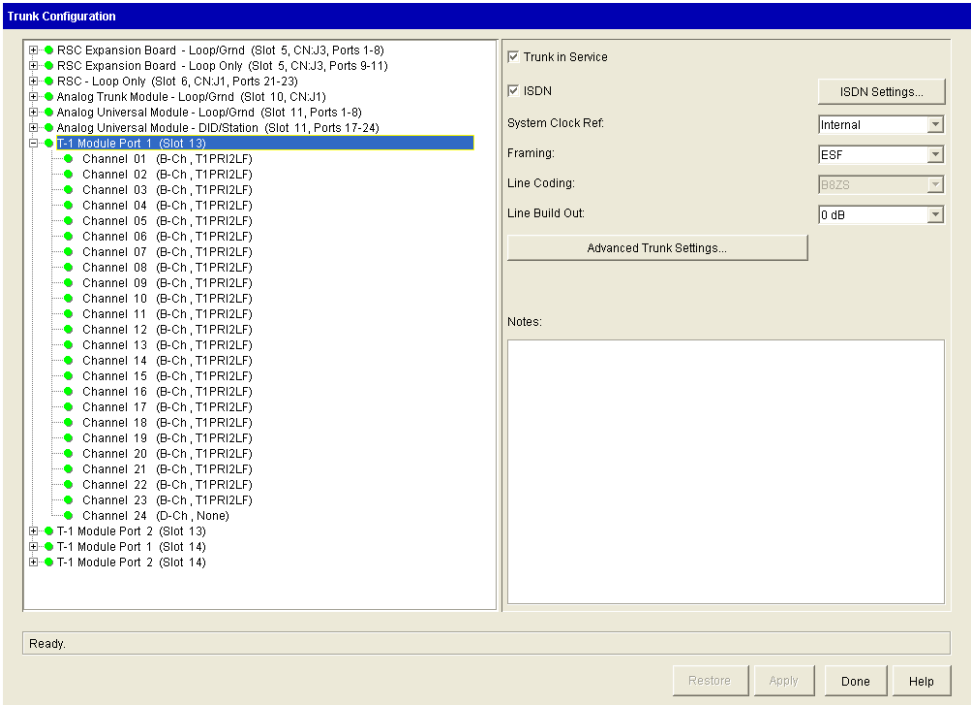


Figure 5-6 Trunk Configuration applet, showing T-1 module settings

Note: If you want to configure a module for cross-connection to a serial interface, Be sure that you select the module labeled with Serial.

4 If the trunk is ISDN, check the ISDN check box, and click ISDN Settings to configure the ISDN trunk settings as follows:

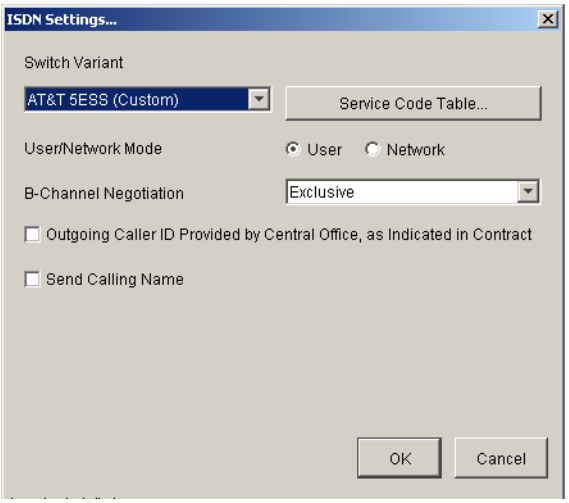


Figure 5-7 ISDN Settings dialog

Note: If you do not select the ISDN check box, the trunk will be a CAS (Channel Associated Signaling) T-1 trunk, which implies robbed-bit signaling or clear channel for data. Clear channels (whether ISDN or CAS) must be assigned to data connections, and channels grouped for data connections must be contiguous. All other channel types, like B channels, must be assigned to voice trunk groups. If you configure ISDN to use a voice trunk group, you can configure that ISDN connection for dial-up data; see "Configuring dial-up routing" on page 22-1.

a Select a variant in the Switch Variant drop-down list.

Refer to your T-1 Service Confirmation Letter to determine which of the following ISDN switch variants to use:

- AT&T 5ESS (Custom)
- AT&T 4ESS
- NT DMS-100 (NI-1)
- AT&T 4ESS (NI-2)
- NT DMS-100 / S-100

Select the NT DMS-100 /S-100 variant when connecting to a Northern Telecom Meridian DMS-100 PBX configured with a subtype profile of S-100. In this scenario, the DMS-100 must be configured as the network side. Wave is always the user side.

b Click Service Code Table to modify the service code table for the switch variant that you specified in the previous step.

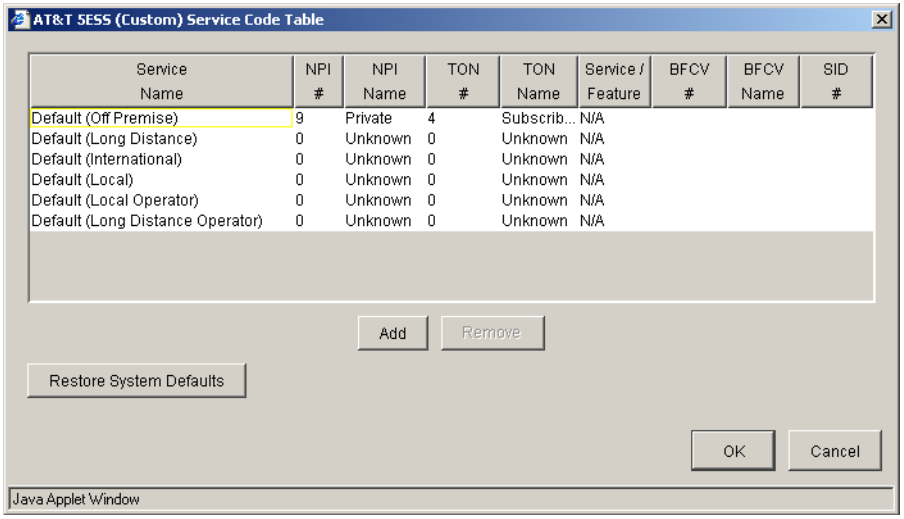


Figure 5-8 Service code table for the ATT 4ESS switch variant

Note: You do not need to modify the service code table during initial configuration. The defaults should be sufficient for connecting to a local exchange carrier.

c If your ISDN trunks support multiple services, click Add to add new service name records to the service code table, then modify the new records by clicking in each field to open a text field or a drop-down list.

Note: The new entries in the service code table appear as ISDN Setting options in the outbound routing tables. You will configure the outbound routing tables in “Configuring outbound routing tables” on page 9-13. You can select these settings on a call-by-call basis.

You can modify the following fields for new entries and existing entries:

- Service Name—A text string, such as OUTWATS, FX, TIE, VNET
- NPI #—Numbering Plan Identifier, 0 through 15

0 = unknown, the network has no knowledge of the numbering plan so it uses the NANP.

1 = ISDN / telephony number plan. Enter the name `E.164` in the NPI Name field.

9 = private numbering plan (private network)

- NPI Name—A text string describing the Numbering Plan Identifier; typically E.164, Unknown, or Private
- TON #—Type of Number

  There can only be four different types of entries:

  0 = unknown

  1 = international number

  2 = national number

  4 = subscriber number
- TON Name—A text string describing the Type of Number; typically National, International, or Unknown
- Service / Feature—Service vs. Feature. Typically left N / A unless the provider states that it should be either Service or Feature.
- If you select Service or Feature, you need to configure the next three settings:

  BFCV #—Binary Facility Coding Value, 0 through 31

  A number for the service must be entered in the BFCV field. The provider provides this number. The number can be from 0 through 31.

  Some common Service IDs:

  1 = SDN (including GSDN) ..... in / out

  2 = Toll free MEGACOM ..... in

  3 = MEGACOM ..... out

  6 = ACCUNET Switched Digital Service ..... in / out

  7 = Long Distance Service ..... in / out

  8 = International Toll Free Service ..... in

  10 = ATT MultiQuest ..... in

  17 = Call Redirection Service ..... in

  BFCV Name—A text string describing the BFCV value

  SID #—Service Identifier, 0 through 127. Used primarily by Bell Canada.

If you are not sure of your changes, click Restore System Defaults to restore your changes to the system defaults.

d Select the appropriate mode.

- User—This is the typical setting, unless you are connecting two Wave ISMs together.
- Network—Use this setting if you are connecting two Wave ISMs together. In this case, one Wave ISM must be set to User and the other set to Network.

Caution: *Do not modify these settings unless you are an expert.*

e Select the Outgoing Caller ID Provided by Central Office check box if your contract specifies that the central office will provide caller ID.

In this case, the central office will typically provide the ISDN trunk's billing number as caller ID for all outgoing calls.

To configure ISDN channel settings, see "Configuring digital channels for ISDN" on page 5-21.

f Check the Send Calling Name check box if you want Wave to send the name specified in the General Settings applet when calls are sent over this trunk.

5 Specify the system clock reference in the System Clock Ref drop-down list.

Available options are:

- Internal—The selected T-1 trunk will not be a clock reference source for the Wave ISM, rather, the selected T-1 will act as a clock reference for the equipment connected to the T-1 trunk. This is useful if the Wave ISM is to be master clock to another Wave ISM or internal device. In this case, the other device should be configured as External.
- External Primary—The Wave ISM gets its primary clock reference from the selected T-1 trunk. Use this for a T-1 trunk connecting to the PSTN. Only one trunk can be primary.
- External Secondary—If the primary T-1 trunk fails, the Wave ISM will get its primary clock reference from the secondary T-1. Only one trunk can be secondary.

Note: If you configure one trunk as secondary, the other trunk must be primary. If you have only one T-1 connection between your Wave ISM and the PSTN, that connection must be the primary one. If you have two T-1s connected, the connection you are using for voice must be the primary one, and the other (typically set for data use) is secondary.

6 Set the following fields using the information on your T-1 Service Confirmation Letter.

- Framing—ESF (Extended Super Frame) or SF / D4 (Super Frame - D4). ISDN PRI is generally ESF.
- Line Coding—B8ZS (Bipolar 8 Zero Substitution) or AMI (Alternate Mark Inversion). ISDN PRI is B8ZS; AMI is not supported for ISDN.
- Line Build Out—0 dB, -7.5 dB, -15 dB, and -22.5 dB are available if DSX mode is selected in Advanced Trunk Settings. Otherwise, in CSU mode, 0, -7.5, and -15 are available. (For details about line build out settings, see "Line Build Out settings" on page 33-1)

7 Record information in the Notes field.

This information could include circuit specific information or other information from the Trunk Configuration property sheet. Circuit number and carrier information or brief notes regarding issues encountered can be entered in this comment field. Field personnel can use this data to locate and identify the physical circuit connected to the Wave ISM.

8 Configure the digital channels (see "Configuring digital channels" on page 5-17).

9 Click Apply to save your changes.

10 Click Done to return to the Management Console.

Configuring digital channels

1 Display the card or module channels, and select the channels you want to configure.

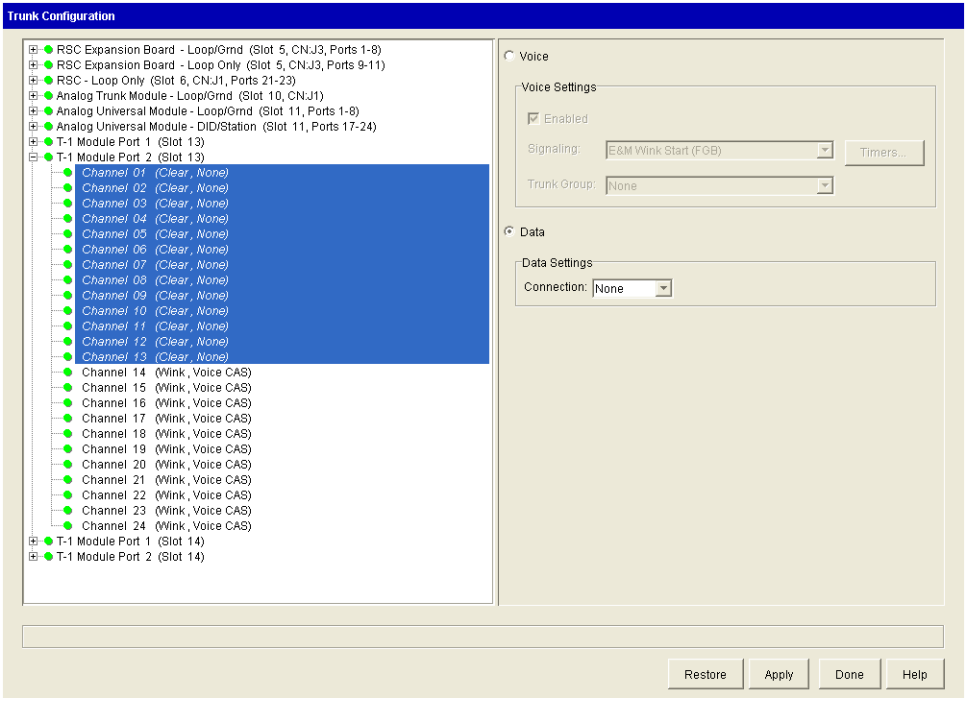


Figure 5-9 Trunk Configuration applet, showing channel settings

Note: If you checked the ISDN check box in step 4, you will see channel settings for ISDN and data. If you did not check the ISDN check box, you will see channel settings for voice and data.

2 Select Voice or Data, or if you selected ISDN in “Configuring digital trunk card or module settings” step 4, select ISDN or Data.

3 Configure the appropriate settings based on the channel type.

- For voice channels, complete “Configuring digital channels for voice” on page 5-18.
- For data channels, complete “Configuring digital channels for data” on page 5-20.

- To assign channels to a serial interface, complete “Assigning digital channels to a serial interface” on page 5-22.

Note: For ISDN channels, Channel 24 is automatically set to D-Ch, None.

4 Click Apply to save your changes.

5 Click Done to return to the Management Console.

Configuring digital channels for voice

1 Be sure that the channels are enabled; the Enabled check box should be checked.

2 Select the signaling method from the Signaling drop-down list.

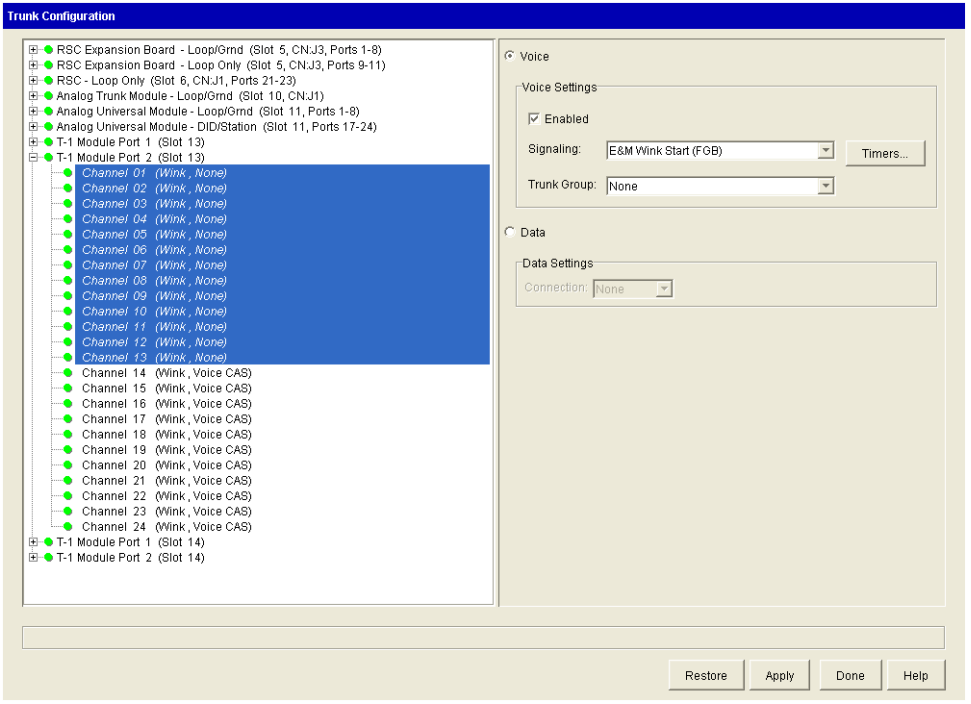


Figure 5-10 Trunk Configuration applet, showing voice settings

Caution: *Do not set **Timers** settings unless you are an expert.*

For T-1 voice channels, E&M Wink Start (FGP), E&M Immediate Start, or Ground Start are valid options.

If you have a fractional T-1 trunk, be sure all voice channels that are not in service on your trunk have the Enabled check box unchecked.

Note: If you chose the ISDN trunk type when you configured the T-1 module settings, Wave automatically sets the Signaling fields for channels 1 through 23 to B-channel; channel 24 is automatically set to D-channel.

3 Specify the Trunk Group for the selected channels.

One or more channels can be assigned to a particular voice trunk group. For example, if your trunk has 12 (1-12) DID 2-way voice channels, you can assign the Digital DID trunk group to channels 1 through 12.

Note: Trunk groups can be named in any way you like. You might want to rename your trunk groups to be more meaningful to you (see the Hint in “Creating new trunk groups” on page 5-1).

For more information about trunk groups and how they are used, refer to “Trunk groups” on page 26-4.

4 Click Apply to save your changes.

5 Click Done to return to the Management Console.

Configuring digital channels for data

1 Specify the Connection for the selected channels.

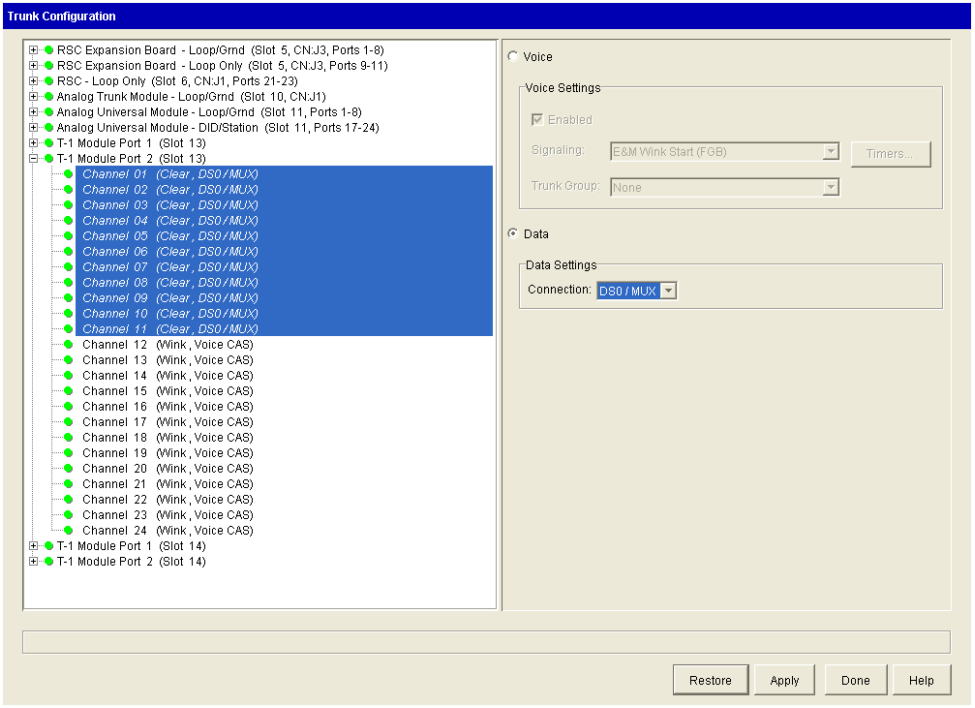


Figure 5-11 Trunk Configuration applet, showing data settings

One or more channels can be assigned to a particular data connection. For example, if your trunk has 12 (13-24) data channels, you can assign the DS0/Mux connection to channels 13 through 24.

Note: Channels assigned to the same digital connection or DS0/Mux trunk group must be contiguous.

You can select from the following connections to transport data between the Wave ISM and the WAN:

- None
- DS0/Mux

If you are configuring your T-1 trunk to be a T-1 / DS0 multiplexor, choose the T-1 / DS0 Mux connection for the channels you want to multiplex. You must also assign the same number of channels to T-1 / DS0 Mux on the other T-1 port.

Note: When a channel is set to T-1 / DS0 Mux, the trunk is automatically enabled.

2 Click Apply to save your changes.

3 Click Done to return to the Management Console.

Configuring digital channels for ISDN

Note: For information about configuring an ISDN data connection for dial-up, see "Configuring dial-up routing" on page 22-1. The information in this section also applies to ISDN PRI.

1 Ensure that the Enabled check box is checked.

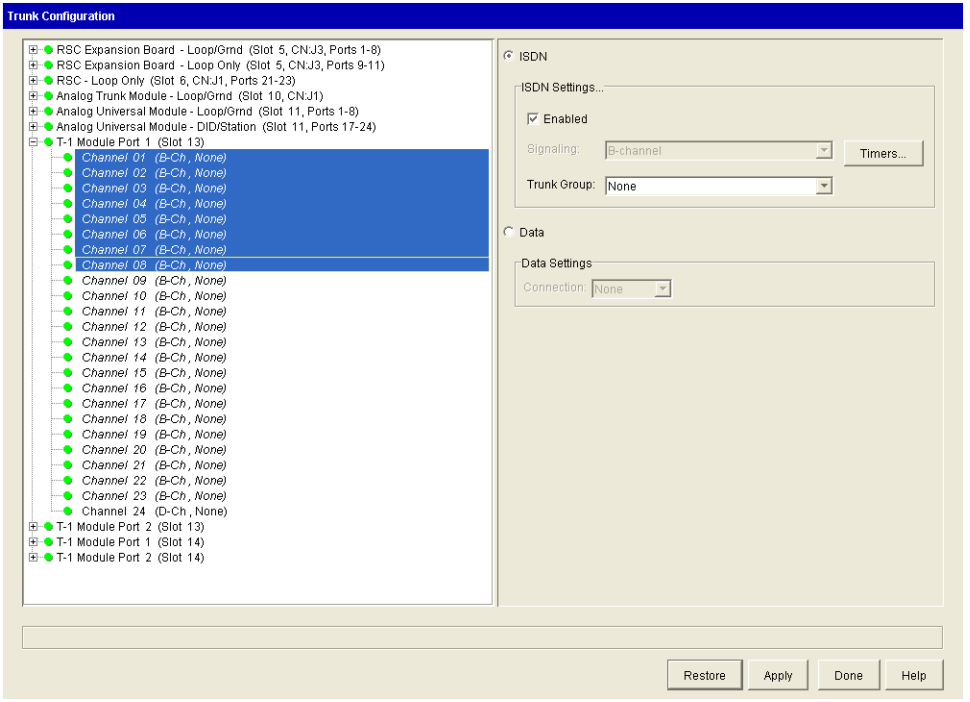


Figure 5-12 Trunk Configuration applet, showing ISDN settings

2 Select a Trunk Group from the drop-down list.

3 Click Apply to save your changes.

4 Click Done to return to the Management Console.

Assigning digital channels to a serial interface

1 Select the Data option.

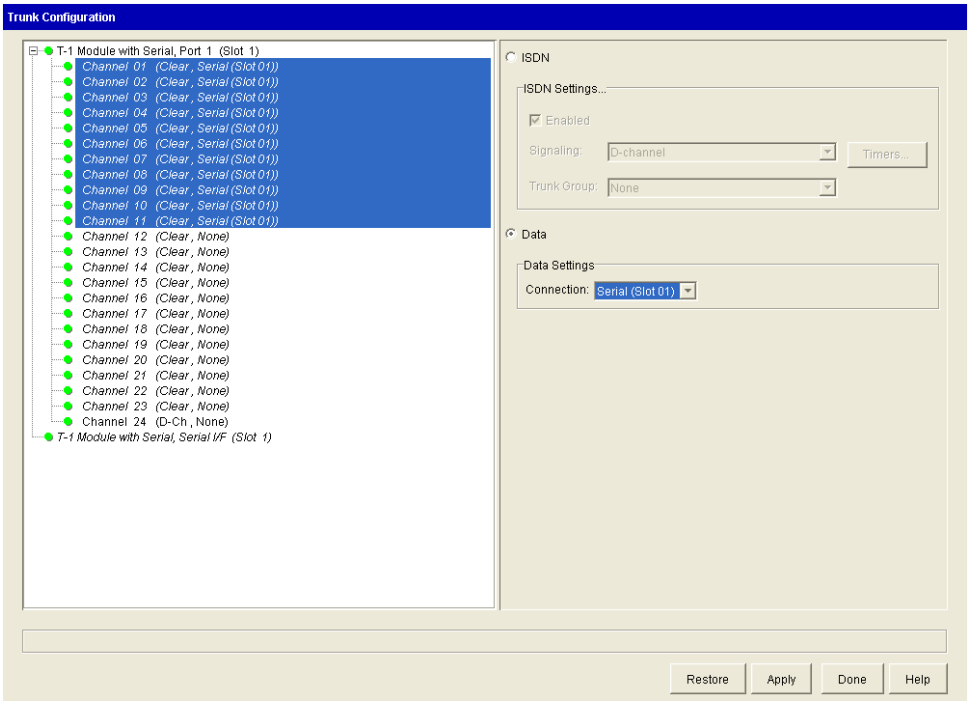


Figure 5-13 Trunk Configuration applet, showing data settings assigned to serial interface

Hint: Unlike other data channels, you can select and configure *non-contiguous* channels for the serial interface.

2 Select the Serial connection from the Connection drop-down list.

3 Click Apply to save your changes.

4 Click Done to return to the Management Console.

Typically, assigning channels to the serial connection is all you need to do. You might want to ensure that your serial interface's configuration is correct, or make some changes to it, if your connection is not working. For more information, see "Ensuring that your T-1 serial interface is set correctly" on page 14-1.

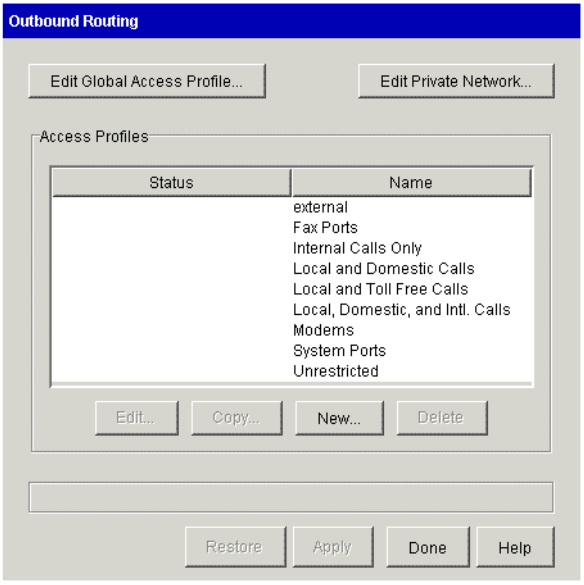
Enabling paging and notification on PRI trunks

If your system uses PRI trunks, you must make the following configuration changes for external paging and call notifications to work on those trunks.

1 If necessary, click the Administration tab of the Management Console.

Click 

2 Click the Outbound Routing icon, located in the Trunk Administration section.



3 Select the **System Ports** access profile and click **Edit**. The Access Profile dialog box opens.

4 Click the **Destination Access Codes** tab.

5 Check the **Permission Allowed** box for all access codes that are being used for users' paging and call notifications.

6 Click **OK**, then **Done**.

For information on setting up users' paging and call notification, see "The Voicemail \ Notification tabs" on page 11-20.

IP Telephony Configuration

CHAPTER CONTENTS

This chapter describes how to configure the IP telephony features available on the Wave system.

Allocating IP telephony resources

You must have a SIP trunking license before configuring trunks.

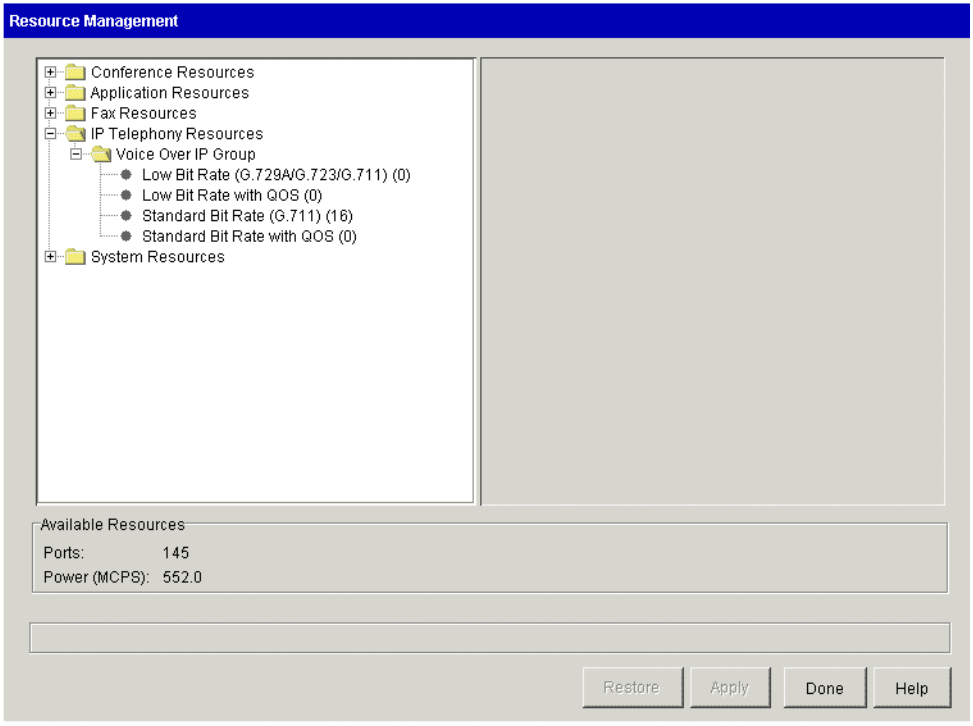
Before you configure your system for IP telephony, you must allocate Digital Signal Processor (DSP) resources that are required for each IP telephony channel. For more information about the DSP resources required for Wave IP telephony, refer to “DSP resources and licensing for IP telephony resources” on page 27-4.

To allocate IP telephony resources:

1. If necessary, click the Administration tab of the Management Console.
2. Click the Resource Management icon, located in the PBX Administration section

Click

3. Expand the IP Telephony Resources folder.
4. Expand the Voice Over IP Group folder, and select the G.729A / G.711 codec.



Resource Management applet, showing IP Telephony Resources

5 Select the appropriate number of available IP telephony resources in the drop-down list (on the right side of the applet).

6 Click Apply to save your changes, and return to the Management Console.

Configuring site-to-site call routing for IP telephony

Configure call routing in order to use Signaling Control Points for the following outbound call routing scenarios:

- Automatic route selection
- Off-premise extensions
- Destination access codes

See Chapter 9 for information about configuring outbound call routing.

To configure call routing for IP call destinations you will need to do the following procedures:

- Enabling IP telephony trunk signaling protocols
- Configuring Signaling Control Points
- Configuring default inbound IP call routing
- Including Signaling Control Points in the outbound call routing configuration

Enabling IP telephony trunk signaling protocols

To enable IP telephony trunk signaling protocols:

1 If necessary, click the Administration tab of the Management Console.

Click 

2 Click the IP Telephony icon, located in the PBX Administration section.

3 Click **SIP** in the left pane.

4 Check the **SIP Enabled** checkbox.

5 Select the **SIP Local IP Address** from the drop-down list.

Note: Clicking **Advanced** opens a dialog box where you can adjust various advanced SIP parameters. You should not modify the defaults in this dialog box unless instructed to do so by Vertical technical support.

6 Click **Apply** to save your changes.

Configuring Signaling Control Points

Configure Signaling Control Points to determine how to handle IP calls to and from specific IP addresses.

To configure Signaling Control Points:

Click 

1 In the IP Telephony applet select Signaling Control Points from the Call Routing folder.

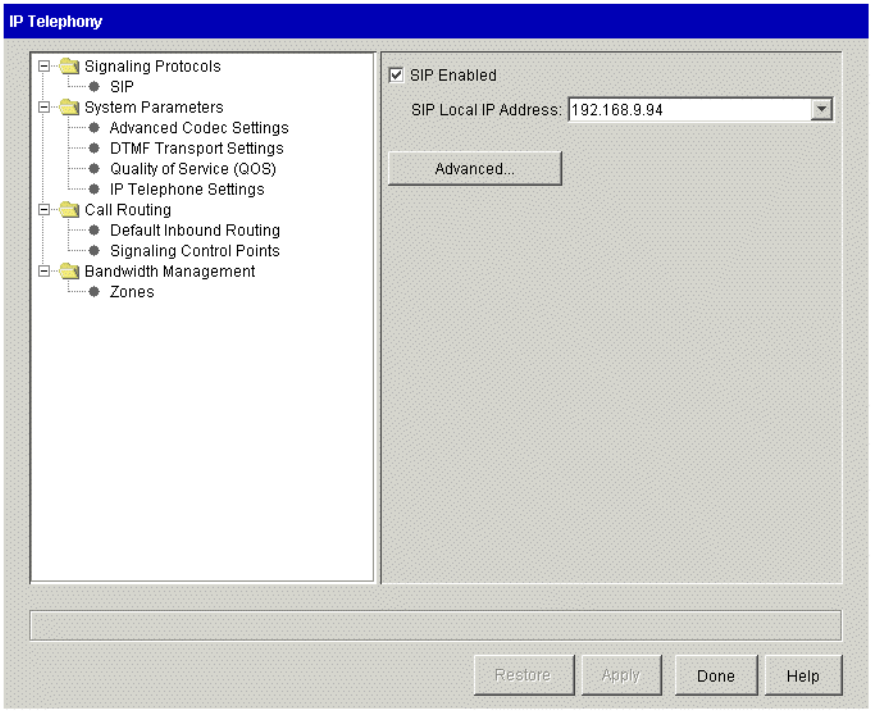


Figure 6-1 IP Telephony applet, Signaling Control Point configuration

2 Click New to add a new destination, or select an existing destination to edit, then click Edit.

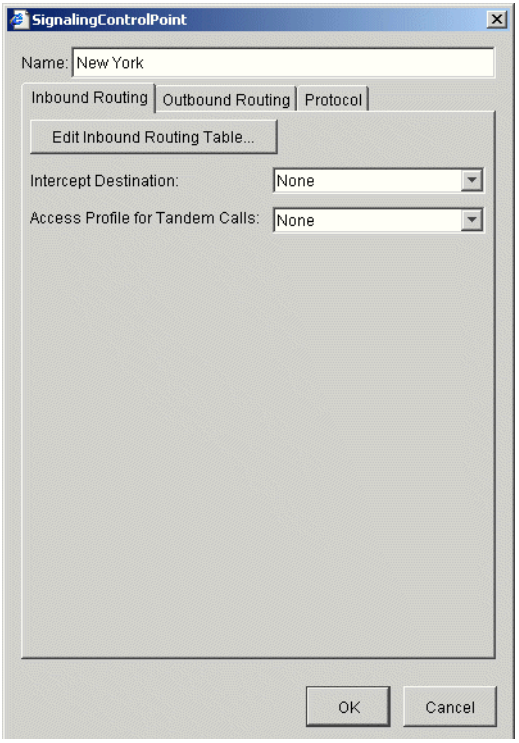


Figure 6-2 Signaling Control Point dialog

3 Enter a Name.

When you configure outbound call routing, this name will appear as IP, a vertical bar (|), and the name you enter here. For example, if you enter New York, it will be displayed as IP | New York in your outbound call routing configuration. See "Including Signaling Control Points in the outbound call routing configuration" on page 6-11 for more information.

Note: The Name field accepts alphanumeric characters as well as the following special characters:

` ~ ! # $ % & * ( ) - = + | { } ; : " , . / < > ?

4 Configure the settings for handling calls received from this Signaling Control Point on the Inbound Routing tab.

You can find information about configuring the Inbound Routing Table, Intercept Destination, and Access Profile for Tandem Calls in Chapter 9.

5 Choose one of the caller ID formats for sending caller ID with calls to this Signaling Control Point in the Outbound Routing tab.

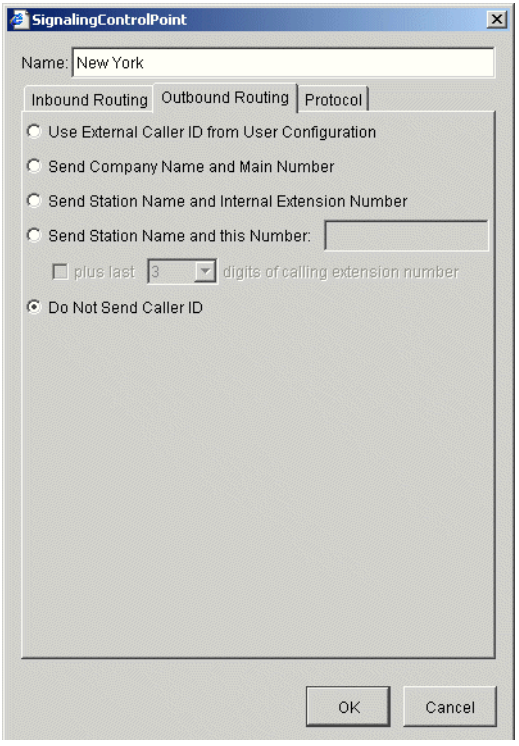


Figure 6-3 Signaling Control Point Outbound Routing settings.

Select the SIP protocol, then enter the IP address of the destination SIP endpoint in the Destination Address field, and enter the port number in the Port field. The default SIP port number is 5060.

Note: The default port value is 1720. This port is generally used for IP telephony, but, if your system configuration requires, you can specify another port.

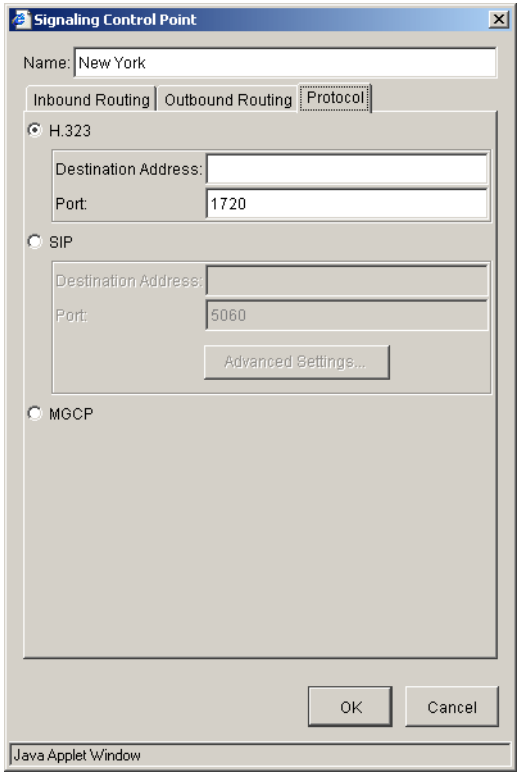


Figure 6-4 Signaling Control Point Protocol settings

6 If the SIP endpoint (usually third party SIP servers) requires authentication, or registration, click **Advanced Settings**. Do the following:

- If the remote SIP endpoint requires Authentication, check **Authentication Required**, then enter the authentication credentials (user name, authentication name, and password) provided by the remote SIP endpoint administrator. You may then need to configure each Vertical SIP Telephone on your system with the same authentication credentials.
- If the remote SIP endpoint requires Registration, then check **Registration Required** and enter the SIP Registrar address and port number provided by the remote SIP endpoint administrator.

7 Click OK to add the Signaling Control Point to the table.

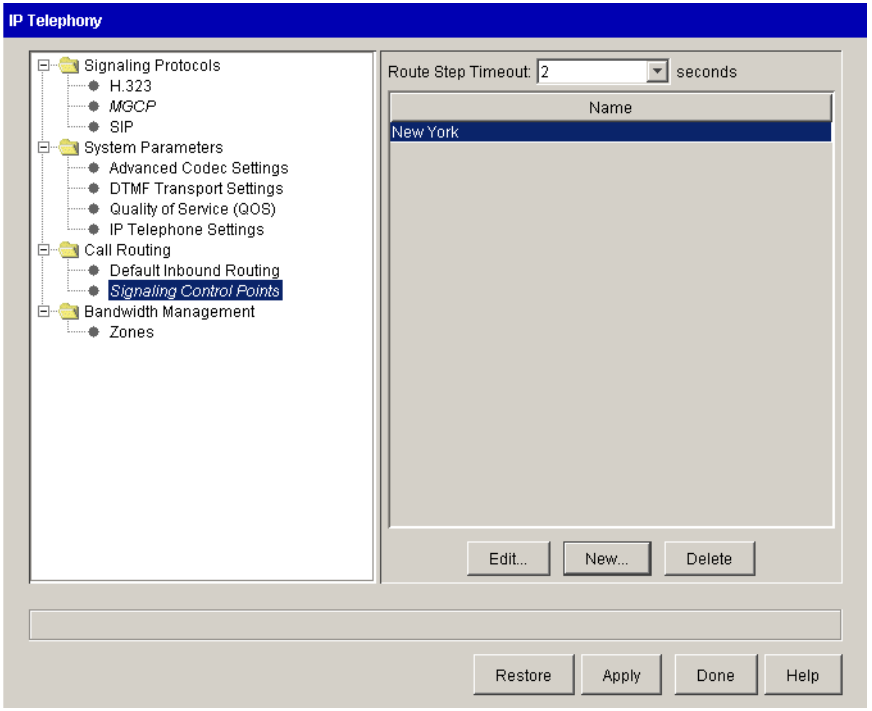


Figure 6-5 Signaling Control Point table

8 Click Apply to save your changes.

Setting the route step timeout

You can adjust the amount of time that a Signaling Control Point step in an outbound routing table is given to operate before the system tries the next step in the table.

To set the Signaling Control Point route step timeout:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the IP Telephony icon, located in the PBX Administration section.

3 Select Signaling Control Points from the Call Routing folder.

4 In the Route Step Timeout drop-down list, select the number of seconds before the system times out and tries the next step in an outbound call routing table.

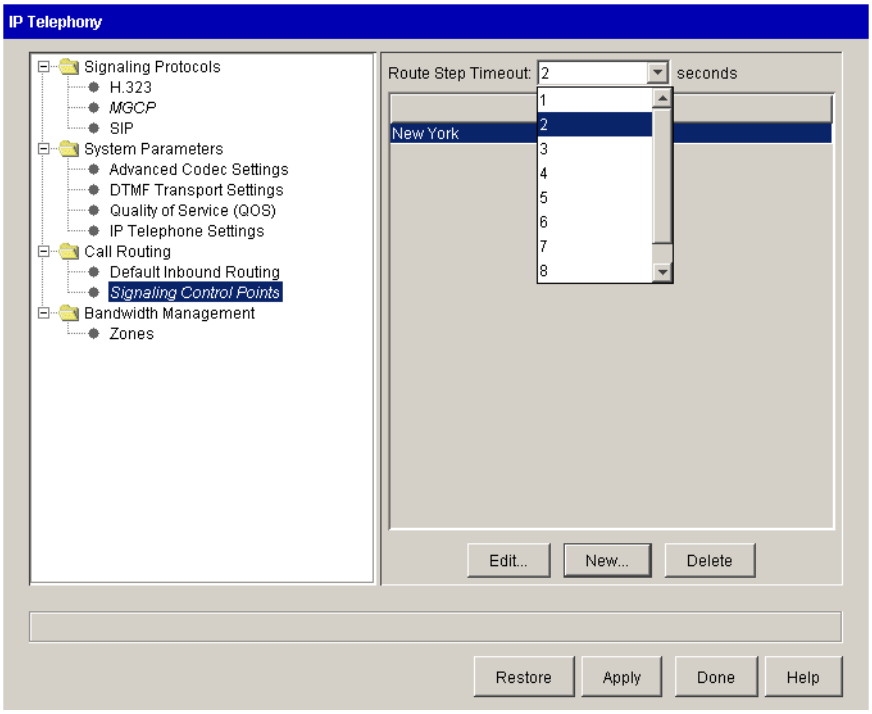


Figure 6-6 Selecting the Signaling Control Point route step timeout

Configuring default inbound IP call routing

To specify how to route incoming IP calls from unknown sources (that is, sources that are not included in your list of Signaling Control Points), configure the call handling rules with the default inbound call routing settings.

To configure default inbound IP call routing:

Click 

1 In the IP Telephony applet select Default Inbound Routing from the Call Routing folder.

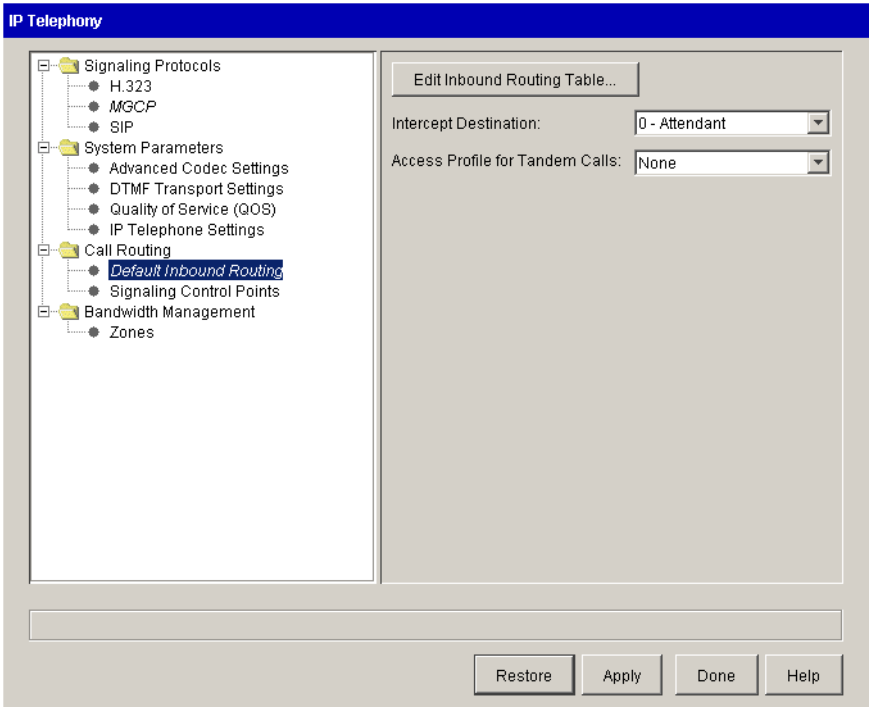


Figure 6-7 IP Telephony applet, default inbound routing configuration

2 Click Edit Inbound Routing Table to specify the call sources, schedules, and routing.

For detailed information about configuring inbound routing, refer to the *Wave Administrator's Guide*, Chapter 8, Configuring Inbound Call Routing.

Note: If you want to route all incoming calls as received, there is no need to edit the inbound routing table. Only edit the inbound routing table if you want to route by schedule or do inbound digit translation.

3 Choose an extension from the Intercept Destination drop-down list.

4 Select an access profile in the Access Profile for Tandem Calls drop-down list.

5 Click Apply to save your changes.

Including Signaling Control Points in the outbound call routing configuration

To route outbound calls to IP call destinations, select Signaling Control Points instead of trunk groups in your outbound call routing configuration.

To include Signaling Control Points in outbound call routing:

While you are configuring your outbound call routing, select a Signaling Control Point from the destination drop-down list at the point when a trunk group might be selected.

For example:

Configuring an outbound routing table in the Outbound Routing applet:

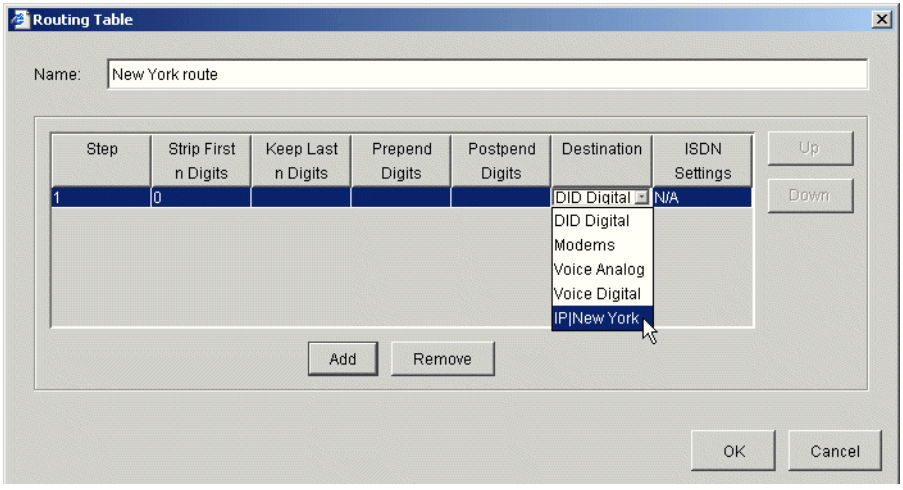


Figure 6-8 Selecting a Signaling Control Point is an outbound routing table

Configuring the External digit in the First Digit Table:

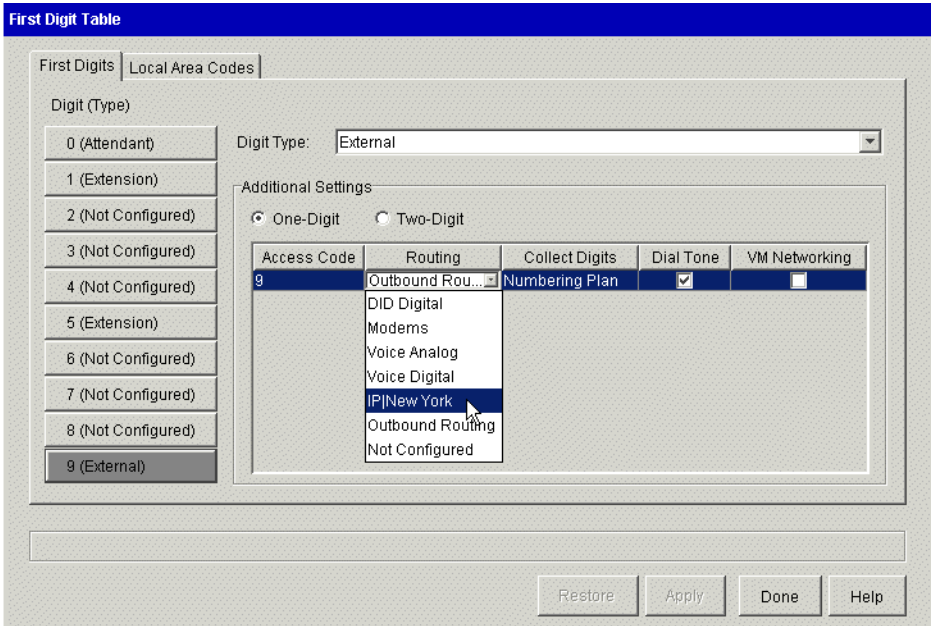


Figure 6-9 Selecting a Signaling Control Point in an External digit configuration

Configuring IP telephones

This section provides instructions on configuring the desktop, wireless and software IP telephones certified for use with the Wave system. The procedures assume you are already familiar with configuring Wave digital telephones, and only address the steps specific to configuring IP telephone options.

IP telephones require the ability to log into and download files from the Wave FTP or TFTP server. Any network configurations that do not allow that connectivity will result in the IP telephones being unable to initialize. These configuration areas include, but are not limited to, the following:

- incomplete routing
- external firewalls
- internal firewalls, such as Check Point FireWall-1

- RRAS address / port filtering
- TFTP / FTP directory security

Configuring IP telephone extensions

This procedure assumes you are already familiar with configuring Wave telephone extensions, and only addresses configuration tasks specific to configuring IP telephone extensions.

To configure IP telephone extensions:

1. If necessary, click the Administration tab of the Management Console.
2. Click the User / Workgroup Management icon, located in the PBX Administration section. The User / Workgroup Management applet opens, with the Users view showing.

Click

3. Double-click the user you want to edit. The User dialog box opens.
4. If you are configuring the extension for a Vertical SIP telephone, select the **Telephone MAC Address** field but leave the field blank.
5. Choose the appropriate **Telephone type** from the drop-down list.

Configuring a Vertical SIP Telephone

Vertical SIP telephones are configured in a manner similar to digital telephones (see Chapter 10). The following section contains advanced configuration information specific to SIP telephones.

Vertical SIP telephone advanced configuration

Be sure to have the documentation included with the Vertical SIP Telephone on hand as a reference for this procedure. Configuring a Vertical SIP Telephone is a multi-part process as follows:

Customizing the configuration files

SIP Telephone Setup

Customizing the configuration files

Each Vertical SIP Telephone needs two phone configuration files available on the Wave:

- A common configuration file which all Vertical SIP Telephones use called aastra.cfg. This file needs to be customized for your Wave system.
- A configuration file that is unique to the individual SIP Telephone. A default configuration file called [Aastra_MAC].cfg needs to be modified for each specific phone and then saved with the following naming convention: MAC_address_of_SIP_Telephone.cfg.

Both files are in the following location in your Wave system:

C:\Inetpub\tftproot

These files will be configured by remotely accessing the Wave desktop from the Management Console. The following procedures will guide you in customizing these two files.

Customizing aastra.cfg

Follow the procedures below to configure the aastra.cfg file.

1. If necessary, log on to your Wave system.
2. Click the Wave Desktop in the Management Console.
3. Click OK when the warning dialog appears.
4. Enter your Wave user name and password, and click OK.

   The Wave desktop appears
5. Click on the Start menu and Navigate to the following application:

   Start > All Programs > Accessories > Notepad
6. Click File then Open.
7. Navigate to C:\Inetpub\tftproot
8. Select “All Files” in the “File of type” option list.
9. Select aastra.cfg and click Open.
10. Make the changes specified in “aastra.cfg Configuration Parameters” on page 15.

11 Save the file.

12 Close Notepad and log off the Wave desktop to return to the Management Console.

aastra.cfg Configuration Parameters

Edit the file by making changes to the fields in each of the following sections. Refer to the Vertical SIP Telephone's administrator guide for specific details regarding each of the fields in these sections.

TFTP Server Section

- tftp server: <IP address of your Wave>

SIP Registrar and Proxy Server Settings Section

- sip proxy ip: <IP address of your Wave>
- sip registrar ip: <IP address of your Wave>

Time Server Settings Section

- time server1: <IP address of your Wave>

DNS Section

- dns1: <IP address of the DNS server on the same network as the Wave>
- dns2: <IP address of an alternate DNS server on the same network as the Wave>

Soft Keys Section

You can define default soft keys in this section for all phones with soft keys. This section has four lines for each key that needs to be configured as follows:

- softkey1 type: see "Vertical SIP Telephone Feature Configuration" on page 19
- softkey1 label: user defined, contained in quotes (e.g. "DND")
- softkey1 value: see "Vertical SIP Telephone Feature Configuration" on page 6-19
- softkey1 states: see "Vertical SIP Telephone Feature Configuration" on page 6-19

Programmable Keys Section

You can define default programmable keys in this section for all phones with programmable keys. This section has four lines for each key that need to be configured as follows:

- prgkey1 type: see “Vertical SIP Telephone Feature Configuration” on page 19
- prgkey1 label: user defined, contained in quotes (e.g. “DND”)
- prgkey1 value: see “Vertical SIP Telephone Feature Configuration” on page 6-19
- prgkey1 states: see “Vertical SIP Telephone Feature Configuration” on page 6-19

Customizing [Aastra_MAC].cfg

Follow the procedures below to configure the [Aastra_MAC].cfg file.

1. If necessary, log on to your Wave system.
2. Click the Wave Desktop in the Management Console.
3. Click OK when the warning dialog appears.
4. Enter your Wave user name and password, and click OK.

   The Wave desktop appears
5. Click on the Start menu and Navigate to the following application:

   Start > All Programs > Accessories > Notepad
6. Click File then Open.
7. Navigate to C:\Inetpub\tftproot
8. Select “All Files” in the “File of type” option list.
9. Select [Aastra_MAC].cfg and click Open.
10. Make the changes specified in “[Aastra_MAC].cfg Configuration Parameters” on page 17.
11. Save the file using the following naming convention: mac_address.cfg

    Note: mac_address is the actual MAC address of the SIP telephone (e.g. 00085d03576c.cfg). The MAC address for a phone can be found on a label on the bottom of the phone.

    To save the file under this unique name:

a. Click File then Save As.

b. In the file name field, enter the MAC address of the SIP telephone followed by ".cfg" and click Save.

12. Close Notepad and log off the Wave desktop to return to the Management Console.

[Aastra_MAC].cfg Configuration Parameters

Edit the file by making changes to the following fields. Refer to the Vertical SIP Telephone's administrator guide for specific details regarding each of these fields.

Network Settings

- ip: <IP address of the SIP Telephone>
- subnet mask: <subnet mask of the network used by the Wave>
- default gateway: <default gateway of the network used by the Wave>

Line Keys

You must configure two line keys with the primary extension number for that phone and leave the rest blanks as in the provided Aastra_MAC.cfg file. The second line key is used for call waiting and transfer. Configure these settings as specified below.

Note: The Vertical SIP Telephones are not multi-line phones that support multiple extensions, therefore, the second line key simply serves to support the call waiting and call transfer features for the primary extension.

Note: The extension number and user name used below are the same values configured in User Configuration.

- sip line1 user name: <extension number for SIP Telephone>
- sip line1 display name: <user name for SIP Telephone>
- sip line1 screen name: <user name for SIP Telephone>
- sip line2 user name: <extension number for SIP Telephone>
- sip line2 display name: <user name for SIP Telephone>
- sip line2 screen name: <user name for SIP Telephone>

Soft Keys and Programmable Keys

The default soft keys and programmable keys are defined in the aastra.cfg file. You can override the configuration of these default keys by defining phone specific keys in these sections. Follow the instructions for defining these keys in the aastra.cfg file on page 15 and page 16, but make the changes in these sections instead.

SIP Telephone Setup

After the configuration has been completed on the Wave and the configuration files have been customized on the Wave system, you will need to setup your SIP Telephones.

Use the Vertical SIP Telephone's installation guide included with the Vertical SIP Telephone to assemble and power up the telephone. Additionally, use the included documentation along with the *Vertical SIP Telephone Quick Reference Card* to familiarize yourself with the Vertical SIP Telephone features and keys.

For each phone, you will need to configure the following options so the phone can communicate with the Wave.

1. Press the Options button on the phone and navigate to “Network Settings”. Select this option and enter the administrator password. The default is “22222”.

   Refer to the Vertical SIP Telephone's administrator guide for details on configuring network settings on the Vertical SIP Telephone.
2. Change the DHCP option to “Off”.
3. Enter the IP address for the phone.
4. Enter the subnet mask for the network the SIP telephone is connected to.
5. Enter the gateway IP address for the network the SIP telephone is connected to.
6. Enter in the primary and secondary DNS IP addresses, if applicable.
7. Enter in the IP address for the Wave system for the Primary TFTP server.
8. Restart the phone.

When the phone restarts, it will read the configuration files from the Wave system and the phone will come up with the buttons configured as specified.

Vertical SIP Telephone Feature Configuration

The following table shows the values needed to configure the programmable keys and soft keys in the configuration files. The values in the second, third, and fourth columns need to be used for the key configuration.

Table 6-1 Vertical SIP Telephone Feature Configuration

Feature	Type	Value	State
Call Waiting - Disable	speeddial	*45	idle
Caller ID Blocking	speeddial	*67	idle
Conference	speeddial	!*71	connected
Do Not Disturb	speeddial	*41	idle
Do Not Disturb - Cancel	speeddial	*42	idle
Flash	flash	n/a	n/a
Hold	speeddial	!*54	connected
Retrieve Hold	speeddial	*55#	idle
Message Waiting	speeddial	550	idle
Night Answer - Activate	speeddial	*85	idle
Night Answer - Deactivate	speeddial	*86	idle
System Page	speeddial	*11	idle
Zone Page	speeddial	*12<zone>	idle
Directed Park	speeddial	!*56<ext>	connected
Self Park	speeddial	!*54	connected
Retrieve Park	speeddial	*55<ext>	idle
Retrieve System Park	speeddial	*53<slot>	idle
Group Pickup	speeddial	*74	idle
Extension Pickup	speeddial	*75<ext>	idle

Table 6-1 Vertical SIP Telephone Feature Configuration

Feature	Type	Value	State
Reconnect	speeddial	*72	idle
System Speed Dial	speeddial	*89<index>	idle
Toggle	speeddial	!*73	connected
User Forward	speeddial	*43<dest>	idle
User Forward - Cancel	speeddial	*44	idle

Note: The values inside the <> brackets in the table are optional. These values can either be pre-defined here in the configuration files or the user can enter the value on the phone after pressing the feature button. If the value is pre-defined, the user will not be able to override the default when using the associated feature.

Enabling IP call bandwidth

IP telephones cannot make external telephone calls until the bandwidth is allocated for them. To do this, configure the Home bandwidth management zone in “Configuring the home zone” on page 6-25.

Changing the password for the IPPhone user account

For security reasons, Vertical Communications recommends that you change the password for the IPPhone user account from the default password of Vertical4VoIP!

To change the password for the IPPhone user account:

1. Log on to the Management Console.
2. Open the Password Administration applet.
3. In the Password Administration dialog box, click the IPPhone user account and click **Edit**.
4. Enter the new password in the **Password** and **Confirm Password** fields.
5. Click **OK**.
6. Click **Done**.

Configuring advanced IP telephone settings

The following advanced settings can be configured if required in your installation:

Call Agent Adapter IP address

MAC address cleanup

Call Agent Adapter IP address

If changes are made to the Wave system IP addresses, and one of those changed is the IP address of the interface used by the IP telephones, the telephones may lose communication with the Wave system.

Note: This procedure will restart all of the IP telephones.

To reset the IP Call Agent IP address:

1. If necessary, click the Administration tab of the Remote Management Console.

Click

2. Click the IP Telephony icon, located in the PBX Administration section.
3. Within the System Parameters folder, select the IP Telephone Settings node.

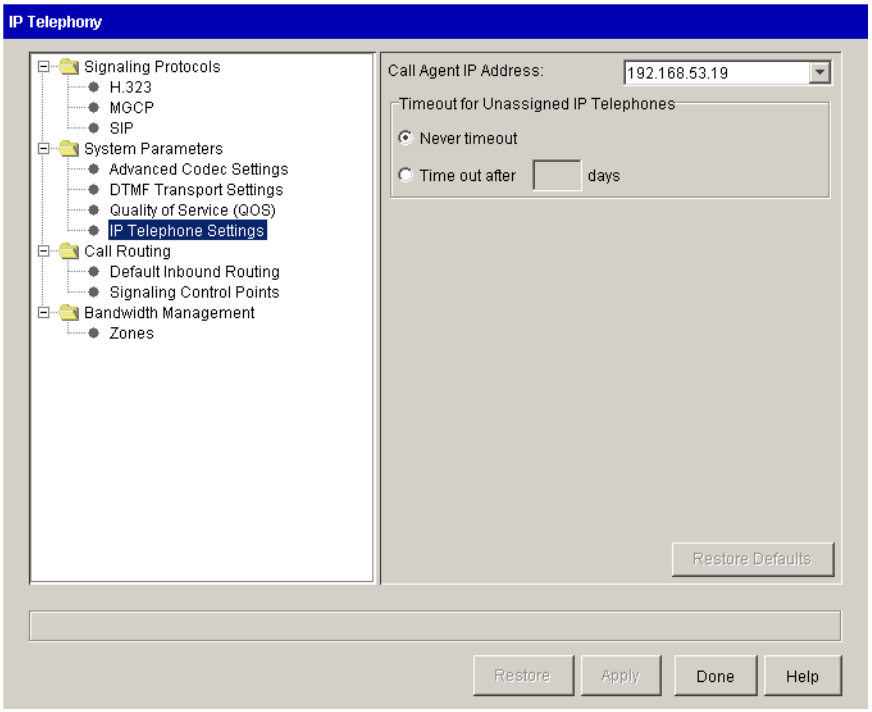


Figure 6-10 IP Telephony applet IP Phone Settings

4 Select the IP address from the Call Agent IP Address drop-down list.

Note: A description of the interface holding the call agent IP address is available in a tooltip on the Call Agent IP Address field.

5 Click Apply to save your changes.

All of the IP telephones will restart automatically after clicking Apply.

MAC address cleanup

The IP telephone MAC address cleanup timeout is a mechanism by which IP telephone MAC addresses that are not associated with an extension in the User Configuration applet can be removed after a period of time.

To set the IP telephone MAC address clean up timeout:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the IP Telephony icon, located in the PBX Administration section.

3 Select the IP Telephone Settings node in the System Parameters folder (see Figure 6-10).

4 Select an IP Phone Timeout option.

- Never time out—Unused IP telephone MAC addresses will never be removed from the drop-down list in the User Configuration applet.
- Time out after *n* days—Unused IP telephone MAC addresses will be removed from the drop-down list in the User Configuration applet after the specified number of days.

5 Click Apply to save your changes.

Configuring bandwidth management zones

Configure the home, remote and default remote zones using the procedures in this section. For information about the bandwidth management zones, refer to “Bandwidth management” on page 27-10.

Zone configuration recommendations

Keep in mind the following rules while configuring zones:

1 A zone is defined by a set of IP address ranges. Any number of Signaling Control Points (SCP) and IP telephones can exist in the same zone. Any SCP or IP telephone whose IP address is not explicitly configured as part of a zone is automatically included in the Default Zone. All TDM devices, including Voice Mail ports and conference bridges reside in the Home Zone.

2 For devices in two different zones to be able to communicate, it is necessary that a common codec is configured in each of the zones’ inter-zone preference lists. In the absence of a common codec, calls between the two zones will not be allowed.

3 Calls between zones always engage the inter-zone rules for both zones.

4 When an IP device is involved in a conference, the inter-zone rules between the IP device's zone and the Home Zone come into play. If there are no common codecs, or there is insufficient bandwidth, then the device is not permitted to participate in the conference.

With these rules in mind, Vertical Communications recommends the following configuration guidelines:

1 Whenever possible, all zones should be configured with both the G.711 codec (either u-law, a-law, or both) and the G.729 codec included in the inter-zone codec preference lists. For zones which prioritize bandwidth over voice quality, the first codec should be G.729 and the second G.711. Conversely, for zones which prioritize voice quality over bandwidth, the first codec should be G.711 and the second G.729. Configuring all zones with both G.711 and G.729 up front will minimize the need to reconfigure them later when new zones are added or bandwidth considerations change.

2 If there is a zone requiring G.729 exclusively, then G.711 should be left off of its inter-zone preference list. In this situation, it is essential that all remaining zones include G.729 on their inter-zone codec preference lists. Devices in zones configured to use G.711 exclusively will not be able to call devices in zones configured to use G.729 exclusively.

Codec negotiation

The Wave chooses a codec based on the following rules:

- It filters out all codecs not supported by both endpoints.
- It scores the remaining codecs based on their positions in the preference lists (for example, if G.711 is first on one list and third on the other, its score is 4).
- The Wave system chooses the codec with the lowest score.
- If two codecs have the same score, the Wave system prioritizes lower bandwidth over voice quality.
- If G.711 Mu-Law and G.711 A-Law tie for the lowest score, the Wave system uses Mu-Law.

Configuring the home zone

To configure the home zone:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the IP Telephony icon, located in the PBX Administration section.

3 Select Zones from the Bandwidth Management folder.

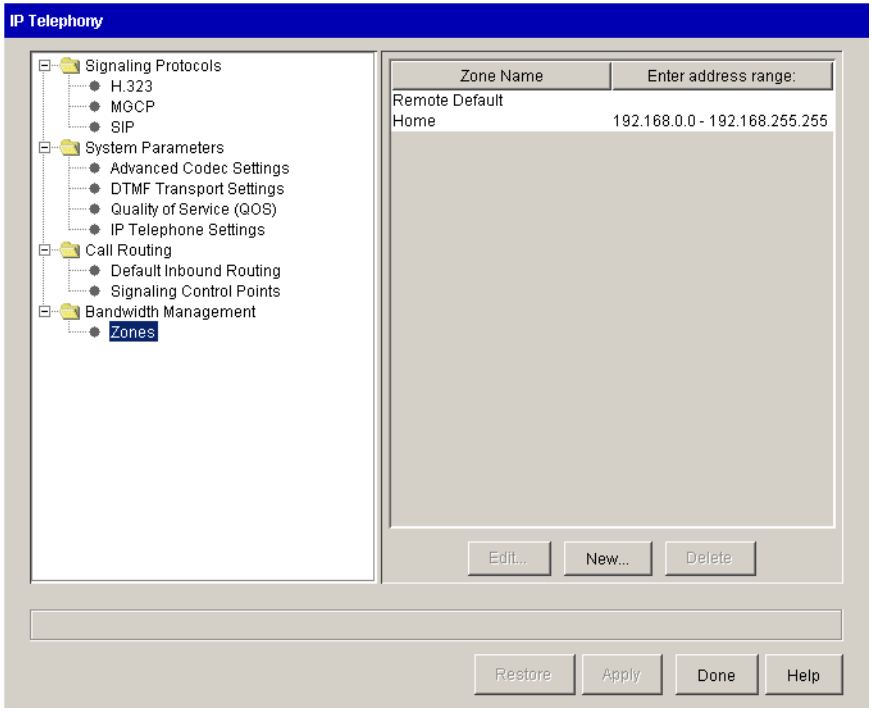


Figure 6-11 IP Telephony applet showing Bandwidth Management zones

4 Select Home from the table, and click Edit.

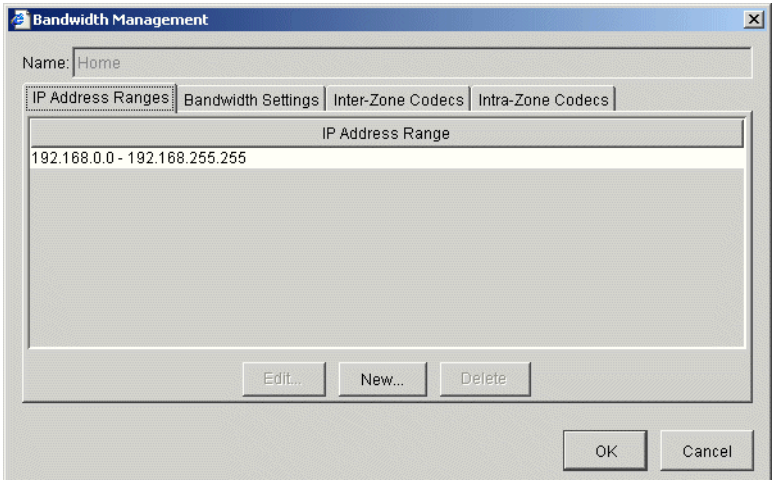


Figure 6-12 Bandwidth Management dialog showing IP address ranges.

5 Configure the IP address range.

Include all the applicable IP address ranges used by the IP telephones on the local Wave system. The Home Zone always includes the IP address of the Wave for bandwidth and call control purposes, whether or not it is explicitly specified in the IP Telephony applet.

To add an IP address range:

a Select the IP Address Ranges tab.

b Select the IP address range and click Edit to alter the existing range, or click New to add a new IP address range.

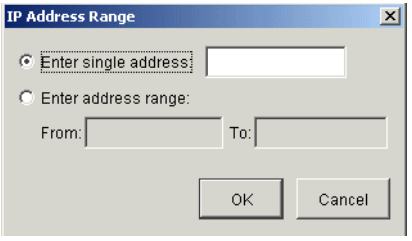


Figure 6-13 Entering a new IP address range or single IP address

You can also add single IP addresses.

6 Configure the bandwidth settings.

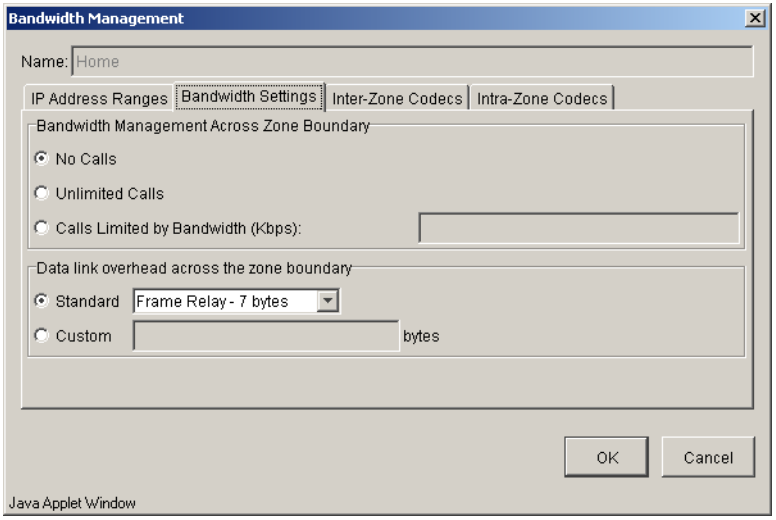


Figure 6-14 Bandwidth Management dialog showing Bandwidth Settings tab

a Select the Bandwidth Settings tab.

b Select a Bandwidth Management Across Zone Boundary setting.

- No Calls—No calls are allowed to IP addresses outside the ranges defined in this zone.
- Unlimited Calls—All calls to or from all IP addresses are allowed.
- Calls Limited by Bandwidth (Kbps)—Calls placed to or received from IP addresses outside this zone are limited to the number that can be supported by the bandwidth specified here.

c Select a Data link overhead across the zone boundary setting.

- Standard—Select one of the standard data links from the drop-down list. The option you select determines the amount of overhead the system adds to the bandwidth when calls cross the zone boundary. Specifying enough overhead is important in preventing too many calls from being placed over the WAN link; if the transport overhead is not included, then more calls would be allowed than the link could support. Be sure to use the option that most accurately reflects the type of data link used in this zone. If you need to use a different value than those provided, enter the value in the Custom bytes field.

- Custom—Enter a custom data link overhead in the field provided.

Note: This helps the Wave system calculate Inter-zone bandwidth availability for IP telephone calls. This setting must be changed if the physical data link type across this zone is changed.

7 Configure the inter-zone codecs.

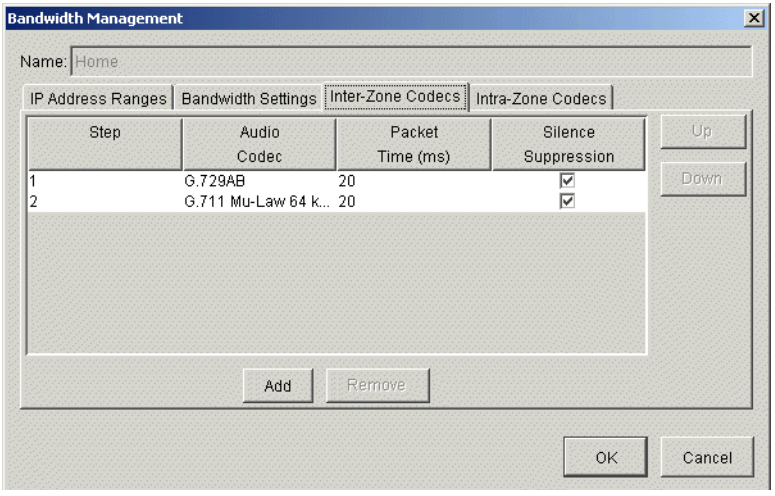


Figure 6-15 Bandwidth Management dialog showing Inter-Zone Codecs tab

a Select the Inter-Zone Codecs tab.

The default codecs are displayed in a table.

b You can edit the default settings, and add and remove records in the table.

- To change the default settings, select any of the table cells. Audio Codec and Packet Time are selected in a drop-down list. Silence Suppression is enabled by checking the check box.
- To add a codec to the list click Add.
- To remove a codec, select a codec in the table and click Remove.

c Click Up or Down to change the order of the codecs.

8 Configure the intra-zone codecs.

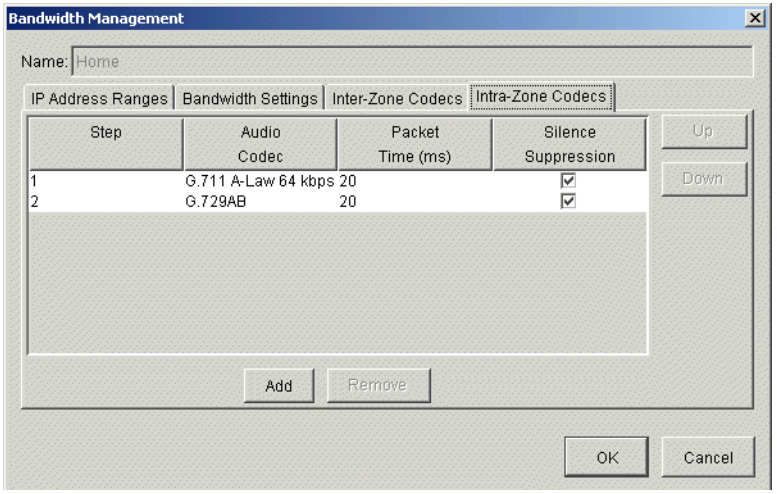


Figure 6-16 Bandwidth Management dialog showing Intra-Zone Codecs tab

a Select the Intra-Zone Codecs tab.

b You can edit the default settings as explained in step 7b.

9 Click OK to close the Bandwidth Management dialog box.

10 Click Apply to save the Home zone configuration.

Configuring remote zones

To configure remote zones:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the IP Telephony icon, located in the PBX Administration section.

3 Select Zones from the Bandwidth Management folder (see Figure 6-11).

4 Click New.

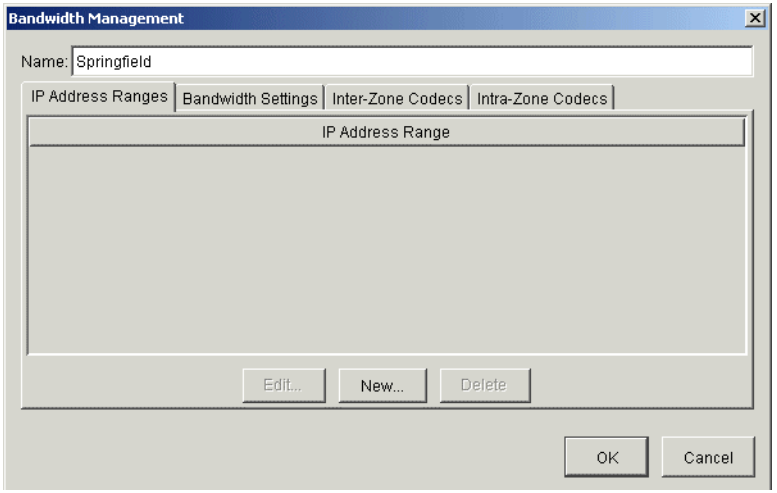


Figure 6-17 Bandwidth Management dialog for a new zone

5 Enter a name for the zone in the Name field.

6 Configure the IP address ranges, bandwidth settings, inter-zone codecs, and intra-zone codecs as explained in “Configuring the home zone” on page 6-25.

7 Click OK to close the Bandwidth Management dialog box.

The new zone appears in the list.

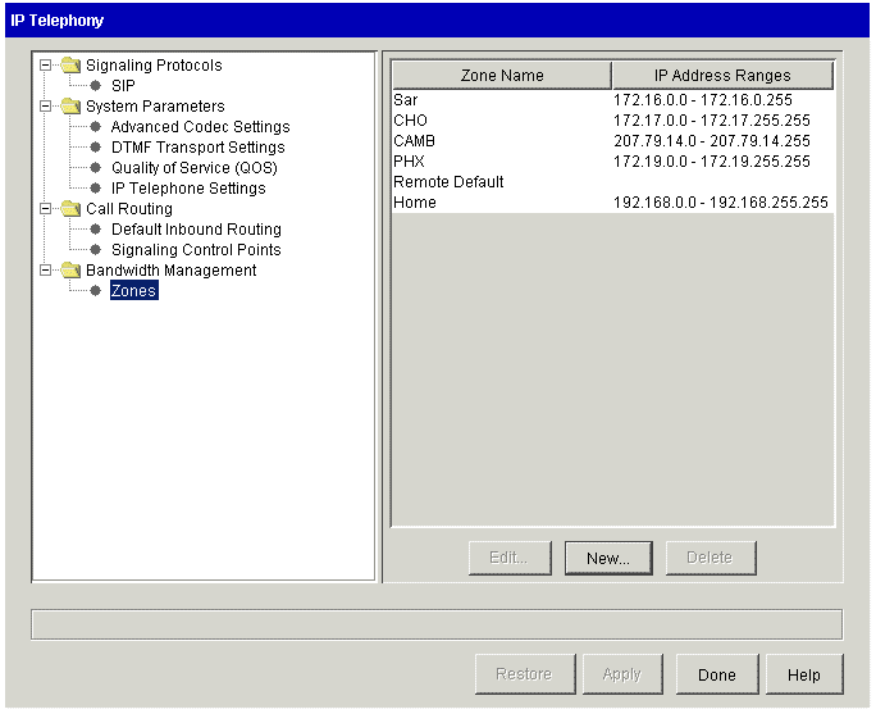


Figure 6-18 New zone shown in Bandwidth Management Zones table

8 Click Apply to save the new remote zone configuration.

Configuring the remote default zone

To configure the remote default zone:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the IP Telephony icon, located in the PBX Administration section.

3 Select Zones from the Bandwidth Management folder (See Figure 6-11).

4 Select Remote Default from the table, and click Edit.

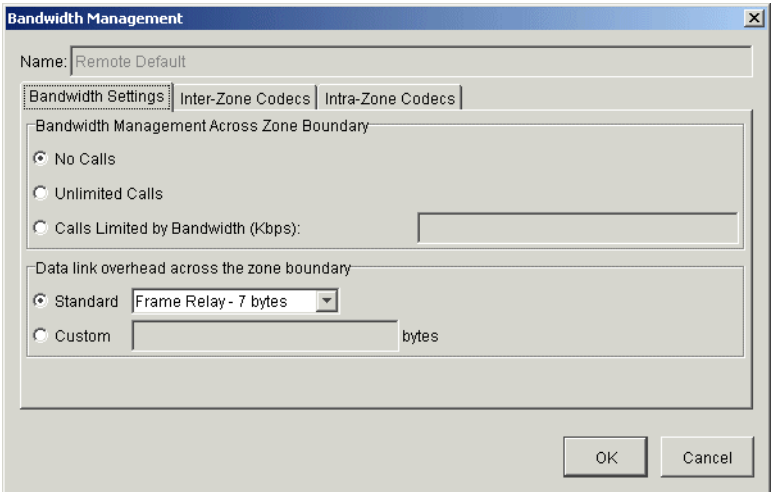


Figure 6-19 Bandwidth Management Remote Default zone dialog

5 Configure the bandwidth settings, inter-zone codecs, and intra-zone codecs as explained in "Configuring the home zone" on page 6-25.

Note: For security reasons the default Bandwidth Management Across Zone Boundary setting is No Calls.

Note: You do not configure IP address ranges in the Remote Default zone configuration because this zone is used to manage bandwidth for all calls from IP addresses not defined in any of your configured zones.

6 Click OK to close the Bandwidth Management dialog box.

7 Click Apply to save the remote zone configuration changes.

Adjusting IP call quality parameters

Click

These parameters only apply to the IP telephony resources on the Wave system and do not affect the performance of the IP telephones.

Most of the IP call quality parameters can be found in the System Parameters folder of the IP Telephony applet. If you are not familiar with IP telephony, you should contact your Wave product support vendor for information about adjusting these settings. If you want to return to the system defaults, click Restore Defaults in any of the System Parameters screens.

Jitter buffer

Voice packets can experience a high level of network delay, especially if the lines are congested. The jitter buffer temporarily holds incoming packets in order to assemble them in the correct order and recreate a high-quality voice signal.

To adjust the jitter buffer:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the IP Telephony icon, located in the PBX Administration section.

3 Select Advanced Codec Settings from the System Parameters folder.

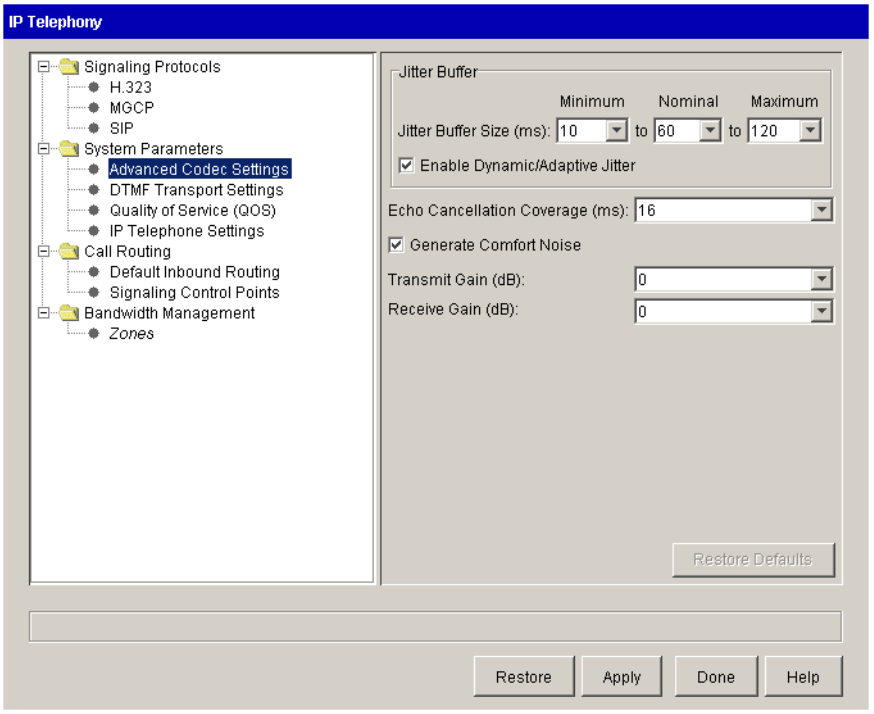


Figure 6-20 IP Telephony System Parameters Advanced Codec Settings

4 Specify the range of acceptable delay in the Jitter Buffer Size drop-down lists.

5 Check the Enable Dynamic / Adaptive Jitter check box (this is the default).

The Dynamic / Adaptive Jitter feature optimizes the jitter buffer based on voice traffic and network conditions. If you disable this feature, the Wave system adheres to the values in the Nominal and Maximum fields.

Echo cancellation

Echo in a telephone network is caused by signal reflections generated by the hybrid circuit that converts between a 4-wire circuit (a separate transmit and receive pair) and a 2-wire circuit (a single transmit and receive pair). Echo is present even in a conventional circuit switched telephone network. However, it is acceptable because the round trip delays through the network are smaller than 5 ms and the echo is masked by the normal side tone every telephone generates.

Perceived echo becomes a problem in packet-switched networks because the round trip delay through the network is almost always greater than 5 ms. Thus, echo cancellation techniques are often used.

Echo is generated toward the packet-switched network from the TDM telephone network. The echo canceller compares the voice data received *from* the packet-switched network with voice data being transmitted *to* the packet-switched network. The echo from the telephone network hybrid is removed by a digital filter on the transmit path into the packet-switched network.

To adjust the echo cancellation settings:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the IP Telephony icon, located in the PBX Administration section.

3 Select Advanced Codec Settings from the System Parameters folder (see Figure 6-20).

4 Select 0, 8, or 16 milliseconds from the Echo Cancellation Coverage drop-down list.

Note: The recommended value is 16 ms.

Comfort noise

This option generates comfort noise during silences on the receiving end of the telephone call in calls where silence suppression is enabled. Comfort noise is white noise that masks “dead” time in a telephone conversation. Use this option to simulate a circuit-switched telephone conversation. This option is enabled by default.

To adjust the comfort noise settings:

1. If necessary, click the Administration tab of the Management Console.
2. Click the IP Telephony icon, located in the PBX Administration section.

Click

3. Select Advanced Codec Settings from the System Parameters folder (see Figure 6-20).
4. Check the Generate Comfort Noise check box if you want the Wave system to automatically generate background noise.

Gain

The gain settings adjust the transmit gain and receive gain levels for the TDM segment of a call.

To adjust the transmit and receive gain values:

1. If necessary, click the Administration tab of the Management Console.
2. Click the IP Telephony icon, located in the PBX Administration section.

Click

3. Select Advanced Codec Settings from the System Parameters folder (see Figure 6-20).
4. Adjust the Receive Gain and Transmit Gain values.
   - Receive Gain—If the volume level from the TDM phone is too low, you can increase the receive gain.
   - Transmit Gain—If the volume level to the TDM phone is too low, you can increase the transmit gain.

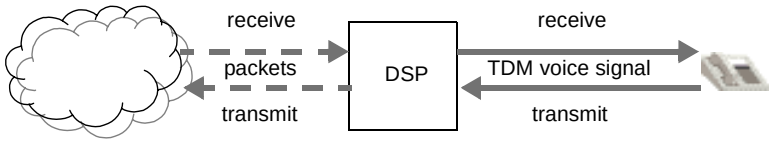


Figure 6-21 Transmit and receive diagram

DTMF transport settings

To configure the DTMF transport settings:

1 If necessary, click the Administration tab of the Management Console.

Click 

2 Click the IP Telephony icon, located in the PBX Administration section.

3 Select DTMF Transport Settings from the System Parameters folder.

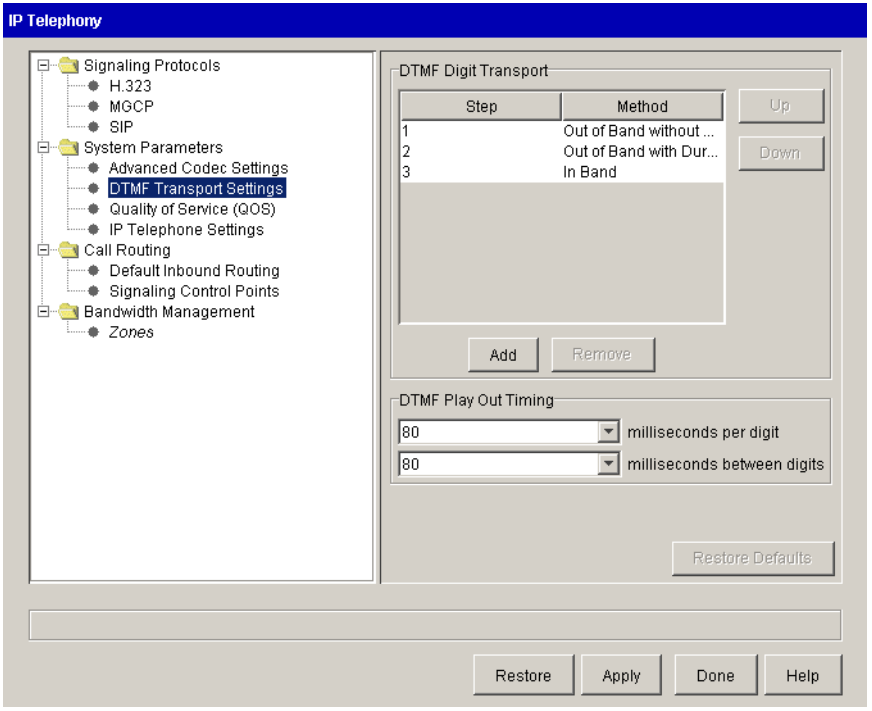


Figure 6-22 IP Telephony System Parameters DTMF Transport Settings

Caution: *Use the default values in this pane. Only adjust these values if you know the requirements of your VoIP network.*

DTMF digit transport

In the DTMF Digit Transport group box (see Figure 6-22), specify whether the DTMF digits are sent in band or out of band in order of preference. In band means that the DTMF digits are left as tones in the original audio stream. Out of band means that the DTMF digits are removed from the audio stream, sent on another signaling path, and played by a DSP at the receiving end.

Note: Since there must be at least one step in the DTMF Digit Transport table, you can remove all of the steps except the In-Band step.

DTMF playout

The DTMF Play Out Timing settings (see Figure 6-22) control the play out length of incoming out of band DTMF tones.

WAN Quality Of Service settings

To configure the WAN Quality of Service settings:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the IP Telephony icon, located in the PBX Administration section.

3 Select WAN Quality of Service (QOS) from the System Parameters folder.

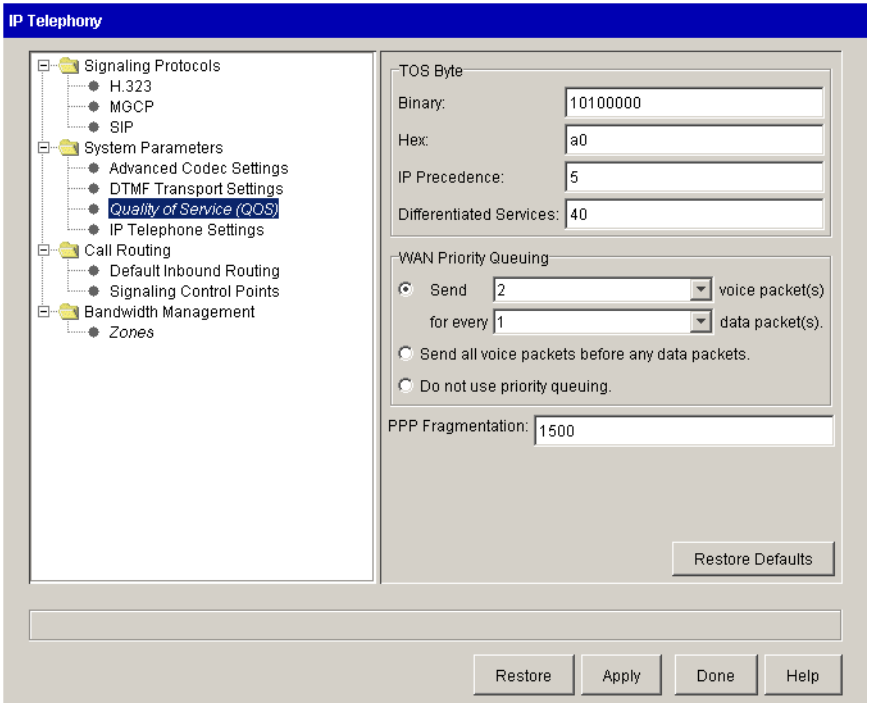


Figure 6-23 IP Telephony System Parameters WAN Quality Of Service settings

TOS Byte

In the TOS Byte group box (see Figure 6-23), specify a value for one of the parameters. Changing the value in any of these fields adjusts the other fields to display equivalent values.

Note: Make a note of these values if you are connecting the Wave system to an external router because you will need to specify these values when you configure prioritization of voice frames in the router.

IP telephony ports

When using Voice Over IP in a network, especially one that includes a firewall, you will need to know the ports used in the packets that carry VoIP traffic. The following table lists the ports used in the packets.

Table 6-2 Wave System

	Receive on ...	Transmit to ...
RTP Voice Transport		
RTP	UDP / dynamic (16384 - 32766) - not configurable	UDP / Dependant on other endpoint
RTCP	UDP / dynamic (16385 - 32767) - not configurable	UDP / Dependant on other endpoint
SIP Transport		
	5060 - configurable to 5061	5060, 5061
	UDP 65000 (used for music on hold)	

Initial Call Routing Configuration

CHAPTER CONTENTS

This chapter provides information about configuring initial call routing options and internal call routing settings.

Configuring extension ranges

In this task you will configure the digits extensions can begin with, and the number of digits in extension numbers.

The default ranges for extensions are as follows:

- user extensions are 100-199 (first digit 1, length 3)
- system extensions are 500-599 (first digit 5, length 3)

  For example, Wave ISM modems are preconfigured to use extension 570.

Note: If you have already configured extensions, and you want to change the extension length, you must first delete all the extensions, hunt groups, and Voice Mailboxes that begin with the first digit in the range you want to modify.

To configure extension ranges:

Click

1 If necessary, click the Administration tab of the Management Console.

2 Click the First Digit Table icon, located in the PBX Administration section.

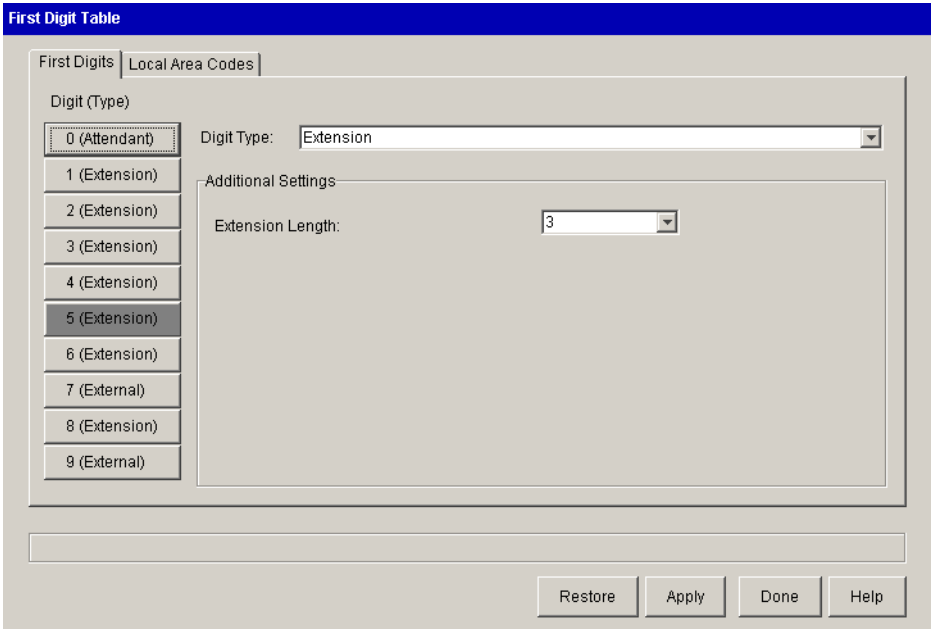


Figure 7-1 First Digit Table, showing Extension settings

3 Select one of the Digit (Type) buttons from the left side of the applet.

4 Select Extension from the Digit Type drop-down list.

5 Select an extension length between 2 and 7 digits from the Extension Length drop-down list.

For example, Digit 1 with Extension Length 3 will provide you with extension numbers in the range 100-199.

6 Click Apply to save your changes.

7 Click Done to return to the Management Console.

Setting the home area code

When the user dials a seven-digit local telephone number, automatic route selection uses the home area code to find a matching rule in the area code tables.

To specify your home area code:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the First Digit Table icon, located in the PBX Administration section.

3 Click the Local Area Codes tab.

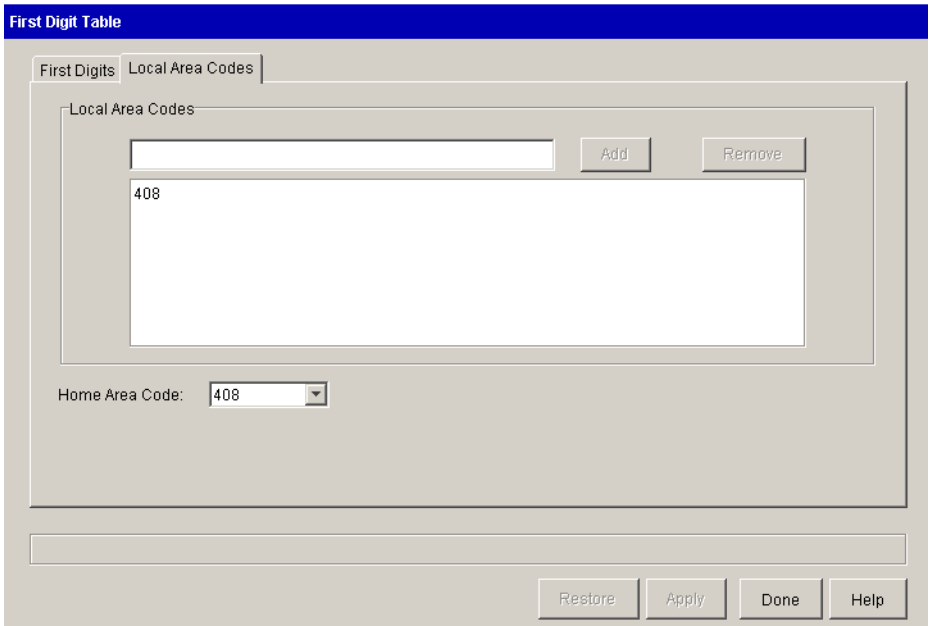


Figure 7-2 First Digit Table, showing the Local Area Codes tab

4 Enter your home area code in the field next to the Add button, then click Add.

The area code appears in the list below the field.

Do not specify any additional area codes unless your calling area requires 10-digit dialing for local area codes. See “Configuring 10-digit dialing” on page 7-4.

The area code that you enter also appears in the Home Area Code drop-down list.

5 Select your Home Area Code from the drop down list.

6 Click Apply to save your changes.

7 Click Done to the Management Console.

Configuring 10-digit dialing

Configure 10-digit dialing when certain telephone numbers that include the area code do not require that a 1 be dialed before dialing the telephone number.

To configure 10-digit dialing:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the First Digit Table icon, located in the PBX Administration section.

3 Click the Local Area Codes tab (see Figure 7-2).

4 Enter each area code in the Local Area Codes field, and click Add to add it to the list.

Note: If you must dial a 1 before using an area code, do not enter that area code in the Local Area Codes list.

Note: Be sure that your home area code is selected in the Home Area Code drop-down list.

5 Click Apply to save your changes.

6 Click Done to return to the Management Console.

Note: In some cases you might want to have users dial ten digits but your service provider requires 11 digits for calls to specific area codes. You will need to add a 1 to the number before placing the call. You will configure this digit manipulation in “Configuring outbound routing tables” on page 9-13.

Configuring the Voice Mail extension

The Voice Mail hunt group default extension (550) is adequate for most Wave configurations. If you wish to use a different extension number to access Voice Mail, it is a good idea to have your Voice Mail hunt group set up before you configure outbound call routing.

To create a new Voice Mail hunt group:

Click

1 Select the Hunt Groups icon from the Management Console.

2 Select the Application tab.

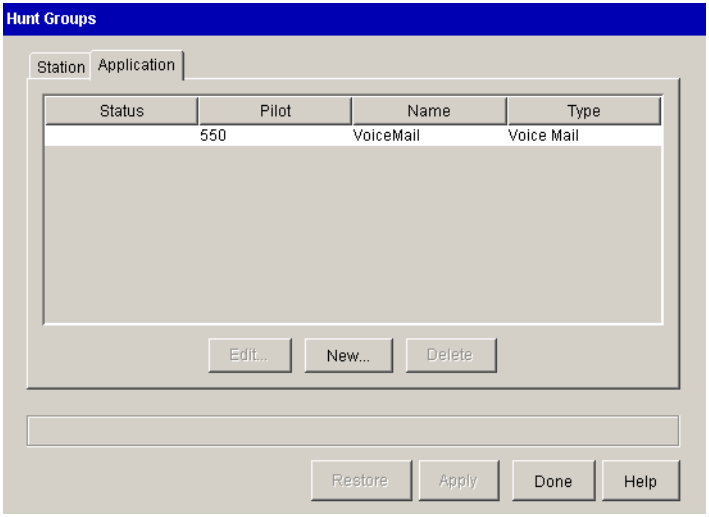


Figure 7-3 Hunt Groups applet, showing the Application tab

3 Click New to open the Application Hunt Group dialog box.

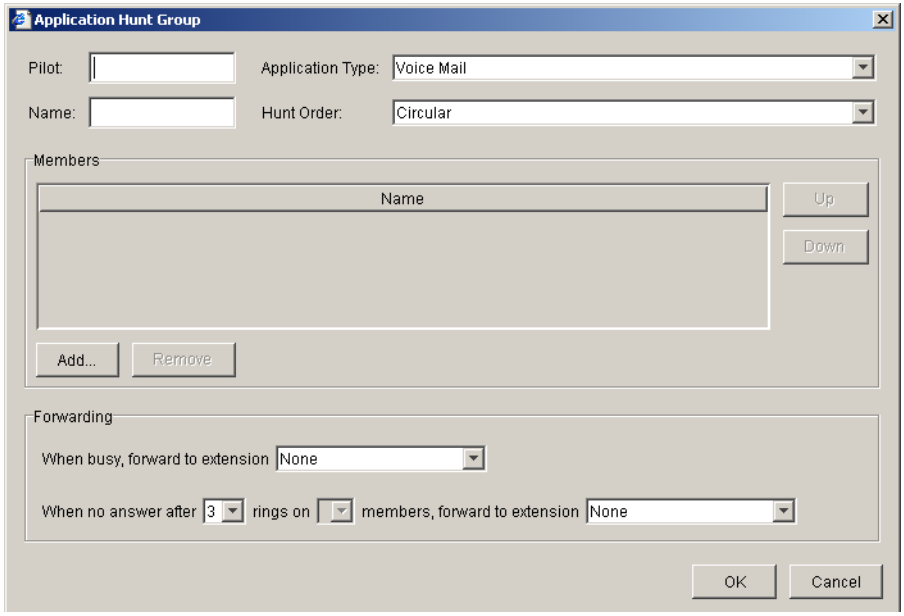


Figure 7-4 Application Hunt Group dialog

4 Type a valid extension number in the Pilot field.

5 Type Voice Mail in the Name field.

6 Select Voice Mail from the Application Type drop-down list.

7 Select Circular from the Hunt Order drop-down list.

8 Click Add to open the Add Hunt Group Members dialog box.

The Add Hunt Group Members dialog lists the available system ports that you allocated to Voice Mail in the Resource Management applet.

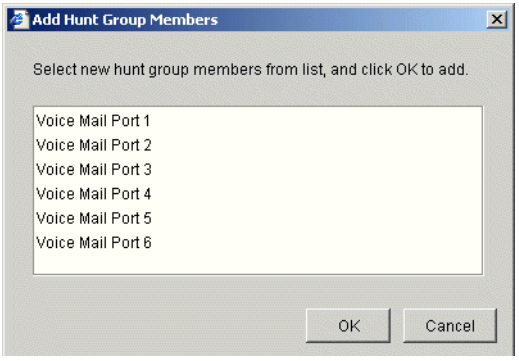


Figure 7-5 Add Hunt Group Members dialog

9 Select all of the system ports listed, and click OK.

10 Select a Busy Forwarding destination if necessary.

You can select a forwarding destination for calls coming into the Voice Mail hunt group when all the system ports included in the hunt group are busy. If you do not select a busy forward destination, callers will hear a busy tone.

Do not select any other forwarding options, because system ports always answer calls unless they are busy.

11 Click OK to close the Application Hunt Group dialog box.

12 Click Apply to save your changes.

13 Click Done to return to the Management Console.

Configuring Inbound Call Routing

CHAPTER CONTENTS

This chapter describes how to configure Vertical Wave for inbound call routing.

For inbound call routing configuration recommendations and examples, see “Inbound call routing” on page 28-15.

Configuring trunk groups for inbound call routing

You created trunk groups, and configured the outbound trunk hunt order in “Creating new trunk groups” on page 5-1.

To configure trunk groups for inbound call routing:

1 If necessary, click the Administration tab of the Management Console.

Click 

2 Click the Trunk Groups icon, located in the Trunk Administration section.

3 Select and edit a trunk group for inbound call traffic.

4 On the In tab, choose one of the options in the Digit Interpretation group box.

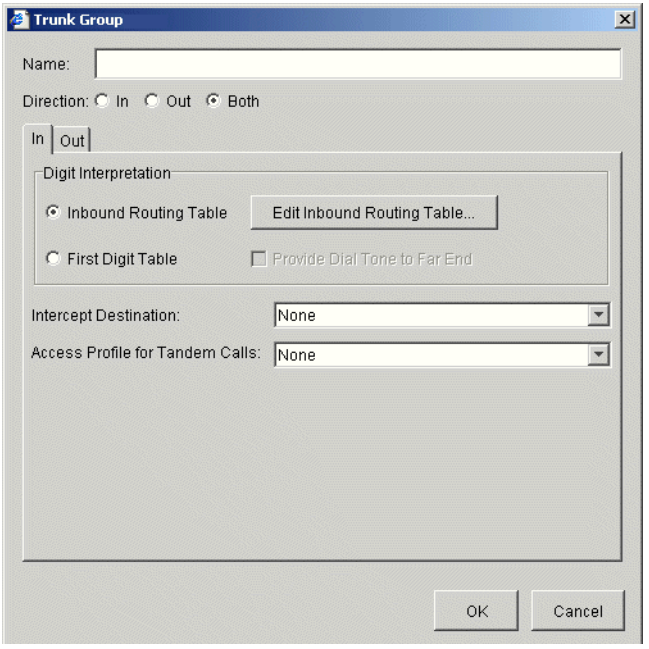


Figure 8-1 Trunk Groups applet, In tab

You can choose whether to interpret received digits from an inbound call in one of two ways:

- **Inbound Routing Table**—Use this option if Wave will be receiving calls from a central office switch. If you choose this option, refer to "Configuring inbound routing tables" on page 8-4, for detailed instructions about setting up your inbound routing tables.
- **First Digit Table**—Use this option if Wave will be receiving calls from another PBX, rather than from a central office switch. Refer to "Configuring extension ranges" on page 7-1, for detailed instructions about setting up the First Digit Table.

  Check the Provide Dial Tone check box if Wave must provide dial tone to the far end.

5 In the Intercept Destination field, enter the extension or hunt group to which you want to send calls that cannot be routed using Inbound Routing Table rules.

If the Intercept Destination is configured to be None, the caller will hear a fast-busy tone.

All calls received on this inbound trunk group that fail for any reason will be sent to the station or hunt group that you specify in this field. Examples of failed calls might be a misdialed DID number or an external number that is blocked by this trunk group's tandem access profile.

Caution: *Do not configure Wave to route inbound calls to the Intercept Destination by default. This might cause your calls to be routed incorrectly. If you would like to create a true inbound call default destination, create a default step in the inbound routing table.*

6 Select the Access Profile for Tandem Calls from the drop-down list.

You can restrict the use of Wave in a tandem call routing configuration to prevent toll fraud. Select None if your call routing does not provide for tandem calls. For information about tandem calls, see "Tandem call routing" on page 28-21.

Click

If you configure Wave to handle tandem (or trunk-to-trunk) calls, you must also select the Allow External Trunk-to-Trunk Connections option in the General Settings applet, PBX (Advanced) tab, Trunking group box.

In this scenario, a call is physically connected across two external trunks through Wave ISM. If you enable external trunk-to-trunk connections, Wave allows calls to be forwarded, transferred, and conferenced between external numbers.

Note: Trunk-to-trunk connections involving analog loop-start trunks are not included in this option by default because such connections may not terminate properly even when a call is completed, resulting in a trunk remaining unavailable even when it is not actively being used. We recommend that you accept this default.

If your particular needs require that users be able to make analog loop-start external trunk-to-trunk connections, make the following additional settings in the Trunking group box:

- Select the Allow Analog Loop-Start Trunk-to-Trunk Connections option.
- Choose a maximum duration for trunk-to-trunk connections from the Trunk-to-Trunk Maximum Connect Time (Minutes) drop-down list. This setting limits the amount of time a trunk may be unavailable when not actively being used, but it also determines the maximum duration of active calls. Be sure to choose a setting that won't result in active calls being cut off prematurely.

Configuring inbound routing tables

For information about and examples of inbound routing tables, see “Inbound call routing” on page 28-15.

To configure an inbound routing table:

1 Click Edit Inbound Routing Table.

You can access the Inbound Routing Table editor in one of two ways:

- Open the Trunk Groups applet, edit an inbound voice trunk group (or create a new one), select the In tab, and click Edit Inbound Routing Table.
- Open the IP Telephony applet, select the Call Routing folder, and click Edit Inbound Routing Table.

The Inbound Routing Table dialog appears.

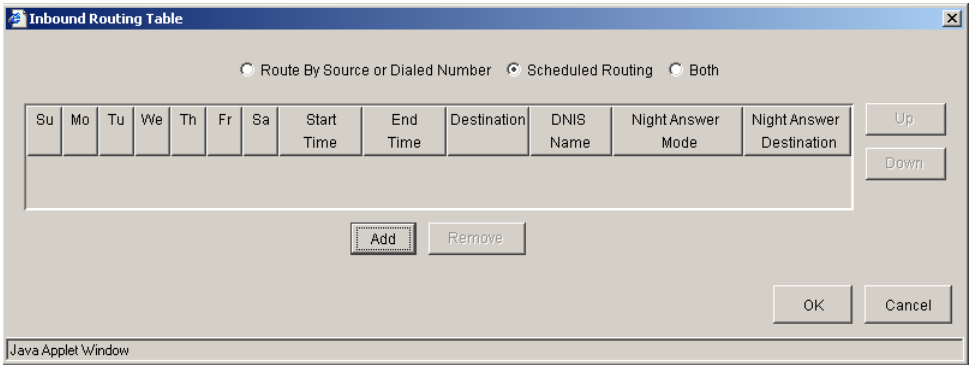


Figure 8-2 Inbound Routing Table dialog, showing Scheduled Routing options

2 Select one of the table options.

- Route By Source or Dialed Number—Using this setting you can decide how calls on this trunk group get routed based on the caller ID (or ANI) sent with the call, or the digits the caller dialed (DID, Lead Telephone Number, or DNIS).
- Scheduled Routing—Use this format to set time and day restraints on the destination to which inbound calls from the specified trunk are routed. This choice is ideal for trunks that receive no digits and require no translation.
- Both—This setting is ideal if calls to the main company number and all DID numbers are sent to the same trunk group.

3 Click Add to insert a new rule into the table.

If you are using Scheduled Routing:

a Uncheck the days of the week that you do not want this rule to affect.

b Select times in the Start Time and End Time fields.

If you are using Route By Source or Dialed Number, click the appropriate table cells to enter values in the following columns:

- Call Source—No value required. May be any string of digits representing caller ID or ANI source number.
- Dialed Number—Default (any number received), or contains a string of zero or more digits, followed by a string of 0 or more x characters. This string may be as large as 32 characters. The dialed number column directly represents the digits expected to be sent from the CO with an inbound call. For example, enter a three-digit DID number beginning with a 2 as the value 2xx.

Note: Default is a wildcard value, indicating that any number, of any length, is accepted.

4 Enter the destination information.

- Destination—Contains a string of zero or more digits, followed by a string of 0 or more x's. This string may be as large as 32 characters. This number is interpreted as if dialed from an internal station. For example, enter a three-digit extension number beginning with a 1, as the value 1xx. If the destination is an external telephone number, append the external access digit (configured in the First Digit Table) before the telephone number.
- DNIS Name—No value required. If the value in the Dialed Number field is a DNIS number, enter a description up to 32 characters long. This description overwrites the calling party (call source) information and appears on the display panel of the destination extension. This string identifies the number that the caller dialed.

5 Enter a night answer mode from the Night Answer drop-down list.

The available Night Answer Modes are as follows:

- Not Used—disables the Night Answer Mode
- Use System Default—uses the Default Night Answer Destination specified in the General Settings applet
- User Defined—uses the destination that you enter in the Night Answer Destination field and overrides the system default specified in the General Settings applet

6 Select a rule, and click Up and Down to rearrange the rule order.

   If you are using Scheduled Routing and there is overlap in the schedule, the rules must appear in order of precedence.

7 Click OK to return to the host applet.

8 Click Apply to save your changes.

9 Click Done to return to the Management Console.

Configuring Outbound Call Routing

CHAPTER CONTENTS

This chapter provides procedures for configuring outbound call routing. See "Outbound call routing" on page 28-4 for information about each type of outbound call routing.

Configuring automatic route selection

This section provides information about configuring outbound call routing using automatic route selection. See "Automatic route selection" on page 28-8 for examples and information about why you might use automatic route selection.To set up your Wave Integrated Services Manager (ISM) for automatic route selection, you need to complete the following tasks:

- Configuring the external first digit
- Configuring the Global Access Profile
- Configuring specific access profiles
- Configuring outbound routing tables

Configuring the external first digit

In this task you will configure an external first digit for outbound call routing by automatic route selection.

To configure the external first digit:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the First Digit Table icon, located in the PBX Administration section.

3 Select a Digit (Type) button and set Digit Type to “External.”

The external digit configuration options appear in the Additional Settings group box.

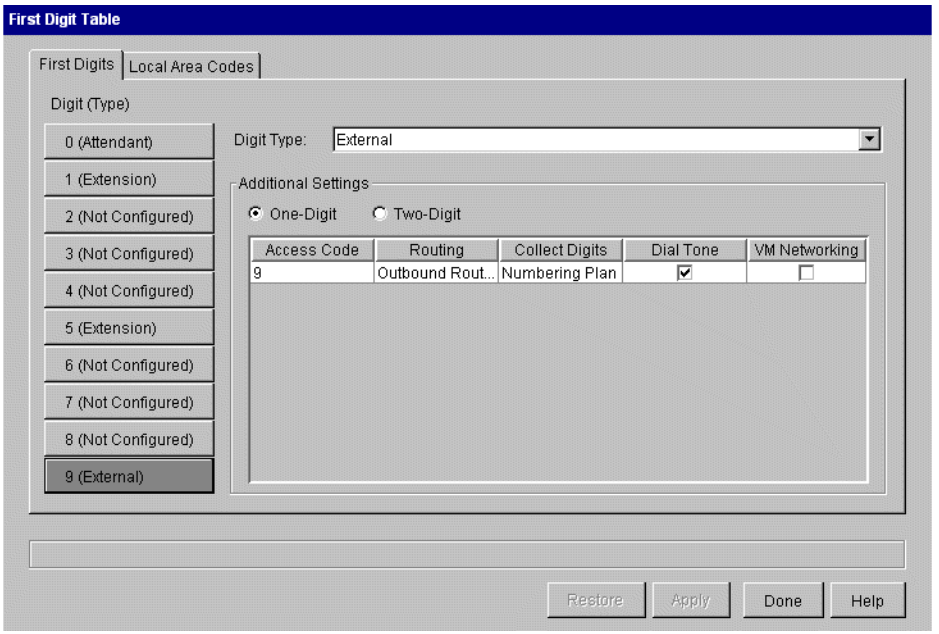


Figure 9-1 First Digit Table, showing External settings

4 Specify whether you want this first digit to support One-Digit or Two-Digit external dialing.

If you select Two-Digit support, access codes *x*0 through *x*9, where *x* is the first digit, appear in the Additional Settings table.

5 Check to make sure the settings for the access code (or for each access code, if Two-Digit support is selected) are as follows. If not, double-click the access code to display the Edit External Access Code dialog box and make the necessary changes.

Your settings should look like those in Figure 9-1.

- Routing—leave this option set to the default of Outbound Routing.
- Collect Digits—leave this option set to the default of Numbering Plan.

  This setting automatically selects the numbering plan for your locale. For North America this is the North American Numbering Plan (NANP).
- Dial Tone—if you want Vertical Wave to provide a dial tone when the external digit or digits are dialed, leave the Dial Tone check box selected. If not, deselect the check box.
- VM Networking—leave this option set to the default (deselected).

6 Click Apply to save your changes.

7 Click Done to return to the Management Console.

Configuring how first digit extensions appear in ViewPoint

You can give an external first digit a name, to make it easier for users to select in ViewPoint. You can also hide an external first digit so that it does not appear in ViewPoint and cannot be dialed. Hiding first digits can be useful when you want to use them for testing purposes.

To configure an external first digit for ViewPoint:

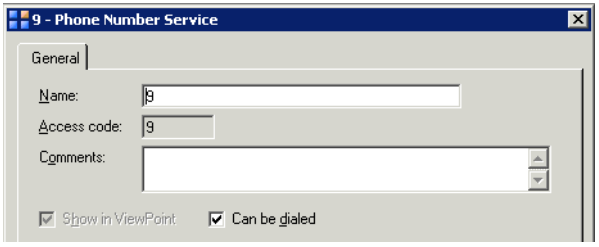
1 From the Management Console, click the icon for **User/Workgroup Management**, located in the PBX Administration section. The User / Workgroup Management

applet opens.

See “Using the User / Workgroup Management applet” on page 2-9 for information about navigating in the User / Workgroup Management applet.

2 Click the Dialing Services icon in the view bar. The Dialing Services view opens, displaying all external first digits that you have defined so far.

3 To edit a dialing service, double-click it in the view. The Dialing Service dialog box opens.



4 Type a name for the dialing service in **Name**.

5 Add any notes about the dialing service in **Comments**.

6 Select the following visibility options:

- **Show in ViewPoint.** This hides the dialing service from all **Call Using** lists in ViewPoint.
- **Can be dialed**. This disables the dialing service so it can't be dialed.

7 Click **OK**.

Configuring the Global Access Profile

Wave examines the Global Access Profile parameters prior to examining the specific access profile for an outbound call.

To edit the Global Access Profile:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Outbound Routing icon, located in the Trunk Administration section.

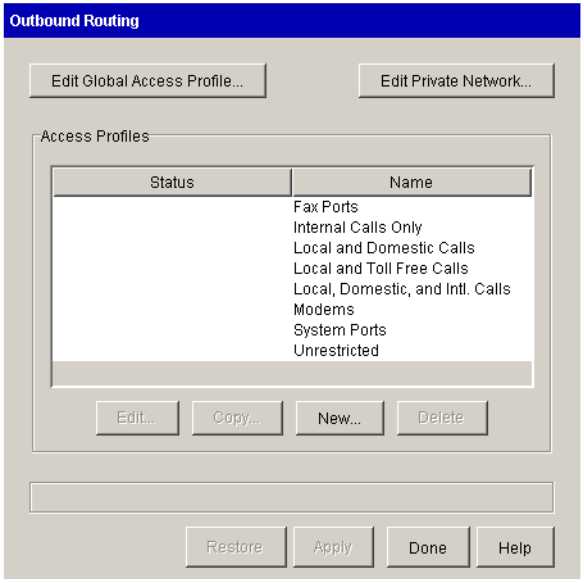


Figure 9-2 Outbound Routing applet

3 Click Edit Global Access Profile to open the Global Access Profile dialog box.

4 Click the Special Digits Table tab.

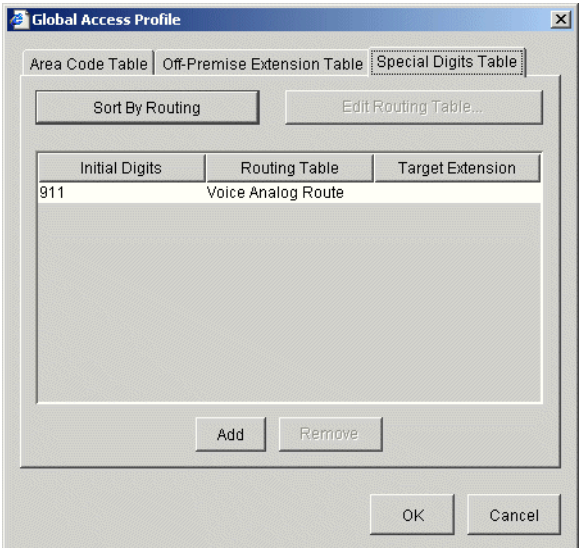


Figure 9-3 Global Access Profile dialog, showing the Special Digits Table tab

Use the Special Digits Table to enter any digits or strings of digits that you want Wave to process before processing the rules in the other tables.

Note: 911 is automatically configured as a special digit string and is routed to the Voice Analog routing table.

5 Click Add to add a new special digit string.

6 Click the Initial Digits field to enter the special digits.

7 Click the Routing Table field to choose an option from the drop-down list.

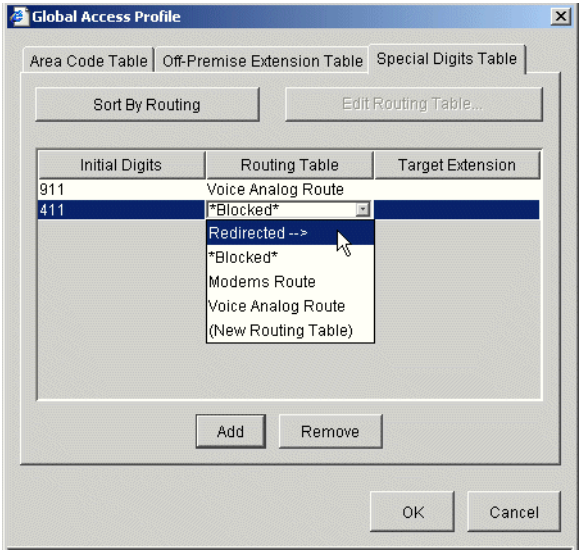


Figure 9-4 Special Digits Table, showing the Routing Table drop-down list

A drop-down list appears that shows the existing routing tables, as well as an option to redirect the call to an extension and an option to create a new routing table.

- If you choose to create a new routing table, refer to the instructions in "Configuring outbound routing tables" on page 9-13.
- If you choose to redirect the call to an extension, click the Target Extension field, and select the extension to which you want to redirect the call. You can come back to this step after finishing "Configuring telephone templates" on page 10-1.

8 Click Sort By Routing to arrange the rules in the order they will be accessed during call routing.

9 Select the Area Code Table tab.

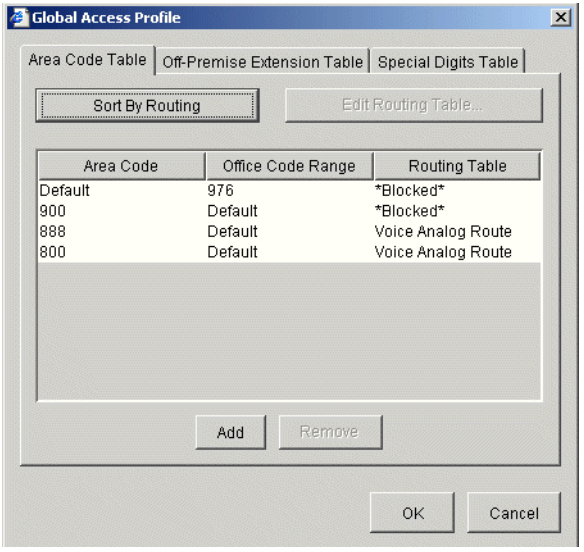


Figure 9-5 Global Access Profile dialog, showing the Area Code Table tab

The Area Code Table is where Wave looks for matching area codes or office codes (or combinations of area and office codes) to determine how to route calls containing those numbers. You can use the Global Access Profile Area Code Table to block undesirable toll calls, as shown in Figure 9-5.

The rules that you specify in the Global Access Profile Area Code Table override the rules that you set for the specific access profiles area code tables you will configure later in this section. If you want to block or route certain numbers for all users in the system, enter the rules in this table.

10 Click Add to add an entry to the Area Code Table.

A new record appears in the list.

11 Edit the Area Code and Office Code fields by clicking in them and entering the codes for which you are providing routing instructions.

- Area Code—Enter the area code for which you want to specify routing instructions that apply to all outgoing calls. You might want to add an entry to block outbound calls with an area code of 900. Enter Default to allow all area codes.
- Office Code Range—Enter the office code (or a range of office codes) within the specified area code. Enter Default to match any office code within the specified area code.

12 Click the Routing Table field to reveal a drop-down list that displays available routing tables, an option to block the specified area codes or office codes entirely, and an option to create a new routing table.

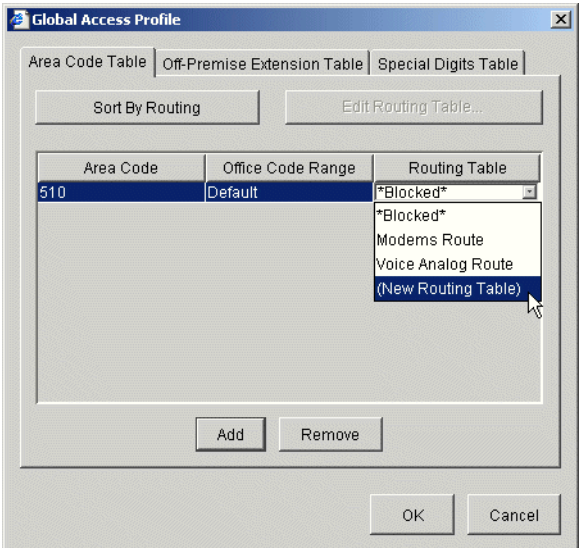


Figure 9-6 Area Code Table, showing the Routing Table drop-down list

Use the *Blocked* option to block all calls to specific area codes or office codes.

Note: To edit a routing table or create a new routing table, refer to the instructions in “Configuring outbound routing tables” on page 9-13.

13 Repeat steps 10 through 12 for additional area code and office code routing entries.

14 Click Sort By Routing to arrange the rules in the order they will be accessed during call routing.

15 When you are finished editing the Global Access Profile, click OK and save your changes.

16 Click Apply to save your changes.

17 Click Done to return to the Management Console.

Configuring specific access profiles

Before going to the Outbound Routing applet, identify the different calling privileges that will be associated with groups of users. From the Outbound Routing applet, you can create, edit, copy, and delete access profiles that you can assign to specific telephone extensions, trunk groups, and digital connections. You can edit the existing access profiles or create new ones.

To configure a specific access profile:

1 If necessary, click the Administration tab of the Management Console.

Click 

2 Click the Outbound Routing icon, located in the Trunk Administration section.

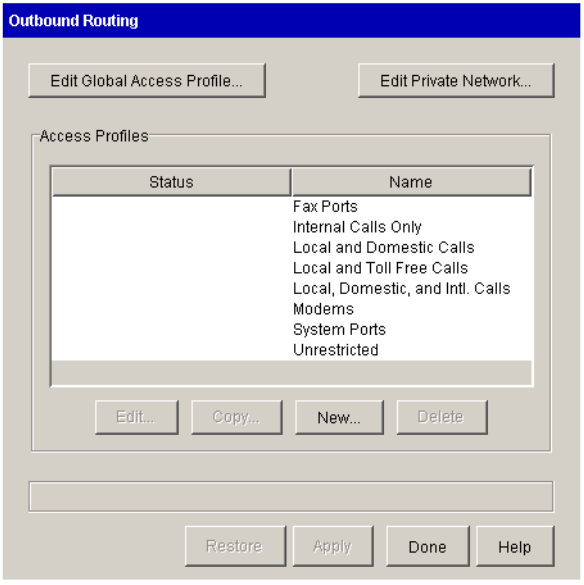


Figure 9-7 Outbound Routing applet

3 Select an access profile from the list, then click Edit, or click New to create a new access profile.

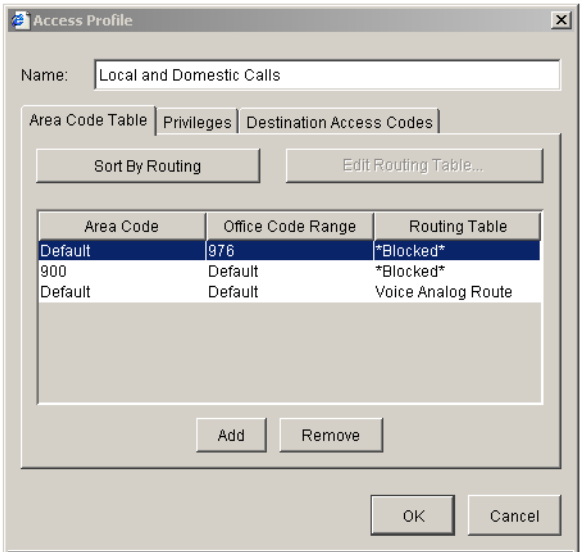


Figure 9-8 Access Profile dialog, showing the Area Code Table tab

In the Area Code Table you can configure Wave to do the following:

- Route calls that did not match rules in the Global Access Profile
- Specify routing for area code and office code combinations

4 Click Add to add an entry to the Area Code Table.

A new record appears in the list.

5 Edit the Area Code and Office Code fields by double-clicking in the fields and entering the codes for which you are providing routing instructions.

- **Area Code**—Enter the area code for which you want to specify routing instructions. Enter Default to allow all area codes.
- **Office Code Range**—Enter the office code or a range of office codes within the specified area code. Enter Default to match any office code in the specified area code.

6 Choose a routing table from the **Routing Table** drop-down list.

The drop-down list displays available routing tables, an option to block the specified area codes or office codes entirely, and an option to create a new routing table.

Use the *Blocked* option to block calls to specific area codes or office codes, for example the 900 area code or the 976 office code (if you did not already do this in the Global Access Profile).

Note: To edit a routing table or create a new routing table, refer to the instructions in "Configuring outbound routing tables" on page 9-13.

7 Repeat steps 4 through 6 for additional area code and office code routing entries.

8 Click Sort By Routing to arrange the rules in the order they will be accessed during call routing.

9 Click the Privileges tab.

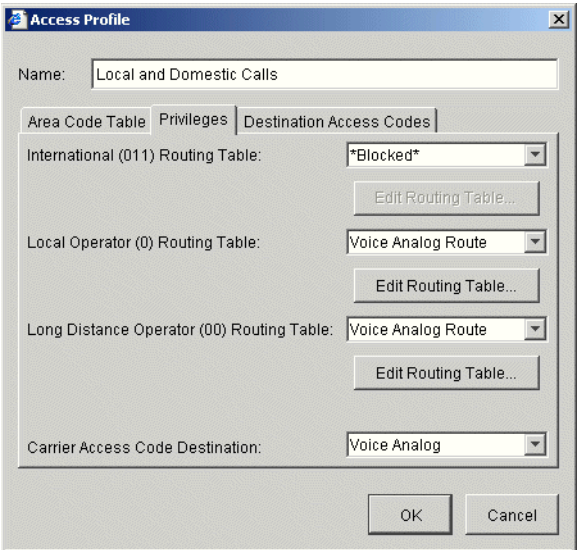


Figure 9-9 Access Profile dialog, showing the Privileges tab

The Privileges tab is where you can specify the routing table to which Wave will send calls, depending on the call type. The call type is determined by the first digits entered in the telephone number. You can send calls to different routing tables depending on the following digit strings:

- **011**—International Routing Table
- **0**—Local Operator Routing Table
- **00**—Long Distance Operator Routing Table

- **Carrier Access Code Destination**—A carrier access code is a code (seven digits, beginning with 101) that you dial to access a long-distance carrier, for example 10-10-321.

10 Choose a routing table from the drop-down field next to each call type.

The drop-down list provides a choice of available routing tables, an option to block the specified call type entirely, and an option to create a new routing table.

Use the *Blocked* option to block calls of that call type.

Note: To edit a routing table or create a new routing table, refer to the instructions in "Configuring outbound routing tables" on page 9-13.

11 Choose the appropriate route for the Carrier Access Code.

Unless you want your users to dial carrier access codes, leave this option *Blocked*.

From the drop-down list, you can choose the trunk group for the call. You cannot assign a routing table to the carrier access code since no translation is required.

Select *Ignored* to strip the carrier access code and route call as a regular long distance call.

12 Click the Destination Access Codes tab.

This tab allows you to specify which external access codes configured in the First Digit Table may be used by this access profile. External access codes may be used to provide access to external paging systems or specific trunks on Wave ISM.

13 To allow users with the access profile you are creating or editing to use an access code, select the code in the list and click the Permission Allowed check box to select it. To block users with this access profile from using the access code, leave the check box deselected.

14 Click OK to close the Access Profile dialog box.

15 Click Apply to save your changes.

16 Click Done to return to the Management Console.

Configuring outbound routing tables

You can access outbound routing tables through the Outbound Routing applet.

To add or edit an outbound routing table:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Outbound Routing icon, located in the Trunk Administration section.

3 Click an Edit Routing Table button or choose New Routing Table from any of the following places.

- Area code tables
- Special digits table
- Off-premise extension table
- Privileges

The Routing Table dialog appears.

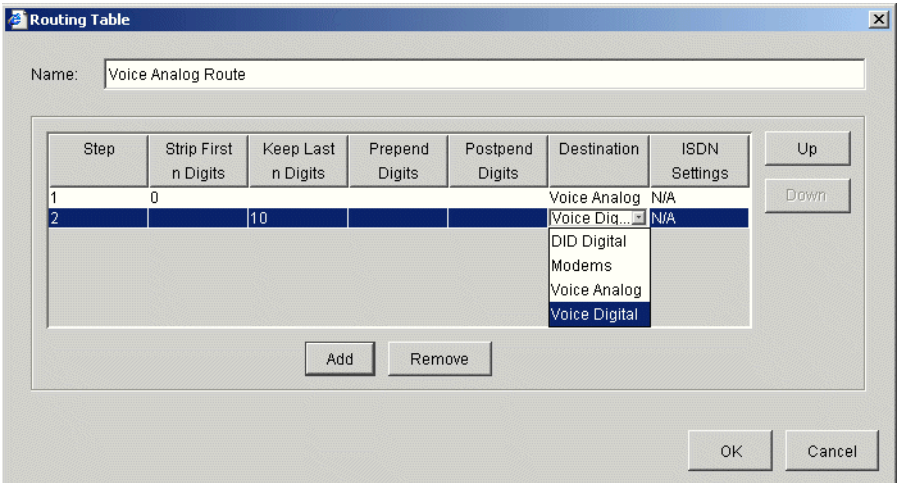


Figure 9-10 Routing Table dialog

4 If this is a new routing table, enter a descriptive Name.

5 Click Add to add a new step to the routing table.

6 For each step, you can click in the fields and edit the following settings, depending on the translation your CO requires.

- Strip First ***n*** Digits—Enter the number of digits, if any, that you want to strip from the beginning of the outgoing telephone number.

Note: The external access code digit (for example, 9) does not need to be stripped. It is not included in any call routing decisions after the call type is determined.

- Keep Last ***n*** Digits—Enter the number of digits, if any, that you want to keep at the end of the outgoing telephone number.

  Note: For a particular route step, you can enter a value into *either* the Strip First Digits *or* Keep Last Digits field. Entering `0` for Strip First Digits will not remove any digits. Entering `0` for Keep Last Digits will remove all the digits.

- Prepend Digits—Enter the digits that you want to add to the beginning of the outgoing telephone number.
- Postpend Digits—Enter the digits that you want to add to the end of the outgoing telephone number.
- Destination—Select a destination trunk group (or Signaling Control Point for IP telephony) from the drop-down list. (The Signaling Control Points have the following format: `IP|`*Signaling Control Point name*. See the *Vertical Wave IP Telephony Administrator's Guide* for more information.)
- ISDN Settings—If you selected a trunk group that is associated with an ISDN trunk in the Trunk Configuration applet, you can select an ISDN setting from the drop-down list. If you did not select a trunk group that is associated with an ISDN trunk, this field is disabled. For more information about how to configure ISDN settings, refer to "Configuring digital channels for ISDN" on page 5-21.

7 Repeat steps 5 and 6 to add steps to the routing table.

8 Click the Up and Down buttons to move a selected step up or down in the list.

The order of the routing steps is important. Wave tries placing the call to the destination specified in the first step. If the specified trunk is busy, disabled, or disconnected, the system tries the next routing step, and so on. The caller will hear a fast busy tone if all steps have been tried unsuccessfully.

9 Click OK to close the Routing Table dialog box.

All routing tables are available throughout the Outbound Routing applet. You can use the same routing tables for different outbound routing steps and requirements, but be aware that some places in the applet may require different translation, hence different routing tables.

10 Click Apply to save your changes.

11 Click Done to return to the Management Console.

Configuring off-premise extension routing

This section provides information about configuring outbound call routing to off-premise extensions. See “Off-premise extensions” on page 28-12 for examples and information about why you might use off-premise extensions. To set up Wave to dial off-premise telephone numbers as if they were extension numbers, you need to complete the following tasks:

- Creating off-premise extension ranges
- Configuring the off-premise extension table

Creating off-premise extension ranges

Use the procedure “Configuring extension ranges” on page 7-1 to create your off-premise extension ranges if you want to use numbers that begin with a different first digit than those you are using for your local extensions.

For example, if you are using 100-150 for your local extensions and you want to use 159-199 for your off-premise extensions you do not need to configure an additional extension digit in the First Digit Table. Continue with “Configuring the off-premise extension table.”

Configuring the off-premise extension table

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Outbound Routing icon, located in the Trunk Administration section.

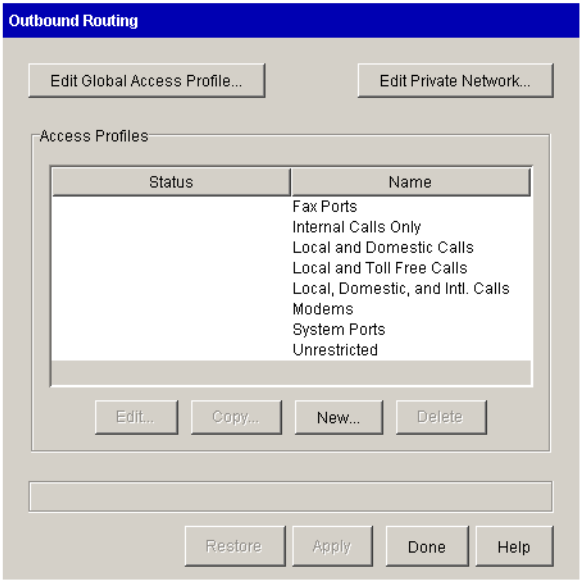


Figure 9-11 Outbound Routing applet

3 Click Edit Global Access Profile to open the Global Access Profile dialog box.

4 Click the Off-Premise Extension Table tab.

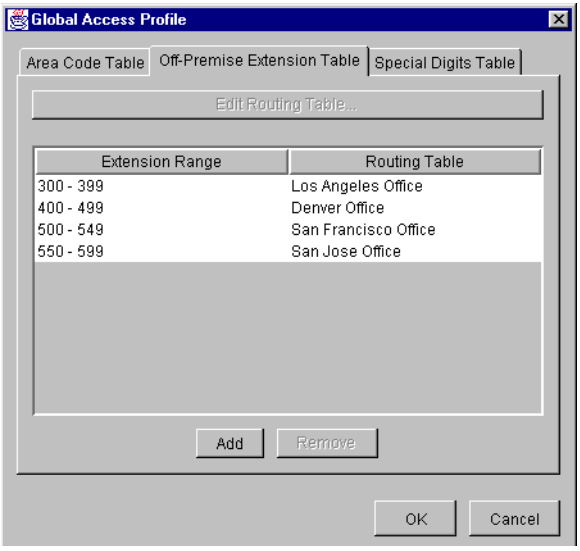


Figure 9-12 Global Access Profile dialog, showing Off-Premise Extension Table tab

5 Click Add to add a range of off-premise extensions.

An entry appears in the list.

6 Click the Extension Range field and enter the range of off-premise extensions you want to configure.

You need to add a new entry for each new range of off-premise extensions (see Figure 9-12).

Note: The First Digit Table must specify the first digit of the off-premise extensions, must have a type of Extension, and must have the same amount of digits as the extensions you specify here.

Note: *Do not* configure off-premise extensions in User / Workgroup Management or the Hunt Groups applet. However, overlap is permitted if you have local extensions that are the same as the off-premise extensions.

7 Create routing tables to translate the digits to go to the telephone company.

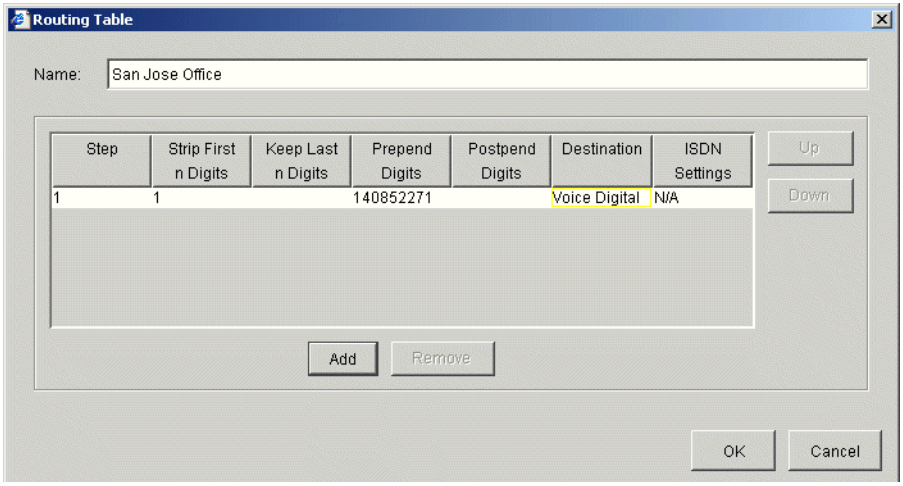


Figure 9-13 Routing table showing off-premise extension translation

To edit a routing table or create a new routing table, refer to the instructions in "Configuring outbound routing tables" on page 9-13.

8 Click OK to close the Global Access Profile dialog, and return to the Management Console.

Configuring destination access code routing

This section provides information about configuring outbound calls using destination access codes. See "Destination access code / direct to trunk group" on page 28-13 for examples and information about why you might use this type of call routing. To set up Wave to use destination access codes, you need to complete the following tasks:

- Creating destination access codes
- Enabling destination access codes

Creating destination access codes

In this procedure you will create destination access codes in the First Digit Table applet.

To create destination access codes:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the First Digit Table icon, located in the PBX Administration section.

3 Click the button with the number that you want to configure.

4 Choose External from the Digit Type drop-down list.

The external digit configuration options appear in the Additional Settings group box.

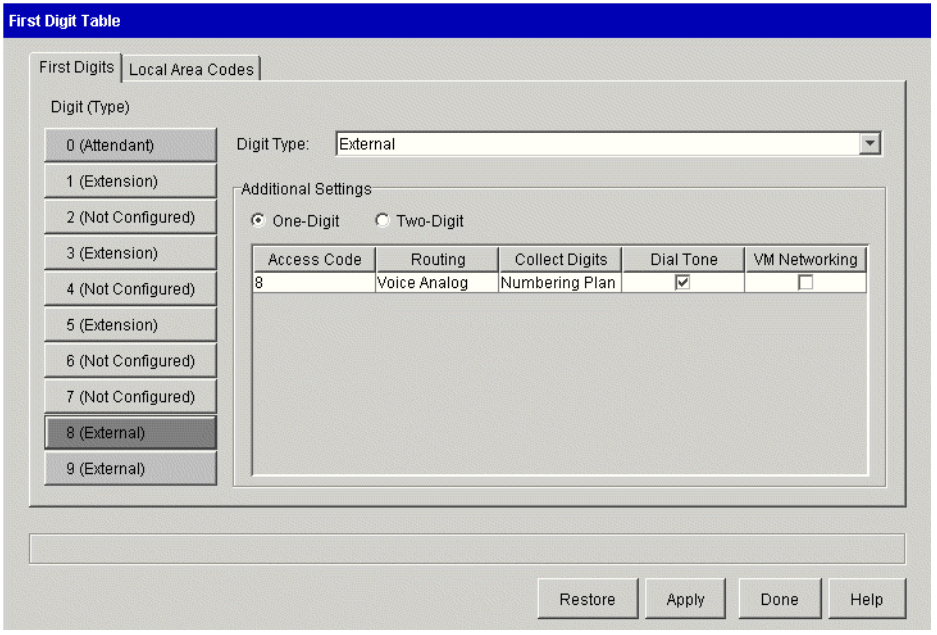


Figure 9-14 First Digit Table, showing External settings

5 Specify whether you want this first digit to support One-Digit or Two-Digit external access codes.

If you select Two-Digit support, access codes x0 through x9, where *x* is the first digit, appear in the Additional Settings group box.

6 Configure the settings for each access code.

Your settings should look similar to those in Figure 9-14.

- **Routing**—Choose the trunk group or IP Signaling Control Point you want to use for routing.
- Collect Digits—Choose one of the following:
  - Specify the number of outgoing digits to collect before the number is sent to the central office. This setting is ideal if you want to limit the number of digits a user can dial using an access code, for example limiting this access code to 11 digits will allow local and long distance calls, but not international calls.
  - Select Numbering Plan to collect the digits expected for the numbering plan specific to your locale. For example, the North American Numbering Plan expects telephone numbers to be 7, 10, or 11 digits (when preceded by a 1).
- **Dial Tone**—Check the Dial Tone check box if you want Wave to provide dial tone after the destination access code is dialed.
- **VM Networking**—Do not check.

7 Click Apply to save your changes.

8 Click Done to return to the Management Console.

9 Continue with the instructions in Enabling destination access codes.

Enabling destination access codes

By default all users are restricted from using new destination access codes. You must enable them in the specific access profiles in the Outbound Routing applet. Enable the access codes only in the specific access profiles that you will assign to groups of users who are permitted to use the codes.

If you haven't already done so, follow the instructions in Creating destination access codes.

To enable destination access codes:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Outbound Routing icon, located in the Trunk Administration section.

3 Select an access profile from the list, then click Edit, or click New to create a new access profile.

4 Click the Destination Access Codes tab.

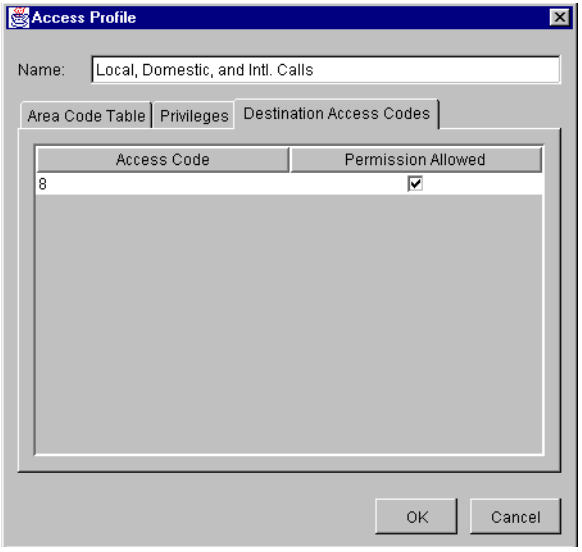


Figure 9-15 Access Profiles dialog, showing Destination Access Codes tab

5. Check the Permission Allowed check box to enable this access profile to use the specified Destination Access Code.
6. Click OK to close the Access Profile dialog box.
7. Repeat steps 3 through 6 for each access profile that you want to edit or add.
8. Click Apply to save your changes.
9. Click Done to return to the Management Console.

Later, when you are configuring extensions and telephones, you will assign specific access profiles to each extension.

Configuring Private Networking

Configuring Private Networking is a four-step process. You need to determine a numbering scheme for your private network. You need to configure Outbound Routing and the First Digit Table to recognize the digits that access the remote Wave systems. Then, you need to go back to the Outbound Routing applet to enable the Private Networking Destination Access Codes.

The following sections describe how to configure Wave for Private Networking:

- "Determining a numbering scheme for Private Networking"
- "Configuring outbound routing for Private Networking"
- "Configuring the First Digit Table for Private Networking"
- "Enabling the new Destination Access Code"

Determining a numbering scheme for Private Networking

Before you can configure your Wave ISMs for Private Networking, you must determine a private networking numbering scheme for your Wave network. The numbering scheme includes the following components:

- External access code (one or two digits) — the first one or two digits that you dial to access the private network
- Location code (between 2 and 6 digits, inclusive) — the code that identifies each Wave ISM on the network
- Extension (between 2 and 7 digits, inclusive) — the telephone extension for each user

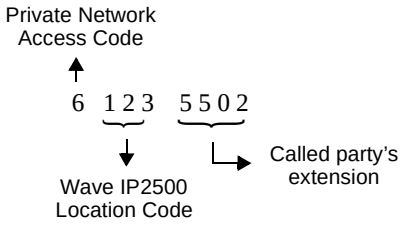


Figure 9-16 Numbering scheme

You need to make decisions about or determine the following things:

- Which external first digit do you want to use for your access code?
- Do you want to use a one-digit or two-digit external access code?
- What length do you want your location codes?

When you dial within the Private Network, you will be prepending the location code to the extension of the person you are calling. Be sure to specify a length long enough to accommodate all the Wave ISMs on your network. You can specify a location code length of 2, 3, 4, 5, or 6 digits. The default value is 3. A location code cannot start with a 0.

- Determine a Home Location Code for each Wave ISM in your network.

Configuring outbound routing for Private Networking

You need to specify the following information about your private network in the Outbound Routing applet:

- The length of your location codes
- The length of your user extensions
- A Home Location Code for this Wave ISM.

You also need to specify ranges of location codes and identify the routing table that you want to use with each range.

To configure location codes in Outbound Routing:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Outbound Routing icon, located in the Trunk Administration section.

The Outbound Routing applet appears.

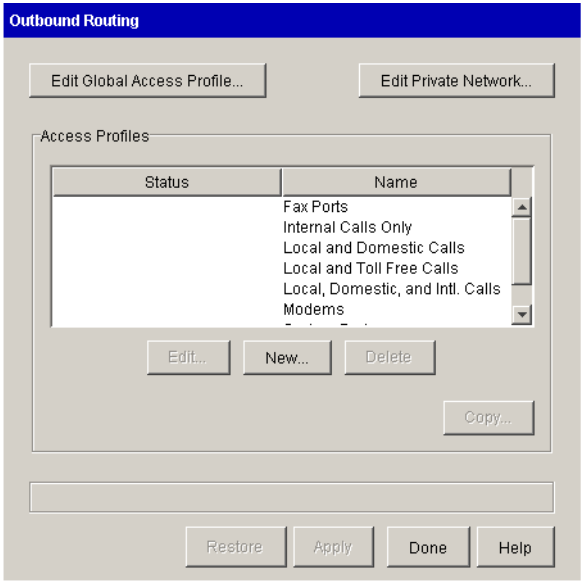


Figure 9-17 Outbound Routing applet

3 Click Edit Private Network.

The Private Network dialog appears.

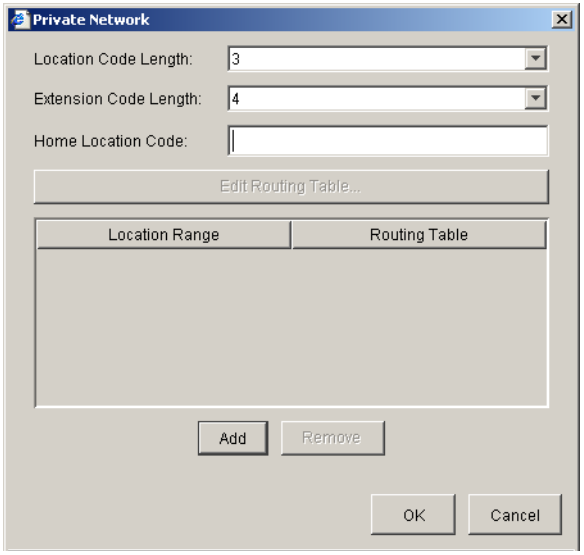


Figure 9-18 Private Network dialog

4 Select the length you want your location codes to be from the Location Code Length drop-down list.

The default is 3. You can select a length of between 2 and 6, inclusive.

5 Select the length of your Wave extensions in the Extension Length drop-down list.

6 Enter a Home Location Code for this Wave ISM.

The Home Location Code must be the same number of digits as the number you specified in the Location Code Length field. The Home Location Code identifies this Wave ISM for internal routing.

7 Click Add to specify a routing table for a range of location codes.

A row appears in the table with a blank Location Code field and a Routing Table entry of *Blocked*.

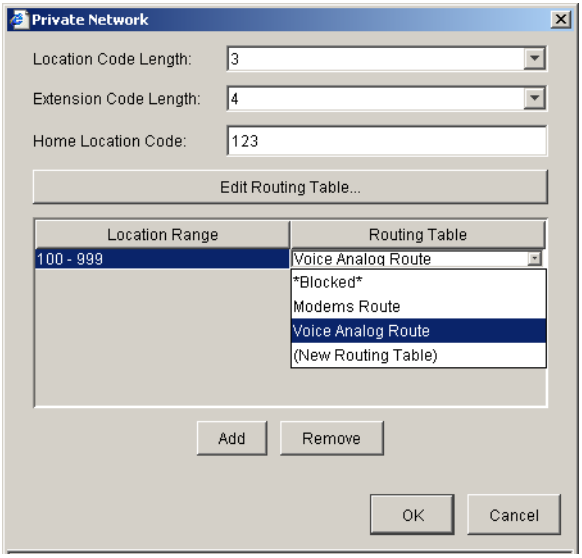


Figure 9-19 Private Network dialog, adding a routing table

8 Click inside the Location Range field and add a range of location fields for which you want to specify a routing table.

Note: You can add multiple ranges of location codes and direct each range to a different routing table.

9 Click inside the Routing Table drop-down list to select the routing table you want to assign to the locations you specified in the Location Range field.

Alternatively, you can add a new routing table by selecting (New Routing Table). For information about creating a new routing table, refer to “Configuring outbound routing tables” on page 9-13.

If you want to edit the routing table you chose for the range of location codes, click Edit Routing Table. For information about editing routing tables, refer to “Configuring outbound routing tables” on page 9-13.

10 Click OK to return to the Outbound Routing table.

11 Click Done to save your changes and return to the Management Console.

Configuring the First Digit Table for Private Networking

You need to specify which first digit to use to access Private Networking.

To configure the First Digit Table for Private Networking:

1 If necessary, click the Administration tab of the Management Console.

Click 

2 Click the First Digit Table icon, located in the PBX Administration section.

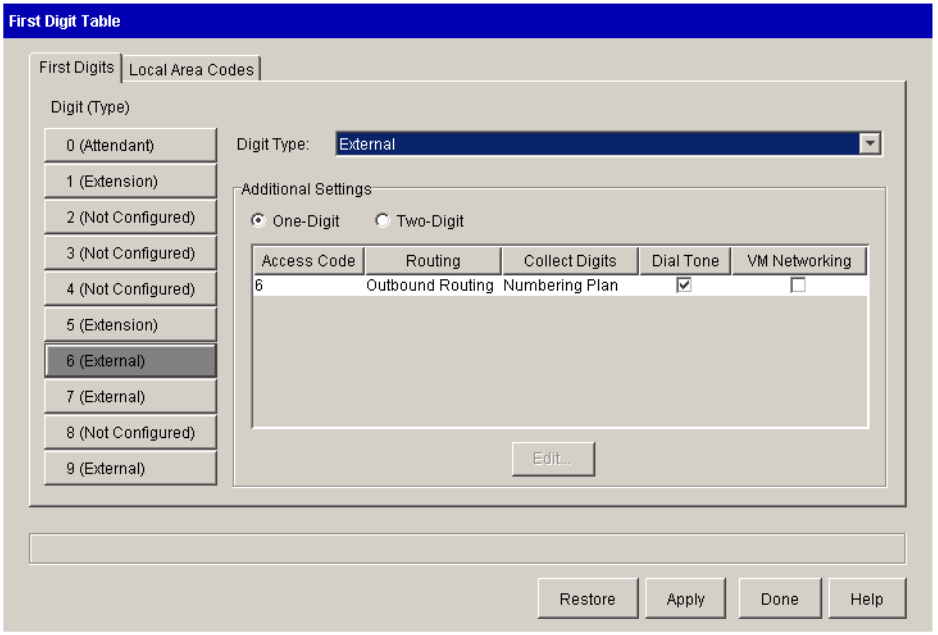


Figure 9-20 First Digit Table applet

3 Select a first digit in the Digit (Type) list.

4 If the digit is not already an external digit, select External from the Digit Type drop-down list.

5 Depending on the type of destination access code you want, select One-Digit or Two-Digit.

If you select Two-Digit, access codes *n*0 through *n*9, where *n* is the first digit, appear in the list.

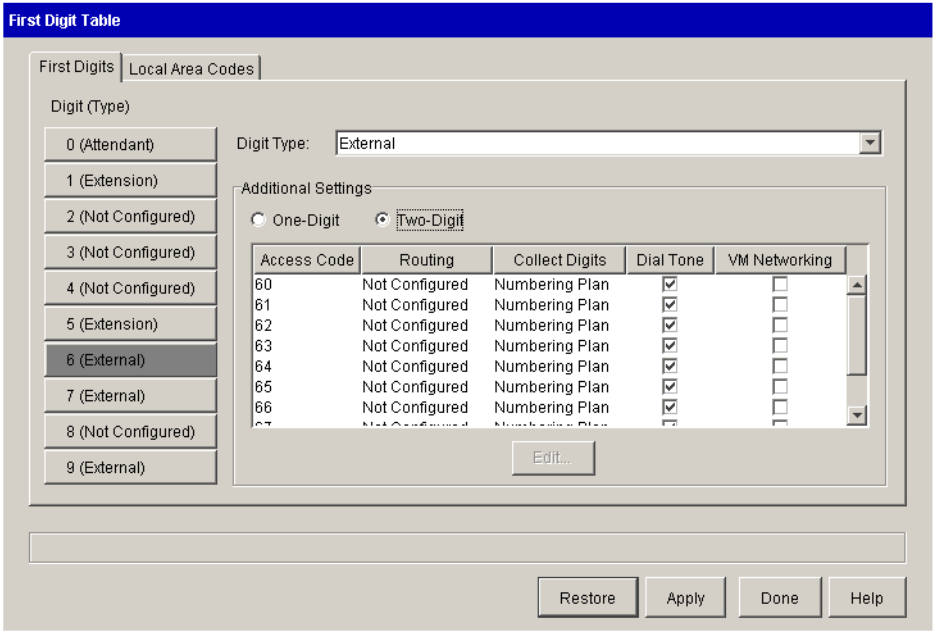


Figure 9-21 First Digit Table, showing Two-Digit access codes

6 Select the Access Code that you want to configure, then click Edit.

The Edit External Access Code dialog appears. The Collect Digits field remains grayed out until you select a routing table from the Routing drop-down list.

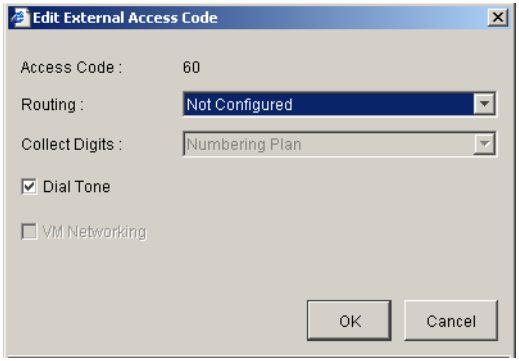


Figure 9-22 Edit External Access Code dialog

7 Select Outbound Routing from the Routing drop-down list.

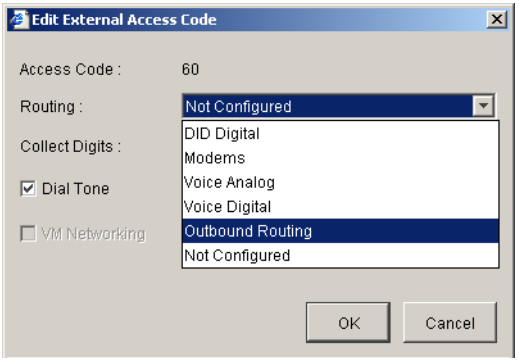


Figure 9-23 Edit External Access Code dialog, showing Routing drop-down list

8 Select Private Network from the Collect Digits drop-down list.

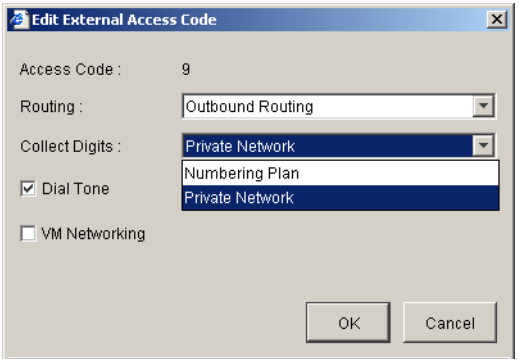


Figure 9-24 Edit External Access Code dialog, showing Collect Digits drop-down list

9 Click OK to return to the First Digit Table applet.

10 If you are configuring multiple External Access Codes, repeat steps 5 through 8 for each.

11 Click Done in the First Digit Table applet to save your changes and return to the Management Console.

Enabling the new Destination Access Code

Every external first digit that is configured in the First Digit Table for a Private Network appears in the Destination Access Codes tab of the Access Codes dialog in the Outbound Routing applet. By default, an Access Profile does not allow access to a Destination Access Code until permission is granted by the system administrator.

If there are users that do not need access to your private network, you can set up an Access Profile for those users and not grant permission for the new Destination Access Code(s).

So, the last step in configuring Vertical Wave Private Networking is to grant permission for the new Destination Access Code.

To enable the new Destination Access Codes:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Outbound Routing icon, located in the Trunk Administration section.

The Outbound Routing applet appears.

3 Select the access profile you want to configure for Private Networking, then click Edit.

Alternatively, you can select New to add an access profile. Refer to “Configuring specific access profiles” on page 9-10 for information about adding access profiles.

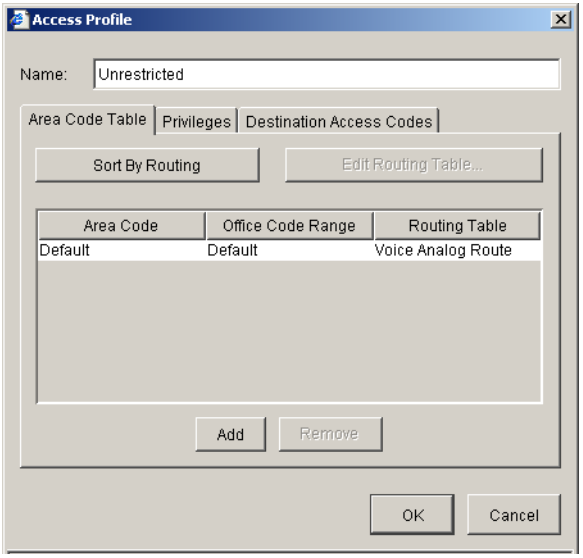


Figure 9-25 Access Profile dialog

4 Select the Destination Access Codes tab.

The Destination Access Codes tab appears.

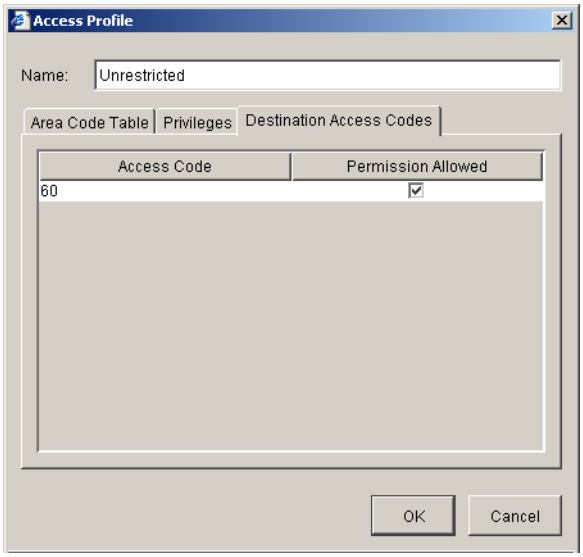


Figure 9-26 Access Profile dialog, showing the Destination Access Codes tab

5 Check the Permission Allowed check box for each Access Code for which you want to grant permission for the selected Access Profile.

6 Click OK to return to the Outbound Routing applet.

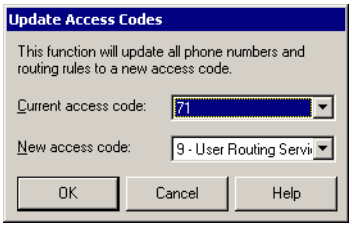
7 Click Done in the Outbound Routing applet to save your changes and return to the Management Console.

Changing an access code in users' saved numbers

When users save phone numbers in ViewPoint that can be speed-dialed or auto-dialed, the dialing service used to make the call is saved with them. Such numbers include contact phone numbers and the phone numbers specified in call forwarding and routing lists. You can do a global replace of one dialing service for another across all users' saved numbers. For example, you can specify that all numbers saved with the "9 - Phone number" service now use your "8 - Centrex" service.

To replace all occurrences of one saved dialing service with another:

1 Choose **Tools > Update Access Codes.** The Update Access Codes dialing box opens.



2 Choose the dialing service you want to replace under **Current access code** and the dialing service you want to replace it with under **New access code.**

3 Click **OK.**

All phone numbers that users have entered in the Wave database with the **Current access code** are changed to use the **New access code**.

Setting default access codes for callbacks

When users return calls or voice messages using the telephone commands or ViewPoint, the system automatically uses a default access code. You can set one default access code for phone numbers and one default access code for Internet addresses. The defaults are used system-wide.

To set default access codes for callbacks

1 From the Management Console, click the icon for **User/Workgroup Management,** located in the PBX Administration section. The User / Workgroup Management

applet opens.

2 Choose **Tools > System Settings**. The System Settings dialog box opens.

3 Choose the External Dialing tab.

4 Change the following as needed:

- **Default phone number access code.** Select the access code for the dialing service that will be used to return a call from a phone number from the Call Log and

Voice Messages views. The default is 9. You can select any dialing service that takes phone numbers as inputs.

- **Default SIP address access code.** Select the access code for SIP Address dialing service that will be used to return a SIP call.

5 Click **OK**.

Where the default access codes appear

In the User / Workgroup Management applet, the Default column of the Dialing Services view shows the current defaults for phone number and Internet callbacks.

In ViewPoint, the Place Call To dialog box always opens with the current default dialing service for phone numbers selected (the user can also choose a different dialing service to place a call). When you import contacts, new phone numbers and IP addresses automatically receive the default access codes.

Setting up emergency dialing

You can configure Wave to support standard 911 emergency dialing service.

Note: A user can make an emergency call from any Wave station, even one not assigned to any user, and even if the user is blocked from making external calls.

Using standard 911 service with Wave

Standard 911 service does not require additional hardware. All standard 911 calls use a Wave trunk and go through the phone company to the emergency dispatching center.

You can change the emergency number from 911 to something else as follows:

1 From the Management Console, click the icon for **User/Workgroup Management**, located in the PBX Administration section. The User / Workgroup Management

applet opens.

2 Choose **Tools > System Settings**. The System Settings dialog box opens.

3 Choose the Emergency tab.

4 Enter the new number in the **Emergency Number** field.

5 Check **Emergency number can be dialed at internal dial tone** if you want users to be able to dial the emergency number without first dialing an access code (such as **9** to get an outside line). If unchecked, users must dial the access code and then the emergency number (for example, **9 911**). This setting affects emergency calls only. Be careful when changing this setting as you may cause accidental emergency calls.

6 Click **OK**.

Configuring Telephones

CHAPTER CONTENTS

This chapter provides information about configuring extensions and features for digital and analog telephones.

Configuring telephone templates

Each Vertical Communications digital telephone model has several preprogrammed feature key templates that you can customize for different types of digital telephone users. If you have several users who use the same digital telephone model and require a similar set of telephone feature keys, create a template for that group of users in the User Configuration (Templates) applet.

Once you create or refine a telephone template, you can then assign it to a user when you create the user. For this reason you should define telephone templates before creating users.

Analog telephones have templates in Vertical Wave that define the physical capabilities of the phone, such as message waiting indicator or caller ID display.

To access telephone templates:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User Configuration (Templates) icon, located in the PBX Administration section. The User Configuration applet opens displaying the Telephone Templates tab.

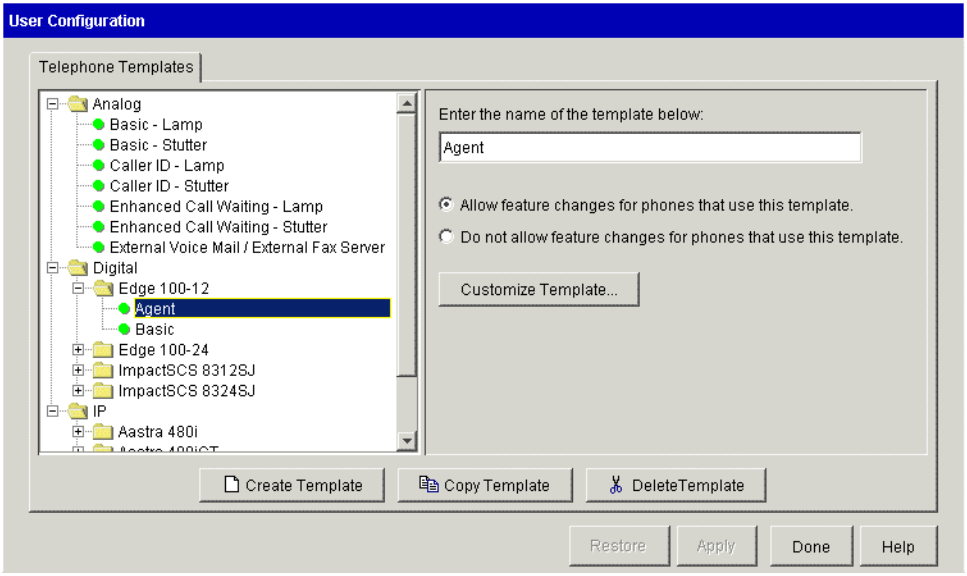


Figure 10-1 User Configuration (Telephone Templates) applet

3 Click one of the folders in the left pane.

- Analog—contains templates for each configuration supported on Wave
- Digital—contains directories for each of the supported Wave digital telephone models
- IP—contains directories for each of the IP telephone types that have been certified for use with Wave.

To create a new template:

1 Select a template folder or template.

2 Click Create Template.

3 Select the new template and rename it in the field in the right pane.

To copy an existing template:

1 Select one of the templates.

2 Click Copy Template to create a copy of the selected template.

A new template appears at the bottom of the template list.

3 Select the new template and rename it in the field in the right pane.

To edit digital telephone templates:

1 Select one of the digital telephone templates.

2 Specify whether to allow feature changes for telephones that use this template.

If you choose to allow feature changes for individuals, you can make those changes while configuring telephone information in the User Configuration applet. See “Configuring telephone templates” on page 10-1. Changes made from the Telephone tab in the Configure User dialog only affect the feature key assignment for the individual user, and do not affect the template.

3 Click Customize Template in the right pane.

A graphical representation of the telephone appears with descriptions of the pre-programmed feature keys displayed on the telephone.

Figure 10-2 Telephone Template dialog, showing the VN16DDS telephone

4 Click the text on a feature key to change the feature assignment.

The Feature Button Configuration dialog appears.

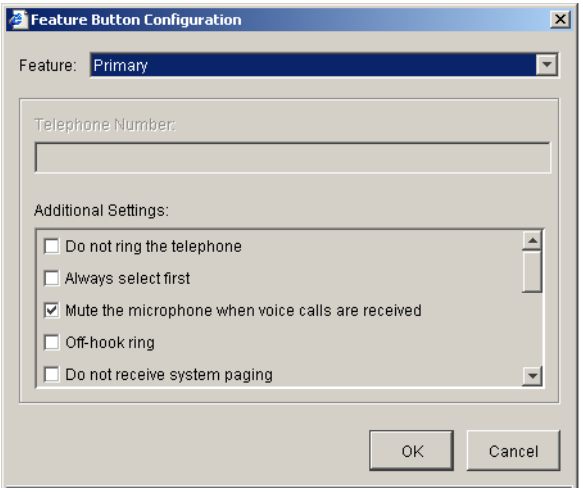


Figure 10-3 Feature Button Configuration dialog

5 Select a Feature from the drop-down list.

Some features have additional settings such as Do not ring the telephone, and Do not allow break-in.

Hint: Right-click a feature key description on the telephone template to open a shortcut menu with the features available for the key. If you select a feature requiring additional information, the Feature Button Configuration dialog opens.

Refer to “Digital telephone featur“The Users view” on page 11-3e keys” on page 10-7 for information about each of the programmable features.

6 Click OK to finish editing the feature key configuration.

7 Click OK to close the template configuration screen, and save your changes.

8 Click Apply to save your changes.

9 Click Done to return to the Management Console.

To edit an analog template:

1 Select one of the analog telephone templates.

See “Default analog telephone templates” on page 10-19 for descriptions of each default template.

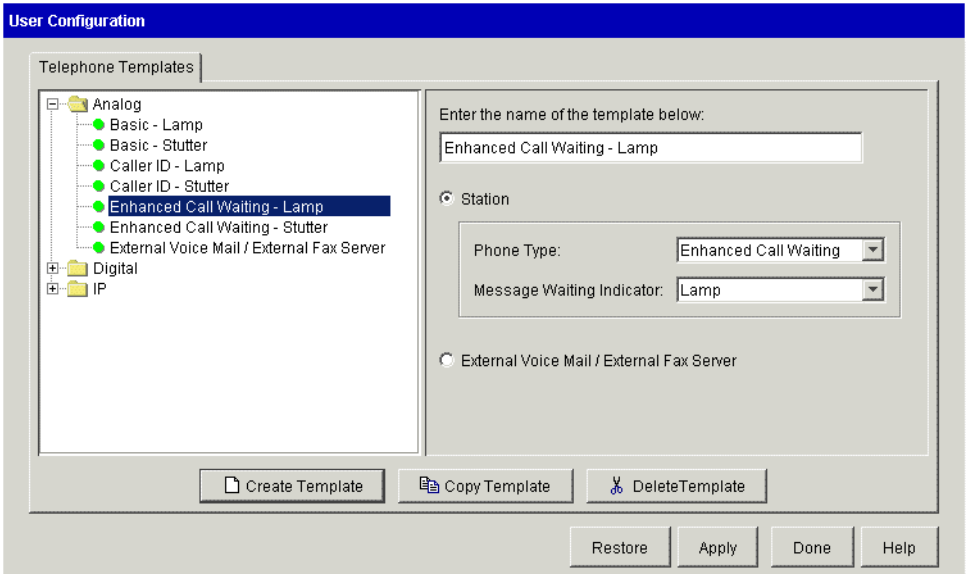


Figure 10-4 Analog telephone template

2 Select the device that this template will be used for:

- Station—analog telephone for making an receiving voice communications
- External Voice Mail / External Fax Server—analog connection for an external Voice Mail system or external fax server

If you select External Voice Mail / Fax Modem go to step 5.

3 Select a Phone Type from the drop-down list.

- Basic—this telephone cannot display caller ID, or no caller ID is supplied by your telephone service provider.
- Caller ID—this telephone can display caller ID on inbound telephone calls when your telephone is idle
- Enhanced CW—this telephone can display caller ID on inbound telephone calls when your telephone is idle and on call waiting calls.

4 Select a Message Waiting Indicator from the drop-down list.

- Lamp—this telephone has a lamp that lights when new messages arrive in the user's Voice Mailbox
- Stutter—this telephone gives the user a stutter dial tone when new messages arrive in the user's Voice Mailbox

5 Click Done to save your changes, and return to the Management Console.

Digital telephone featur"The Users view" on page 11-3e keys

This section provides a list of feature and corresponding feature keys available on Vertical Communications digital and IP telephones, and it provides information about additional parameters you can set for each feature. Refer to the *Wave Phone User's Guide* for detailed information about using each feature on each of the supported telephone models.

For information about configuring IP telephone feature keys, refer to the *Vertical Wave IP Telephony Administrator's Guide* or the Management Console Help.

For information about configuring feature keys used in Vertical Wave Call Navigator, refer to the *Vertical Wave Call Navigator Administrator's Guide.*

To program digital phone feature keys, use the Phone \ Station features tab of the User dialog box in the User / Workgroup Applet. See "The Users view" on page 11-3.

Note: Not all of the features are available on all telephone models.

Auto Dial

Automatically dials a specified telephone number.

You can include multiple Auto Dial keys on a telephone.

Optional setting:

Telephone Number—include any digit sequence up to 32 digits

You can leave this field empty, and the user can program a number from the telephone. Refer to the *Vertical Networks Digital Telephone User's Guide* for instructions.

Call Appearance

Acts as an extra line, enabling you to handle multiple calls on the same phone. If you're on the phone and have a Call Appearance button free, incoming calls ring the phone, and you can take the call by pressing the appropriate Call Appearance button. With multiple calls, you can press the Call Appearance buttons to switch between them, thereby placing the others on hold.

You can set a Call Appearance button for your own extension or program it to work in conjunction with a secondary Line Appearance key. If a line is shared with another user, the corresponding LED(s) on your phone reflect the calls that user is handling, and that user's phone reflects the calls you are handling.

Call Record

Records the current call and saves the recording as a Voice Mail message.

Warning: In some localities, it is illegal to record a telephone call without first notifying the person being recorded.

You can include one Call Record key per telephone.

Call Return

Calls back the extension from which the last inbound call came, if the call originated on your local Wave system.

You can include one Call Return key per telephone.

Call Waiting

Places the existing call on Hold and connects to the second call.

You can include one Call Waiting key per telephone.

Camp-on (Callback)

Calls back an extension when the extension becomes available.

You can include multiple Camp-on keys on a telephone.

Centrex Flash

Accesses Centrex features.

You can include one Centrex Flash key per telephone.

Conference

Adds parties to a conference call.

You can include one Conference key per telephone.

DSS/BLF

Direct Station Select/Busy Lamp Field (DSS/BLF) keys monitor the state of specified extensions, and provides a quick way to transfer calls to those extensions.

You can include multiple DSS/BLF keys on a telephone.

Required setting:

Extension—any valid extension number

Optional setting:

Blind Transfer—transfers a call without first connecting the user to the recipient

Transfers initiated using a key with this option enabled will be completed as soon as the target phone rings. With this option disabled, a consultation transfer is provided for.

Directed Park

Parks a call on a specific extension number.

You can include multiple Directed Park keys on a telephone. Directed Park keys on different telephones, targeted to the same extension are supported.

Optional settings:

Extension—include any valid extension number

A Directed Park key with no extension number assigned requires the user, after pressing the Directed Park key, to enter the extension number on which to park the call.

Display Status—enables the Directed Park LED to indicate the state of a parked call, and simplifies unparking the call by recalling the extension number on which the call was parked

Do Not Disturb

Prevents your telephone from ringing.

You can include one Do Not Disturb key per telephone.

Extension Pickup

Answers a specific ringing extension within your call pickup group.

You can include one Extension Pickup key per telephone.

Optional setting:

Extension—include any valid extension number within the Primary extension number's call pickup group

Refer to "Call pickup groups" on page 18-4 for more information about configuring call pickup groups.

Flash

Allows a user to access any PBX feature by pressing the Flash button followed by the access code (for example, Flash + *54).

You can include one Flash key per telephone.

Group Pickup

Answers any ringing telephone within your call pickup group.

You can include one Group Pickup key per telephone.

Refer to “Call pickup groups” on page 18-4 for more information about configuring call pickup groups.

Headset

Enables the headset.

You can include one Headset key per telephone. The Headset button is only available on 12-button and 24-button telephones. These telephones are not available at this time.

Hold

Places a call on hold.

You can include one Hold key per telephone.

Line Appearance

Line appearances in addition to the Primary line key. The extension number associated with the Line Appearance key can be a primary extension on another telephone, or a virtual extension (does not appear as a primary line on another telephone).

You can include multiple Line Appearance keys on a telephone.

Refer to “Virtual extensions” on page 18-22, for information about configuring virtual extensions.

Required setting:

Extension—any valid extension number

Optional settings:

Do not ring the telephone—disables ringing when a call is received on this line appearance

Off-hook ring—either rings the phone or produces an alert tone (depending on the telephone type) when a call comes in on this line appearance if the telephone is engaged in an off-hook activity

Use Primary Access Profile—applies the access profile configured for the Primary extension number associated with this telephone in the User Configuration applet, Overview tab

Use Primary Caller ID—applies the External Caller ID rules configured for the Primary extension number associated with this telephone in the User Configuration applet, Overview tab

Do not allow break-in—prevents the line appearance from joining an active call when the shared extension is being used by another call

Automatic Line Selection—applies Automatic Line Selection behavior

Refer to “Automatic Line Selection” on page 28-28 for a description of Automatic Line Selection behavior on Line Appearance keys.

Message Waiting

Indicates that a new Voice Mail message is available in the mailbox. Dials the Voice Mail extension number.

You can include multiple Message Waiting keys on a telephone.

Required setting:

Mailbox—any valid Voice Mailbox number

In order for the Message Waiting LED to light on the telephone when a new Voice Mail message arrives, a valid extension must be configured for the Voice Mailbox entered in this field. This can be an extension for a physical telephone station or a virtual extension.

If the Voice Mailbox number does not match the extension number for which this Voice Mailbox was configured, your message waiting indicator keys will not work.

To complete the Message Waiting configuration, be sure to set the system Voice Mail extension number in the General Settings applet, System tab, Voice Mail System drop-down list.

Night Answer

A key used to manually place Wave into a mode where inbound calls are redirected to predetermined destinations. You can configure any on- or off-premise telephone number as the destination. Refer to “Night Answer” on page 18-16 for information about configuring the Night Answer system.

Outside Line

A key used for receiving and placing calls on a specific trunk or set of trunks. Outside Lines must be configured in the Outside Lines applet before this option is available on the telephones. Refer to Chapter 17, “Outside Lines Configuration,”Creating outside lines for more information about configuring outside lines.

You can include multiple Outside Line keys on a telephone.

Required setting:

Outside Line—any Outside Line configured in the Outside Line applet

Optional settings:

Do not allow break-in—prevents the line appearance from joining an active call when the shared extension is being used by another call

Off-hook ring—produces an alert tone when a call comes in on this line appearance if the telephone is engaged in an off-hook activity

Automatic Line Selection—applies Automatic Line Selection behavior

Refer to “Automatic Line Selection” on page 28-28 for a description of Automatic Line Selection behavior on Outside Line keys.

Do not ring the telephone—disables ringing when a call is received on this line

Page

Accesses the public address system and all the digital telephone speakers on your system.

You can include multiple Page keys on a telephone.

Required setting:

Zone Paging Group—pages a specific group or the entire system (System Page)

Refer to “Zone paging groups” on page 18-23 for information about configuring zone paging groups.

Primary

Primary line appearance. This is the main extension number associated with this telephone.

You can include one Primary key per telephone.

Optional settings:

Always Select First—automatically selects the primary line first when answering a ringing line or going off-hook, regardless of where the primary extension key appears on the phone

Mute the microphone when voice calls are received—prevents the calling party from hearing you when a voice call is placed to this extension number

Off-hook ring—produces an alert tone when a call comes in on this line appearance if the telephone is engaged in an off-hook activity

Do not receive system paging—prevents this telephone from receiving pages broadcast to the entire system with the Page key

Note: This option does not prevent the telephone from receiving a zone-specific (non-system) page.

Do not allow break-in—prevents the line appearance from joining an active call when the shared extension is being used by another call

Do not ring the telephone—disables ringing when a call is received on this line appearance

Disable paging alert tone—disables the paging alert tone on this telephone, but allows the telephone to receive the page

Receive call waiting tone when off hook—If checked, a beep sounds if the user is off hook and another call arrives on the line. A beep also sounds if an incoming call hangs up or is forwarded before answering.

Receive splash ring when off hook—If checked, one short ring blip sounds when another call comes in while the user is off hook. The "Do not ring the telephone" setting suppresses this ring too.

Program

Programs programmable feature keys, such as Auto Dial, User Forward, and Voice Call keys, and displays information about feature keys.

You can include one Program key per telephone.

Redial

Dials the last dialed telephone number.

You can include one Redial key per telephone.

Release

Disconnects a user from an active call and cancels button programming.

You can include one Release key per telephone.

Self Park

Places a call in a parked state on the user telephone for retrieval from another telephone.

You can include one Self Park key per telephone.

In the General Setting applet, PBX (Advanced) tab, in the Call Park group box, you can specify the Self park *n* minutes before ring back setting. In the Self park drop-down list, select the number of minutes that Wave waits for a user to pick up a self-parked call. If the call is not picked up within the specified time, Wave rings the extension from which the call was parked. If you specify unlimited minutes, then Wave does not ring back the extension.

Silent Monitor

Allows a user to monitor another user's call without either the user or the caller being aware of the monitoring activity.

This feature requires a license key to be functional.

You can include one Silent Monitor key per telephone.

Speaker/Mute

Toggles the telephone and handset microphone off and on. Enables you to toggle between hands-free and handset speaking.

You can include one Speaker / Mute key per telephone.

System Speed Dial

Enables the dialing of System Speed Dial numbers.

You can include multiple System Speed Dial keys on a telephone.

Optional settings:

Speed Dial Index—enter one to three digits to shorten the length of the speed dial index number required of the user

For example, if you have speed dial index numbers 100-199, and you want the user to dial only two digits to access those numbers (00-99), enter a 1 in the Speed Dial Index field. You can make a System Speed Dial key specific to a particular telephone number by entering the entire Speed Dial index number.

Preview—alters the function of the System Dial key to Dialing Preview mode

Refer to the *Vertical Networks Digital Telephone User's Guide* for information about using System Speed Dial with Dialing Preview.

Refer to "System Speed Dial" on page 18-18 for information on configuring speed dial index numbers.

System Park

Places a call in a parking slot for retrieval from another telephone. *Not available on the VN08D.*

You can include one System Park key per telephone.

In the General Setting applet, PBX (Advanced) tab, in the Call Park group box, you can specify the System park ***n*** minutes before ring back setting. In the System park drop-down list, *n* is the number of minutes that Wave waits for a user to pick up a parked call. If the call is not picked up within the specified time, Wave rings the extension from which the call was parked. If you specify unlimited minutes, Wave does not ring back the parking extension.

Note: An Enhanced Call Waiting analog telephone or a digital telephone with a display is required to system park a call, but any telephone can be used to retrieve a system parked call.

Transfer

Transfers calls to another extension.

You can include multiple Transfer keys on a telephone.

Optional settings:

Extension—allows you to transfer calls to a specific extension

Blind Transfer—transfers a call without first connecting the user to the recipient

Direct Transfer to Voice Mail—transfers a call directly to the specified Voice Mailbox

The Direct Transfer to Voice Mail option generates a telephone key label called Transfer VM. You must specify the Voice Mail hunt group extension in the Extension field if you select this setting.

Unassigned

No feature is assigned to the key.

You can include multiple Unassigned keys on a telephone.

User Forward

Forwards calls to another extension or telephone number.

You can include multiple User Forward keys on a telephone.

Optional setting:

Telephone Number—include a telephone number

You can leave this field empty, and the user can program a number from the telephone.

Configure the following options in the General Setting applet, PBX (Advanced) tab, in the Trunking group box:

Off-Site Call Forward Password Required—Check this check box if users must enter their Voice Mail passwords when forwarding their telephone calls to an external number.

If you select this option, users must enter their Voice Mail passwords after specifying the external number when they dial *43 (or press the Forward key on a digital telephone) to forward their calls to an off-site number.

Allow External Trunk-to-Trunk Connections—Check this check box to enable external trunk-to-trunk connections.

In this scenario, a call is physically connected across two external trunks through Wave. If you enable external trunk-to-trunk connections, Wave allows calls to be forwarded, transferred, and conferenced between external numbers.

Voice Call

Intercom page directed to a specific digital telephone extension.

You can include multiple Voice Call keys on a telephone.

Optional setting:

Extension—include any valid extension number

You can leave this field empty, giving the user the option of programming or dialing a number from the telephone if desired.

Default analog telephone templates

If you use analog telephones on your Wave system, there are seven default templates provided that contain most combinations of analog telephone caller ID and message waiting indicator feature options. There is a Fax modem template provided as well. You should not need to change the templates, but you will need to select them while configuring analog telephone extensions.

The default analog telephone templates are:

- **Basic-Lamp**—use for telephones with no caller ID and a message waiting lamp
- **Basic-Stutter**—use for telephones with no caller ID and no message waiting lamp

- **Caller ID-Lamp**—use for telephones with caller ID and a message waiting lamp
- **Caller ID-Stutter**—use for telephones with caller ID and no message waiting lamp
- **Enhanced Call Waiting-Lamp**—use for telephones with enhanced caller ID and a message waiting lamp
- **Enhanced Call Waiting-Stutter**—use for telephones with enhanced caller ID and no message waiting lamp
- **External Voice Mail/External Fax Server**—use for extensions connected to external Voice Mail systems and external fax servers

Configuring hunt groups of extensions

Create station hunt groups of user extensions when you want to have telephone calls routed to a group of users. The Attendant hunt group is used by the Attendant digit (default=0) for dialing the company operator, and it is used to forward inbound calls to the company operator or AutoAttendant. Other station hunt groups are used for routing calls to groups of extensions.

Note: The Wave system has a maximum of 20 groups, including hunt groups, trunk groups, and zone paging groups.

Configuring the Attendant hunt group

Configuring the Attendant consists of specifying an Attendant digit in the First Digit Table applet, and assigning extensions to the Attendant hunt group in the Hunt Groups applet.

Any digit—but only one—can be configured as the Attendant digit in the First Digit Table applet. If the Attendant digit is changed from the default of zero (0), the Attendant hunt group pilot number must also be changed, to ensure that the company operator and AutoAttendant will receive all calls routed to the attendant.

Internal calls and calls specifically forwarded to the Attendant Hunt Group as the default operator in the AutoAttendant applet are forwarded to the Attendant Hunt Group.

Note: The zero (0) digit can be configured in the First Digit Table as Not Configured, Attendant, or External, but it cannot be configured for extension.

To configure the Attendant hunt group:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Hunt Groups icon, located in the PBX Administration section.

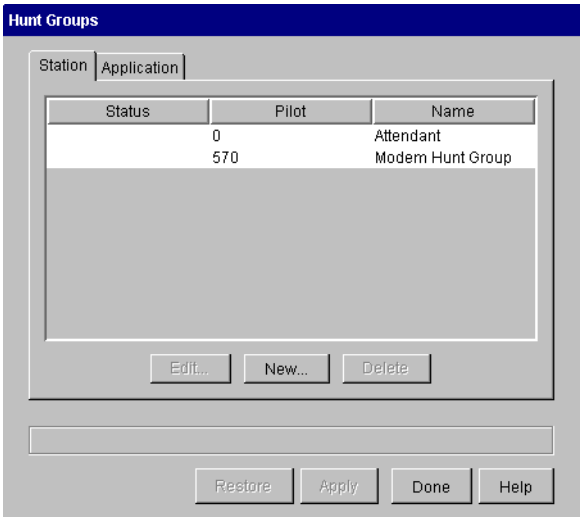


Figure 10-5 Hunt Groups applet

3 Select the Attendant hunt group from the Station tab.

4 Click Edit to open the Station Hunt Group dialog box.

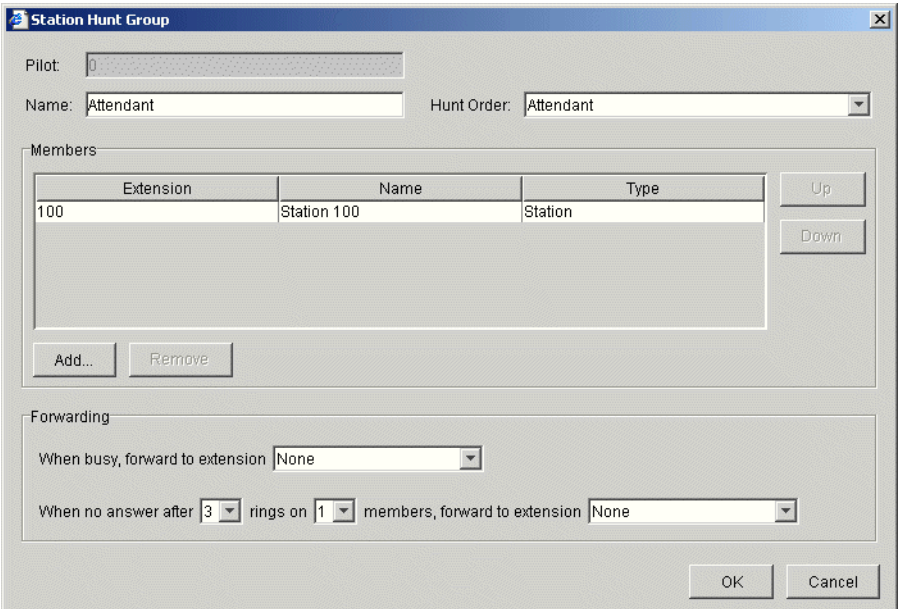


Figure 10-6 Station Hunt Group dialog

Note: The hunt order should be Attendant for this hunt group. Do not change the hunt order.

5 Click Add to open the Add Hunt Group Members dialog box.

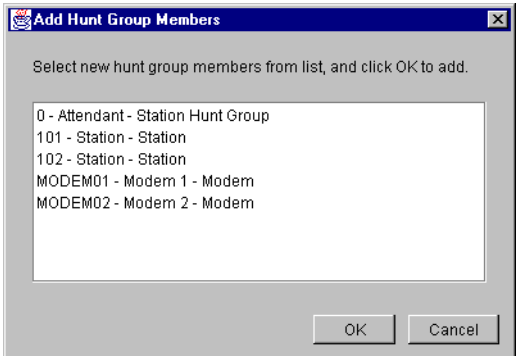


Figure 10-7 Add Hunt Group Members dialog

6 Select the members you wish to add, and click OK.

Use Ctrl-click or Shift-click to select multiple extensions. A maximum of 64 extensions can be in a single hunt group.

7 Set the Forwarding options.

Select forwarding destinations for calls coming into the Attendant hunt group when all the extensions included in the hunt group are busy or do not answer. If you do not select a busy forward destination, callers will hear a busy tone.

The default forwarding destination for the Attendant hunt group is the Voice Mail hunt group pilot number. If you have a main company greeting configured in AutoAttendant the caller will hear the greeting and any prompts you have recorded. You will configure the AutoAttendant menus and greetings later in this chapter.

- Busy Forward—You can specify an extension to which the PBX will forward a call when all of the hunt group member extensions are busy. Generally, you set the When busy, forward to extension to Voice Mail. The caller can leave a message for a hunt group in the mailbox associated with the hunt group pilot number.
- No Answer Forward—When there is no answer, the Wave forwards calls according to the following parameters that you configure.
  - Configure the ring count, or number of rings, before forwarding. The Wave PBX uses ring count to determine when the station should be forwarded to the next member of the hunt group. Keep in mind that a ring cycle is six seconds long, two seconds of ringing and four seconds of silence. Do not configure the hunt group for too many rings or too many stations to ring or the caller will hear only ringing for an extended period and might hang up.
  - Identify the number of stations in the hunt group to be rung in succession. For example, if there are five hunt group members and the number of stations is set to three, only three of the five members will be rung before a call is forwarded to the no-answer destination.
  - Specify an extension—user, hunt group, or Voice Mail—to which the PBX will forward a call when none of the hunt group member extensions answer the incoming call.

Note: When the initial call is placed to a hunt group pilot number, the ring count supersedes the **Ring Phone X Times** count configured in the User dialog box, Phone tab, for extensions in that hunt group.

8 Click OK to close the Station Hunt Group dialog, and return to the Management Console.

Creating a Station hunt group

To create a new Station hunt group:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Hunt Groups icon, located in the PBX Administration section.

3 Click New in the Station tab of the Hunt Groups applet.

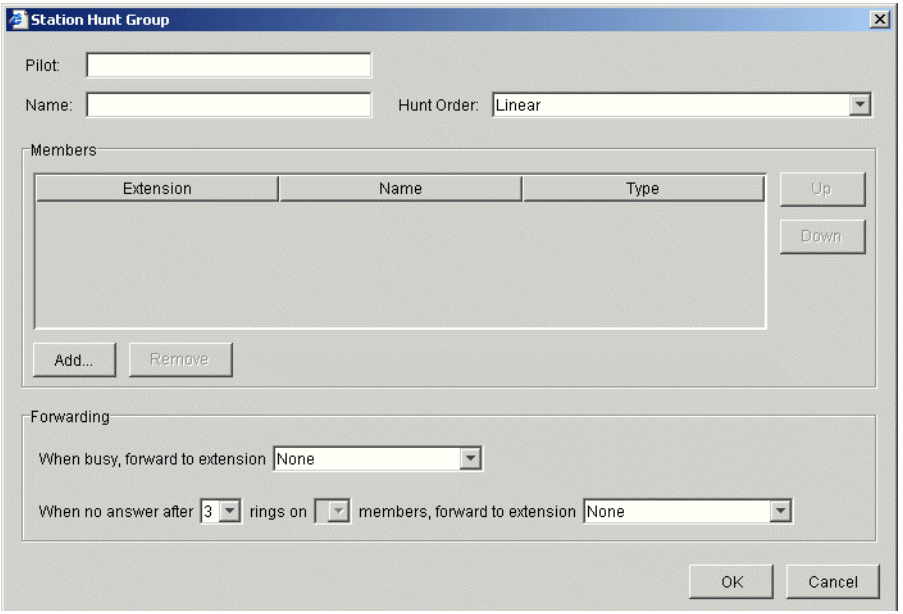


Figure 10-8 Station Hunt Group dialog

4 Enter a unique pilot number for the hunt group in the Pilot field.

A pilot number is the number users dial, or trunk groups use, to reach the members of a hunt group.

The pilot number is similar to an extension:

- it must be unique
- it must fit into your first digit dialing plan for internal numbers
- it must comply with the Internal extension length setting in the First Digit Table

5 Enter a name for the hunt group in the Name field.

You can enter up to 16 alphanumeric characters in the Name field.

6 Select the desired hunting method from the Hunt Order drop-down list.

You have four hunt order options: Linear, Circular, Ring, and Attendant. For descriptions, see “Hunt group hunt orders” on page 28-24.

7 Choose an extension from the When busy, forward to extension drop-down list to which you want to forward calls when all hunt group members are busy.

Select forwarding destinations for calls coming into the hunt group when all the extensions included in the hunt group are busy or do not answer. If you don’t select a busy forwarding destination, callers will hear a busy tone.

For more information about hunt group forwarding settings, see “Configuring the Attendant hunt group” on page 10-20.

8 Click OK to close the Station Hunt Groups dialog box.

The new hunt group appears in the list. To add members to the new group, proceed to step 3 in the next section “Adding members to hunt groups.”

9 Click Apply to save your changes.

10 Click Done to return to the Management Console.

Adding members to hunt groups

Member extensions are the extensions that a hunt group rings when the hunt group pilot number is dialed. Once a hunt group is created, member extensions can be added. A single hunt group can have a maximum of 64 extensions.

To add member extensions to a hunt group:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Hunt Groups icon, located in the PBX Administration section.

3 Click the Station tab.

4 Select the hunt group to which you want to add members.

5 Click Edit.

The Station Hunt Group dialog opens.

6 Click Add.

The Add Hunt Group Members dialog opens.

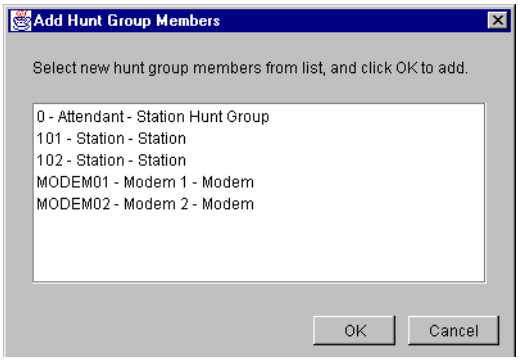


Figure 10-9 Add Hunt Group Members dialog

7 Select the extensions you want to add as members of the hunt group.

Use Ctrl-click or Shift-click to select multiple extensions. A maximum of 64 extensions can be in a single hunt group.

8 Click OK.

The Add Hunt Group Members dialog closes.

9 Click an extension and use the Up and Down buttons to rearrange the order of the extensions in the hunt group, if you desire.

10 Click OK to close the Station Hunt Group dialog, and return to the Management Console.

Managing Users and Roles

CHAPTER CONTENTS

About users

Unlike a traditional PBX, Wave manages phone traffic by user rather than by device, giving the system the flexibility to handle users who move from phone to phone. This chapter explains how to create and manage users and roles. Roles are templates of specific permissions that are used to grant permissions to users (see "Managing roles" on page 11-45).

Warning: *You must have a Station license available for each user that has an assigned internal station ID other than 0. Station IDs of 0 and external stations do not require station licenses.*

Where to set user options

User options are set in both the User / Workgroup Management applet and ViewPoint.

- **Some options can only be set in the User/Workgroup Management applet.** These options are described in detail in this chapter.
- **Some options can only be set in ViewPoint.** These include the user's routing list, contacts, voicemail greetings, call rules, and personal workgroups. To edit these options from the Administrator, select the user in the Users view and choose **Users > Edit All ViewPoint Settings**. See "Modifying a user's ViewPoint settings" on page 11-44. ViewPoint options are described in detail in *Vertical Wave User's Guide*.
- **Some options can be set in both places.** You can set up users with standard defaults for your organization and then individual users can customize the settings further. You also can restrict the options that users can customize.

The Admin user

The Admin user comes pre-defined in Wave, and belongs to the Administrators role. The Admin user and all users who belong to the Administrators role are permitted to run the Administrator application and the Device Monitor application. They also can perform all administrative functions.

You can give individual administrative permissions to any user—for example, permission to shut down the phone system—without making the user a member of the Administrators role. See "Wave permissions" on page 11-49.

Changing the Admin user's password

Immediately after installing Wave, you should change the passwords of the Admin user and Operator user, in order to make your system more secure from unauthorized access. For more information, see Appendix A.

The Users view

You add, edit and delete users in the Users view. To open the Users view:

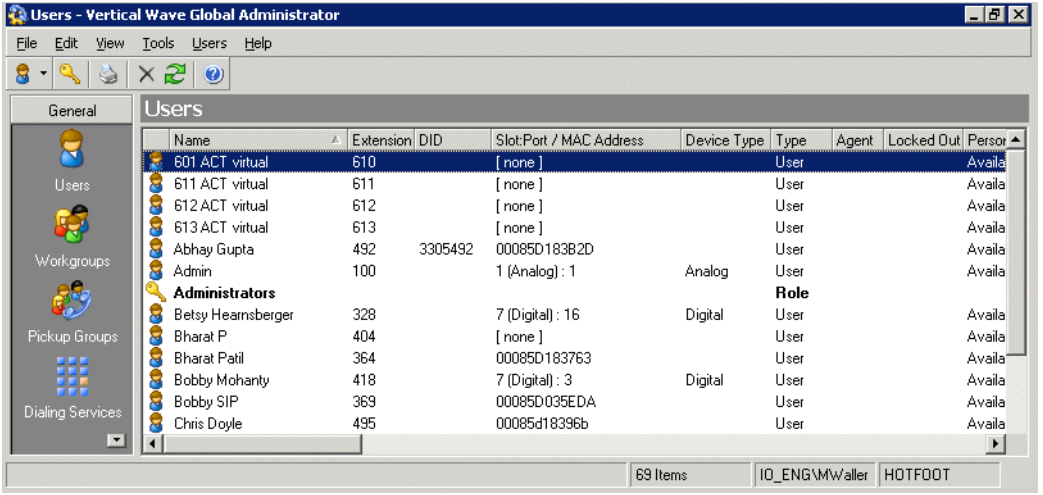
Click

1 If necessary, click the Administration tab of the Management Console.

2 Click the User / Workgroup Management icon, located in the PBX Administration section of the Management Console.

3 Log on to the User / Workgroup Management applet, which opens in a remote access window. Once you log on, the Users view appears.

The Users view presents information about individual users and roles in your organization. Double-click a user in the view to edit that user.



Roles appear in bold in the Users view. For more information about roles, see "Managing roles" on page 11-45.

Each user that you add appears as a row in the Users view. The following table shows the information that is displayed for each user.

Column	Description
Name	User's name.
Extension	Extension number dialed to reach the user.
DID	Direct inward dial number used to dial the user directly.
Station	Default (phone device) assigned to the user.
Device Type	The type of station. The types are: **Analog** **Digital** **IP**
Type	The type of user (see "About users" on page 11-2).
Agent	If checked, the user is an agent in one or more call center queues. See the *Vertical Wave Contact Center Administrator's Guide*.
Locked Out	If checked, the user is unable to log in to his or her account due to multiple failed attempts to access that account as defined in System Settings (see "Enforcing strong password security" on page 4-11).
Personal Status	The name of the user's current personal status.

Column	Description
ACD DND	If checked, the user is not currently accepting ACD workgroup calls.
Mail Usage	Percentage of allocated voicemail space currently used. For details on how the information in this and the following two columns is calculated, see “Viewing the user’s disk usage” on page 11-37.
Greeting Usage	Percentage of allocated greeting and voice title space currently used.
Disk Usage	Amount of disk space in megabytes used by the user's voice message, greeting, and voice title files.
Mailbox Size	Total space allocated to the user for voice messages, in minutes.
Greeting Size	Total space allocated to the user for greetings and voice titles, in minutes.
Forwarding To	Number to which the user is currently forwarding calls.
Gateway Name	Name of the gateway.
Listed	If checked, the user is listed in the dial-by-name directory.
Voice Title	If checked, the user has a recorded voice title. You can record titles for users on the Recordings tab of the User dialog box, or they can record their own.

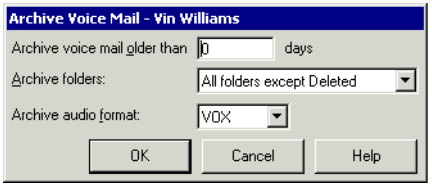
Column	Description
Announce Callers	Displays the types of calls to which the user is applying call announcing.
Exchange Sync	If checked, Wave and Microsoft Exchange Inboxes are synchronized.
Comments	Comments added about the user.

Archiving a user's voicemail and call recordings

You can manually archive a user's voicemail and call recordings from the Users view. Archiving mailbox recordings can save space on your hard drive, especially if the mailbox contains call recordings. For an overview of mailbox archiving and instructions on setting up automatic archiving, see "Archiving call recordings and voice mail" on page 23-34.

To archive a user's mailbox recordings from the Users view:

1 From the Users view, choose **Users > Archive Mailbox Recordings**. The Archive voicemail dialog box opens.



2 Set the following options:

- **Archive voicemail older than __ days.** Enter a number of days. Voicemail older than that will be archived.
- **Archive folders.** Select either "Inbox only" or "All folders except Deleted."
- **Archive audio format.** Select "WAV" or "MP3."

3 Click **OK** to archive the user's mailbox recordings according to the selections made. The recordings are archived in your default archive location (see "Archiving call recordings and voice mail" on page 23-34).

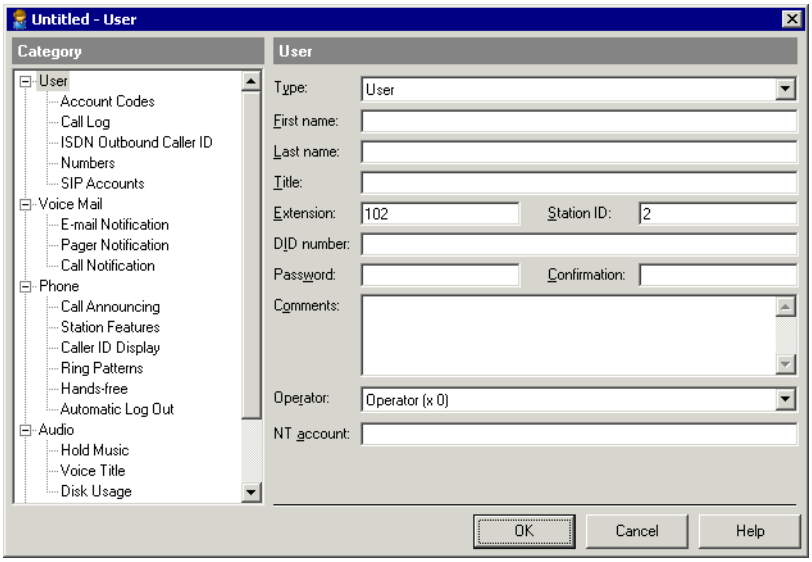
Deleting a user

Deleting a user prevents that user from using Wave and removes all of the user's voicemail files from the system (unless the voice mailbox is being shared with another user). A deleted user's Call Log entries are left in place to maintain an accurate and complete call history on the system.

Note: Before deleting a user you may want to first archive their voice messages to WAV files for later retrieval.

About the User dialog box

To create a user, choose **File > New > User**. The User dialog box opens.



Click in the tree pane on the left to select a tab in the User dialog box. Click a ⊞ to expand a tab category. The following table provides an overview of the tabs, and reference to where each is documented in detail.

User dialog box tab	Overview	See
User	Basic user information, including name, extension, telephone, and password.	p. 11-11
Details	Personal operator and other options	p. 11-13
Account Codes	Whether and under what circumstances Wave prompts the user to enter an account code.	p. 11-14
Call Log	Whether the user's calls are logged, and whether the user belongs to an Organization.	p. 11-14
External Caller ID	Personalized outbound Caller ID information.	p. 11-15
Numbers	The user's personal numbers	p. 11-16
Voice Mail	Voice mailbox size and features, including Exchange synchronization.	p. 11-18
E-Mail Notification	Whether the user is notified of new voice messages by e-mail.	p. 11-20
Pager Notification	Whether the user is notified of new voice messages by page.	p. 11-20
Call Notification	Whether the user is notified of new voice messages by call.	p. 11-20
Phone	Call waiting, ringback, and other phone options	p. 11-29

User dialog box tab	Overview	See
Call Announcing	Verbal announcement of incoming callers' names	p. 11-30
Station Features	Program digital phone feature keys	p. 10-7
Automatic Log Out	Phone login behavior on other users' phones	p. 11-35
Audio	Storage size for greeting and voice title files, and telephone prompt language.	p. 11-36
Hold Music	Personalized hold music source.	p. 11-37
Voice Title	The user's voice title.	p. 11-37
Disk Usage	Space usage report for voice messages, greetings, and voice titles.	p. 11-37
Security	Password expiration control, and whether the user's calls can be supervised.	p. 11-38
Permissions	All user permissions, and the roles to which the user belongs.	p. 11-39
Dialing Permissions	What numbers the user is allowed to dial or disallowed from dialing.	p. 11-41
Dial-by-name Directory	Whether the user is listed in the Wave dial-by-name directory.	p. 11-42
Queue	Not used in this version of Wave.	

User dialog box tab	Overview	See
ViewPoint	ViewPoint application options, including Navigation pane, Tip-of-the-day, and Welcome Wizard options.	p. 11-43

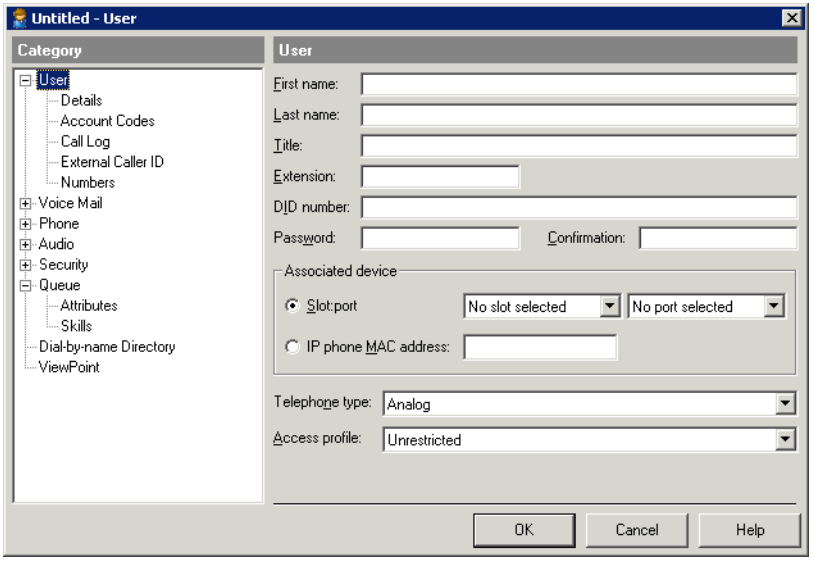
Adding a user by using a template

Create a user, named, for example, “User Template” that has the settings you want all users to share, such as mailbox size and dialing permissions. You can also set up notification options in the template, and you can enable phone features that are applied to all users that are created using the template.

To add a new user based on the template, select the template user in the Users view, and then choose **Edit > Copy.** Choose **Edit > Paste** to open the User dialog box, in which you can customize the new user’s properties, such as first and last name, extension and station ID, e-mail address for notifications, and so on.

The User tab

Choose **File > New > User**, then click **User** in the tree pane.



Identifying the user

In **Type**, choose **User**. Then enter the user's **First name** and **Last name**. You must enter a name in one of the name fields. You can enter the user's **Title** and any **Comments** (such as the user's department) that you want to be displayed along with the user name in the User view.

It can be helpful to use the **Title** field for the user's department, for example, "Sales." When a caller requests to be transferred to someone in Sales, the Operator can see all the users in the Sales department grouped together in ViewPoint's Transfer Call dialog box. You can also use workgroups to group users by department (see Chapter 12).

Assigning an extension

A user's extension is the number callers dial to reach the user. Extensions must comply with the following restrictions:

- Must match the First Digit rules for length and digits allowed
- No longer than 10 digits
- Numeric characters only
- Must be unique

In addition, follow these recommendations when assigning extensions:

- Avoid extensions that begin with another extension or access code. For example, if one user is given extension 17 and another extension 177, users who dial extension 17 will experience a brief delay while Wave waits to see if another "7" is dialed.
- Avoid extensions that begin with the same number used for an auto attendant menu choice. Slow dialers may be unable to dial the extension at the auto attendant, because they will activate the menu choice instead. See "Creating a new auto attendant" on page 13-3.
- Avoid extensions that begin with frequently dialed area codes—if users forget to dial an access code, they may unexpectedly dial the extension instead. For example, if 1-617 is a commonly dialed prefix for your location, do not assign extension 161.

Creating a password

Enter a numeric **Password** that controls access to the user's voicemail and account options. This password also allows the user to log on to ViewPoint. The user's password can be changed either on this tab or in ViewPoint.

Retype the new password in the **Confirmation** field.

Note: Assigning secure passwords is one of the key means by which you can protect your business from unauthorized access, and lost money due to toll fraud. See Appendix A.

Selecting a telephone

Use the fields under **Associated device** to select the user's telephone, as follows:

1 If the user has an analog or digital telephone, select the approriate slot and port for that phone from the **Slot/Port** drop-down list.

   If the user has an IP telephone, select **IP telephone MAC address** and enter the MAC address of the user's IP telphone.

2 Select the appropriate **Telephone type** from the dropdown list.

3 Select an **Access Profile** from the drop-down list.

   The access profiles in the drop-down list are obtained from profiles you configured in the Outbound Routing applet. See "Configuring specific access profiles" on page 9-10.

Selecting a telephone automatically

You can also assign a digital telephone to a user automatically when you plug in the phone. To do so:

1 Create users as described in this chapter, leaving the **Associated device** fields blank.

2 Plug a digital phone into the Wave ISM.

3 Press BEGIN on the phone's display. You can then scroll through a list of users who have no phone assigned, and select the one you want.

The User \ Details tab

The User \ Details tab lets you enter descriptive comments and other information about the user.

Entering comments

Use the **Comments** field to enter descriptive comments about the user as needed.

Setting up a personal operator

By default, Wave dials the Operator user's extension whenever a caller presses 0 while listening to a user's greeting or leaving a message. To transfer calls to another user instead (for example, a departmental operator, personal assistant, or other auto attendant), select the user to whom you want to transfer calls from the **Operator**

dropdown list on the General tab. For more information about operators, see “The Admin user” on page 11-2. A personal operator can be also be set in ViewPoint.

Entering the user’s Microsoft Windows NT account

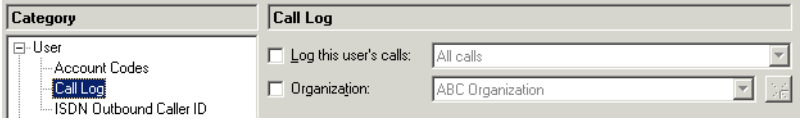
In the **NT account** field, enter the user’s Windows network account name, for example, MAIN\MAnatolia or WORKGROUP\John. This field is primarily for use by Add-ins and Client API developers.

The User \ Account Codes tab

The User \ Account Codes tab lets you set up the user’s account code modes. Account code modes determine whether and under what circumstances Wave prompts the user to enter an account code. For instructions, see “Setting a user’s account code modes” on page 21-9. For an overview of account codes, see “Using account codes” on page 21-6.

The User \ Call Log tab

The User \ Call Log tab lets you define how the user’s calls appear in the Call Log in terms of which calls are logged, whether they are associated with an Organization, and what happens if the user logs onto another user’s station. For more information on the Call Log, see “Using the Call Log view” on page 23-5.



Determining which calls are logged

By default, all inbound and outbound calls made by the user appear in the Call Log. However, there are times when you might not want to log a user’s calls due to space or readability reasons, for example if the user’s station is connected to a fax server used for sending thousands of faxes daily.

To turn off call logging for the user, uncheck **Log this user's calls**. If checked, you can choose whether to log the user's inbound calls, outbound calls, or both.

Notes

- If you turn off call logging for a call center agent, you will not be able to run reports on the agent's personal calls. Reports on queue calls and all statistics in the Queue Monitor are unaffected.
- Users with call logging turned off cannot use ViewPoint's callback feature (File > Return Last Call) or the list of recently dialed calls on ViewPoint's File menu.
- If you have turned off internal call logging at the system level (see "Setting Call Log options" on page 23-12), the user's internal calls will not be logged, regardless of this setting.

Associating the user with an Organization

If you have created one or more Organizations, you can associate the user with the Organization to which he or she belongs. Calls that the user places or receives will be logged with that Organization showing in the Call Log's Organization column. Organizations are a means of setting up multiple companies that share an office and a Wave ISM. See "Using Organizations" on page 21-2.

To associate the user with an Organization, check **Organization**, and select an Organization from the dropdown list.

If unchecked, the user's calls will appear in the Call Log with the Organization column blank.

The User \ External Caller ID tab

You can customize the Caller ID number and name that accompany outbound calls placed by the user. Note that the user can make his or her own selection in ViewPoint, but cannot specify a different custom number or name. If the user selects Custom, the Caller ID number and name are what is entered here.

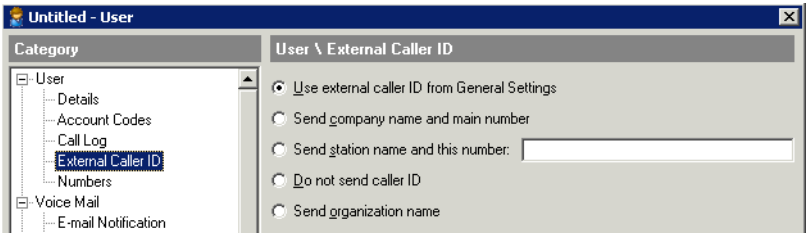
By default all users send the External Caller ID format specified in the General Settings applet (see "Configuring systemwide Caller ID settings" on page 18-10). This

procedure is only necessary if you want to override the systemwide caller ID settings for a user.

To configure user-specific external caller ID settings:

1 Edit or create a user in the User / Workgroup Management applet's User dialog box.

2 Click the User \ External Caller ID tab.



3 Select an External Caller ID setting:

- **Use External Caller ID from General Settings.** Sends the default settings configured in the General Settings applet
- **Send Company Name and Main Number.** Sends the Company Name and Company Main Number (entered in the General Settings applet)
- **Send Station Name and this Number.** Sends the phone's station name Display Name (entered in User Configuration (Templates)) followed by the digits you enter here.

  Use this setting to provide the station name and DID number on outbound calls.
- **Do Not Send Caller ID.** Sends no Caller ID.

The User \ Numbers tab

The User \ Numbers tab lets you view and edit the numbers that appear in the user's "My Numbers" list in ViewPoint. You can also enable automatic login for the user as a whole and for each of the user's numbers. For more information, see "Enabling automatic logon for users" on page 11-43.

To enter or edit a user's number:

1. Click the type of number you want to enter or modify, for example **Home** or **Mobile**, then click **Edit**.

   To delete a number, click it, then click **Clear**.

2. If the **Call Using** field is present, select the dialing service to use when placing calls to this number.

3. In the **Number**, **Address**, **Email**, or **IM address** field, enter the phone number, IP address, email address or instant messaging address.

4. Check **Public** to give other programs access to the number, for example, an add-in that automatically dials certain numbers. If unchecked, other programs cannot read or access the number.

5. Check **Use to authenticate** to enable this number for automatic login when the user calls the system from it. If automatic login is enabled either for the user as a whole (see the next section) or the auto attendant that takes the call, the user is automatically authenticated and can access his or her account without being prompted for a password. See “Enabling automatic logon for users” on page 11-43.

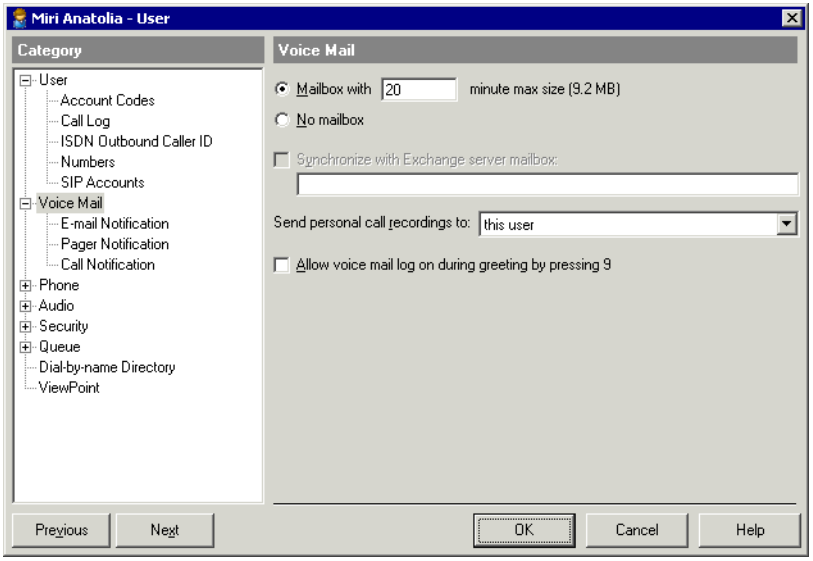
6. Click **OK** to return to the User dialog box.

Enabling the user for automatic login

Check **Authenticate trunk calls via Caller ID** to enable the user for automatic login. With this checked, whenever the user calls the system from a number with **Use to authenticate** checked (see the previous section), the user is automatically authenticated and can access his or her account without being prompted for a password. See “Enabling automatic logon for users” on page 11-43.

The Voice Mail tab

Choose **File > New > User**, then click **Voice Mail** in the tree pane.



Configuring the user's voice mailbox

In **Mailbox with __ minute max size**, enter the maximum size of the mailbox, in minutes. Mailboxes can be as large as 999,999 minutes (447 GB).

Choose the default setting of 20 minutes (9.2 MB of storage) for typical users. You may need to increase the default for users who record calls, because call recordings (including those that were e-mailed to the user) are stored in the user's mailbox.

Note: Voice messages take up disk space on the Wave ISM computer. Once available disk space becomes scarce, system performance will suffer. To avoid this problem, archive your users' voice messages and call recordings regularly. See "Archiving call recordings and voice mail" on page 23-34.

To create an extension without a voice mailbox—for example, a conference room or fax machine—click **No mailbox.**

Enabling Microsoft Exchange Server synchronization

You can enable synchronization of a user's Wave voice messages with the corresponding e-mail notifications in Exchange.

To enable synchronization:

1. Check **Synchronize with Exchange Server mailbox.** If this control is disabled, first set up Exchange Server notification on the E-mail Notification \ Exchange Synchronization tab of the System Settings dialog box. For more information, see "Setting up e-mail notification" on page 4-10.
2. Enter the user's Exchange Server mailbox. This can be obtained from Microsoft Exchange.

   Note: Exchange Server mailboxes must not be confused with the e-mail address supplied when setting up e-mail notification for the user (see "Setting e-mail notification" on page 11-22). One of the e-mail addresses specified for the user for e-mail notification must route e-mail to the Exchange Server mailbox that you specify here.

Choosing the mailbox for call recordings

By default, call recordings that the user makes manually from ViewPoint's Call Monitor are sent to the mailbox of the user who made them. To send personal recordings to another user's mailbox instead, select a name from the **Send personal call recordings to** dropdown list.

Note: This field applies only to call recordings manually made by the user. The destination for automatic call recordings made by the system and by queues are set separately. See Chapter 20 and the *Vertical Wave Contact Center Administrator's Guide*.

Enabling voicemail greeting logon

By default, users can log on to their Wave accounts from a Wave station or auto attendant only. You can also choose to let this user log on by pressing 9 during his or her voicemail greeting. (For this type of logon, the user is prompted only for password.) If you have a DID-based system without auto attendants, you should enable this feature for all users, because it is the only way for them to access their

accounts remotely. To enable the feature, check **Allow voicemail log on during greeting by pressing 9**.

Note: voicemail greeting logon can be slightly less secure than auto attendant logon, because the caller does not need to know the extension number. If you enable voicemail greeting logon, you should enforce secure passwords. See “Enforcing strong password security” on page 4-11.

The Voicemail \ Notification tabs

Expand the Voicemail tab category to select the E-Mail, Pager, and Call Notification tabs.

You can have Wave notify a user by e-mail, page, or phone call whenever he or she receives a new voice message. This powerful feature enables users to keep abreast of their Wave voicemail no matter where they are. Notification messages include important details about the call, and give users quick access to hearing the message and responding to it. You have notifications sent for all voice messages or for Urgent messages only. You can also have notifications sent only at certain days or times.

Users can also configure notifications in ViewPoint.

Note: Paging and call notification will not work with access codes that route over PRI trunks unless you make configuration changes. See “Enabling paging and notification on PRI trunks” on page 5-23 for details.

Note: Notifications are sent only for new voice messages, not new call recordings that arrive in a user’s Inbox.

Notification information

The following information is attached to notifications of each type, making them a powerful tool for voicemail management, even at a remote location.

E-mail notifications can contain:

- Caller’s name
- Phone number at which the call originated

- Wave extension at which the message was left
- Voice message length
- Notes associated with the message
- Voice message as a .WAV file attachment

Pager notifications can optionally contain:

- Caller ID for message
- Wave extension that was dialed
- Voice message length

Call notifications contain:

- Voice title of the user who received the message
- Voice title or recorded name of the person who left the message, if available
- Identification of urgent messages
- Length of the voice message
- Ability to press **#** right from the call and hear the message, then press **43** to call them back.

Note: You can use call notifications to log onto your account from a remote location and have Wave pay for the call rather than your remote phone. See Chapter 6 of *Vertical Wave User's Guide*.

Determining which voice messages send notification

For each notification type—e-mail, pager, and call—you can define how often notifications are sent, using the following dropdown list options:

- **Do not send notifications.** The user does not receive notification of new voice messages.
- **Send notification for all messages.** The user receives a notification whenever new voice messages arrive.
- **Send for Urgent messages only.** The user receives a notification whenever voice messages marked Urgent arrive.

Setting e-mail notification

Make sure e-mail notification is configured properly as described in *Vertical Wave Installation Guide*. See "Configuring e-mail notification support" in Chapter 10 of that manual for more information.

1. Select the E-mail Notification tab.
2. Select whether e-mail notifications occur, and if so, how often. See the previous section.
3. In the **E-mail address(es)** field, enter the e-mail address to which notifications are sent. Separate multiple addresses by semicolons (;).

   Note: If using SMTP, valid e-mail addresses must be in the format of `user@company.com`. If using MAPI, e-mail addresses must be resolvable via the Microsoft Outlook address book.
4. In the next dropdown list, choose whether the voice message is attached to the e-mail as a .WAV file, by selecting one of the following:
   - **Do not attach voice message.** The voice message is not attached to the e-mail.
   - **Attach voice message.** Messages are attached to the e-mail and also appear in the user's Wave Inbox marked as unheard.
   - **Attach voice message and mark as already heard.** Messages are attached to the e-mail and appear in the user's Inbox marked as already heard.
   - **Attach voice message and delete from Inbox.** Messages are attached to the e-mail only, and do not appear in the user's Wave Inbox. You cannot select this option if Exchange synchronization is enabled for a user (see "Enabling Microsoft Exchange Server synchronization" on page 11-19).

Setting pager notification

1. Select the Pager Notification tab.
2. Select whether pager notifications occur, and if so, how often. See "Determining which voice messages send notification" on page 11-21.
3. In the **Page using** field, select the dialing service that you want Wave to use to dial the user's pager.

4 In the **Dial Sequence** field, enter the dial string for the pager, including the phone number of the paging service and the pager's PIN if required. The dial string can contain any touch tone digit (0-9, *, #). You can enter commas to indicate 1-second pauses in the dial sequence.

   You can also use the following special characters to add information to the page:

   - I or i sends the Caller ID number (for an external call) or Wave extension (for an internal call).
   - E or e sends the Wave extension that the caller dialed.
   - L or l sends the length of the voice message in seconds.

For example, the dial sequence `18007771000,,,1245983#E` causes Wave to dial the paging service, pause for 3 seconds, enter the pager's PIN (1245983) followed by # to indicate end-of-PIN, enter your extension (where the voice message was left), and then hang up. In this example, your pager displays only the extension number.

If users receive only the last portion of the pager data specified, there are not enough pauses between the pager number and the information. If this problem occurs, add more commas.

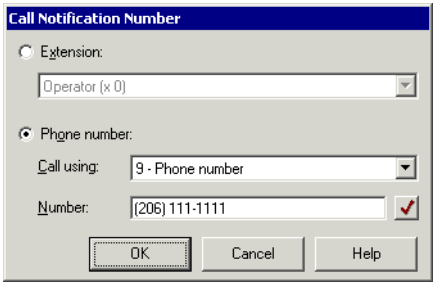
Note: Do not enter multiple stars (*) in a row in the pager string. Use only one star to send a dash. Multiple consecutive stars can terminate the page message.

Setting call notification

1 Select the Call Notification tab.

2 Select whether call notifications occur, and if so, how often. See "Determining which voice messages send notification" on page 11-21.

3 Click ... in the **Number** field to open the Call Notification Number dialog box.



4 Choose one of the following options:

- Click **Extension** and select an extension from the dropdown list.
- For an external number, use the **Call Using** dropdown list to select the access code and dialing service to use when placing notification calls. Then enter the number to dial in **Number**, exactly as it should be dialed.

5 Click **OK**.

Scheduling notifications

If you do not want to receive notifications 24 hours a day, 7 days a week, you can schedule notifications to occur at specific times only. For example, you can have Wave send notifications only during business hours or after business hours on work days. You can also set up custom hours. You can create different schedules for e-mail, pager, and call notification. Notifications can also be scheduled in ViewPoint.

Note: When you turn notification on for a user, by default Wave sends notifications 24 hours a day, 7 days a week. If this is what you want to do, you do not need to schedule notifications.

Note: Notifications are never queued for later delivery. When you use a schedule, voice messages that arrive during an unscheduled time do not produce notifications at all.

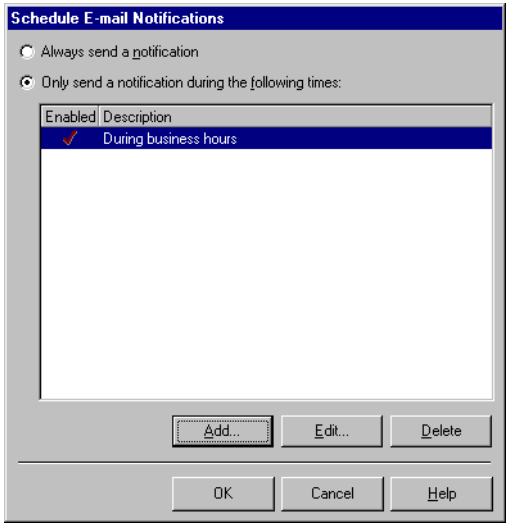
A schedule contains individual schedule entries. For example, if you want a user to be notified of new voice messages during business hours and all day on holidays, you would add a schedule entry for "during business hours" and another schedule entry for "on holidays." You (or users) can define custom schedule entries for even greater precision.

You can enable or disable each schedule entry as needed. For example, if you do not want a user to be paged during a specific upcoming holiday, disable the schedule entry for "on holidays." You can enable it after the holiday has passed.

Defining a schedule for notifications

After setting the options in the e-mail, pager, or call section on the Notifications tab, click **Schedule** in the appropriate section to define a schedule for notification. The

Schedule (E-mail / Pager / Call) Notifications dialog box opens. The **Schedule** button is unavailable until you have created notification settings on the Notifications tab.

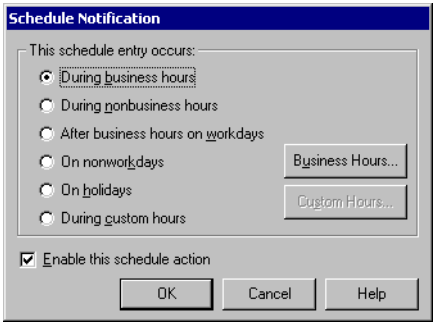


The Schedule Notifications dialog box lists the schedules that have been defined so far, if any. Click one of the following:

- **Always send a notification.** The schedule entries in the list (if any have been created) are ignored, and the user receives notification of new voice messages at all times.
- **Only send a notification during the following times.** The user receives notification only during the times specified in the schedule entries that appear in the list with a check mark in the Enabled column.

To add a schedule entry:

1 To add a schedule entry, click **Add**. The Schedule Notification dialog box opens.



2 To view or change the business and holiday hours used for scheduling, or to create other sets of business hours, click **Business Hours**. See “Setting business hours” on page 4-6

3 Under **This schedule entry occurs**, choose one or more of the following time periods during which you want to notify the user of new voice messages. For purposes of illustration, each of the time periods in the following list show in parentheses what would be the result of selecting that time period in a company whose business hours are Monday through Friday, from 9:00 a.m. to 5:00 p.m.

- **During business hours.** (Notifications are sent during business hours, Monday through Friday, from 9:00 a.m. to 5:00 p.m.)
- **During nonbusiness hours.** (Notifications are sent at all times other than business hours, including early mornings, evenings, weekends, and holidays. Notifications are sent Monday through Friday, 5:01 p.m. to 8:59 a.m., and on Saturdays, Sundays, and holidays.)
- **After business hours on workdays.** (Notifications are sent Monday through Friday, 5:01 p.m. to 8:59 a.m.)
- **On nonworkdays**. (Notifications are sent on Saturdays and Sundays.)
- **On holidays.** (Notifications are sent on holidays.) See “Setting business hours” on page 4-6.
- **During custom hours.** (Notifications are sent during specific days and hours independent of the business and holiday hours already defined.) See “Setting up custom hours” on page 11-27.

4 Be sure to check **Enable this schedule action**, and then click **OK**. Now the schedule in the Schedule Notifications dialog box includes the schedule entry you just created. Add more schedule entries as needed, and then click **OK** when you are finished.

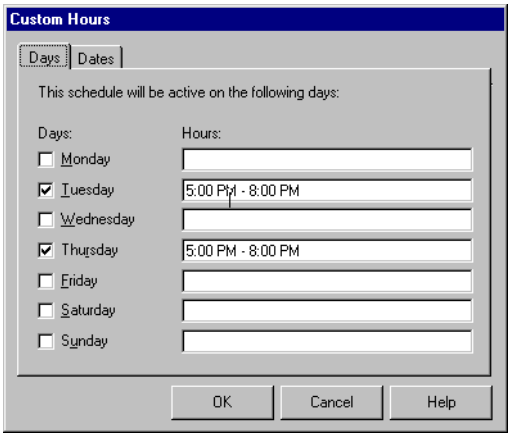
Setting up custom hours

You can define custom hours that are not related to your office's business hours and holidays and use them to schedule notifications, auto attendant actions, and routing list actions. Custom hours are specific to the user, auto attendant, or routing list for which you create them. That is, the custom hours you set up for a user do not apply automatically to other users. Custom hours for a user can also be set up in ViewPoint.

When setting custom hours, you can enter dates and times in most formats—they are converted to a standard format based on your Windows regional settings.

To set custom hours:

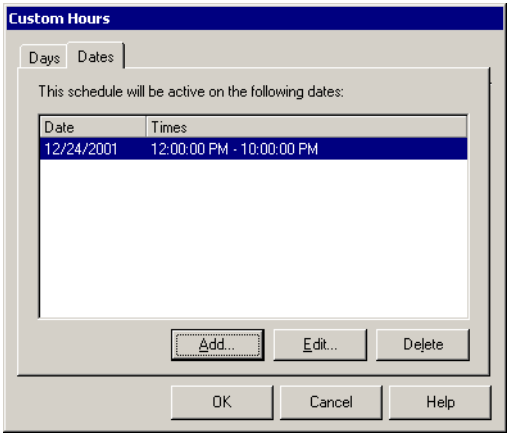
1 Click **Custom Hours** in either the Schedule Notification dialog box (for users) or the Schedule Action dialog box (for auto attendants). The Custom Hours dialog box opens.



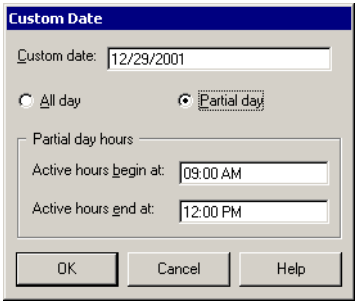
2 On the Days tab, check each day of the week for which you want the custom schedule to be active. If you leave the **Hours** field blank for a selected day, the entire day is included in the custom schedule. To include only part of a day, enter starting and ending hours.

Note: You can enter multiple time ranges separated by commas, for example, "9:00 AM - 12:00 PM, 3:00 PM - 6:00 PM."

3 On the Dates tab, click **Add** if you want to apply the custom schedule to a specific date.



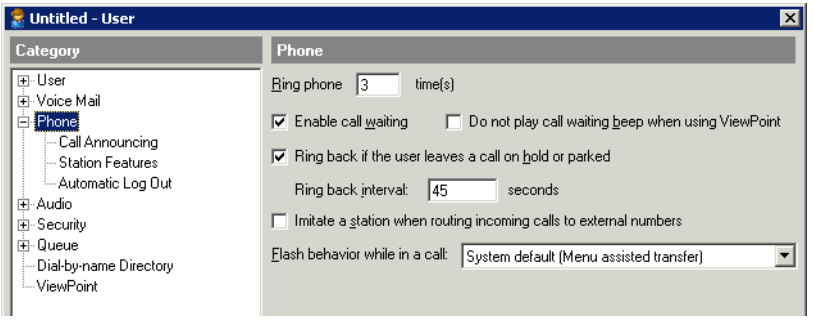
4 In the Custom Date dialog box that opens, enter the **Custom date**, and then click **All day** or **Partial day.** For a partial day, enter starting and ending times.



5 Click **OK** to add the custom date to the list on the Dates tab of the Custom Hours dialog box.

The Phone tab

Use the Phone tab to configure the user's phone. Choose Choose **File > New > User**, then click the Phone tab.



Setting the number rings for the phone

In the **Ring phone __ times** field, enter the number of times Wave rings the user's extension before proceeding to the next action in the user's routing list. This option can also be set in ViewPoint.

Using call waiting

To give the user call waiting, check **Enable call waiting**. If unchecked, when the user is on a call new calls go straight to voicemail without playing the call waiting beep.

If the user uses ViewPoint's Call Monitor folder to spot incoming calls, and thus does not want the audible beep over the phone, check **Do not play call waiting beep when using ViewPoint.** The beep will play only when the user is not running ViewPoint.

Configuring ringback behavior

Check **Ring back if the user leaves a call on hold or parked** to use Wave's ringback feature, which rings the user back if he or she leaves a call on hold or parked for too long. If checked, enter the **Ring back interval** in seconds to specify how long Wave waits before ringing the user back.

Configuring Flash behavior

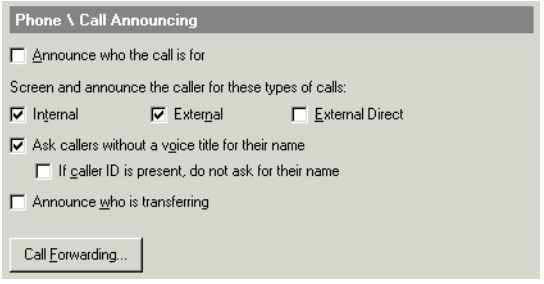
This section does not apply to digital phones.

You can use the **Flash behavior while in a call** field to select what happens when this user presses Flash (or quickly presses the hook) while on a call. The options are as follows:

- **System default.** The user's behavior is whatever you have chosen as the system-wide behavior. See "Setting general Wave options" on page 4-3.
- **Menu assisted transfer.** Pressing Flash takes the user to a menu giving you options for transferring the call.
- **Direct transfer.** Pressing Flash lets the user immediately enter an extension to transfer the call. Choose this option to create faster, simplified telephone transferring for a user who answers and transfers many calls. Note that with direct transfer, the user cannot access Conference or the other commands on the call handling menu unless he or she has ViewPoint.
- **Manage current call.** Pressing Flash takes the user to the Wave call handling menu, of which one of the options is transferring the call (for details, see Appendix A of *Vertical Wave User's Guide*).

The Phone \ Call Announcing tab

Use the Phone \ Call Announcing tab in the User dialog box to set call screening, announcing, and forwarding options for the user's phone.



Announcing who the call is for

With **Announce who the call is for** checked, when the user picks up the phone he or she hears a recorded message that says "Call for," followed by the name of the user being called. This setting is useful when users are sharing a station.

Customizing or turning off call announcing

Call announcing allows the user to screen callers using their telephone. When the user answers his or her phone, Wave plays, "Call from," followed by the name of the caller. The user can then accept or decline the call (see *Vertical Wave User's Guide* for detailed instructions).

Under **Screen and announce the caller for these types of calls**, choose any of the following:

- **Internal.** Calls from other Wave users.
- **External.** Calls from external callers who reached the auto attendant (including those transferred to the user by another user).
- **External Direct.** Calls from external callers who dialed the user's DID number.

To turn call announcing off for a type of call, uncheck it for that type. With call announcing turned off, the user is connected directly to the caller when he or she answers the phone.

Other call announcing options

Use the following options in conjunction with call announcing:

- **Ask callers without a voice title for their names**. By default, if call announcing is turned on, contacts and users without voice titles are prompted to say their names. When you pick up the phone, you hear, "Call from," followed by what they say. If you uncheck this field, callers are not prompted to say their names.

  With this field unchecked, when you receive a call from a caller without a voice title you will hear either "Call from internal user," "Call from external caller," or "Call from contact," depending on the caller.

- **If Caller ID is present, do not ask for their name.** If checked, incoming callers with Caller ID are not prompted to say their names. This is a useful setting if you have

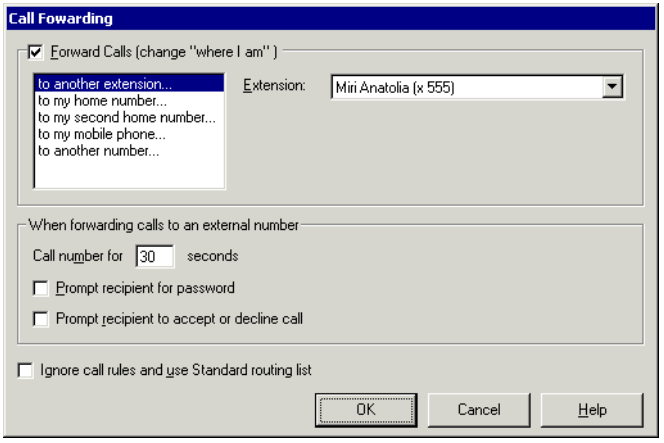
a phone with a Caller ID display. You can skip asking the caller for a name if you can see on your Caller ID display who is calling.

If unchecked, all callers without voice titles are prompted to say their names.

- **Announce who is transferring.** Check this option if you want to hear the name of the person transferring a call to you. For example, if checked, you would hear "Helen Shire is transferring a call from Shane West." To announce who is transferring, you must have call announcing turned on for internal calls. If it is not turned on, you are connected directly to transferred calls.

Forwarding the user's calls

Click **Call Forwarding** on the Phone \ Call Announcing tab to forward the user's calls. The Call Forwarding dialog box opens.



To forward the user's calls, do the following:

1. Check **Forward calls**.
2. Select the type of forwarding destination in the list below.
3. Enter the forwarding extension or phone number. For external numbers, select the dialing service to use from the **Call Using** dropdown list.

For an explanation of Attempt Centrex/PBX transfer, see "Forwarding calls over Centrex/PBX trunks" on page 11-34.

You can also set the following call forwarding options:

- **Call number for __ seconds.** Determines for how long a call rings at the forwarded phone before proceeding to the next step on the user's routing list (usually voicemail). If the option **Prompt recipient for password** or **Prompt recipient to accept or decline call** is checked (described below), you must allow at least 30 seconds. Otherwise the call might be sent to voicemail before the user finishes listening and responding to the prompts.
- **Prompt recipient for password.** If checked, the person who picks up the phone hears, "Call for <the user's voice title>. Please connect me." To be connected to the caller, the recipient must enter the user's Wave password. Choosing this option ensures that only users can receive their forwarded calls.

  This option is used only when calls are forwarded to an external number and the user has a voice title recorded.
- **Prompt recipient to accept or decline call.** If checked, when the user picks up the phone, Wave announces the caller ("Call from") and intended recipient ("Call for") and offers the option to accept or decline the call. Declined calls proceed to the next step in the user's routing list, usually voicemail.

  Note: When you forward calls to a mobile phone, make sure that you check **Prompt recipient to accept or decline call**. See the next section, "Mobile phone issues with forwarded calls."
- Select **Ignore call rules and use Standard routing list** if you want to send all of the user's incoming calls to the forwarded phone. This setting disables the user's call rules and uses the Standard routing list for all calls. See *Vertical Wave User's Guide* for an explanation of routing lists and call rules.

  Leaving this field unchecked keeps the user's active routing list and call rules in effect, which means that some calls might ring elsewhere than the forwarded phone.

Mobile phone issues with forwarded calls

Calls to a mobile phone are picked up by the mobile phone company first and then passed to the individual phone. When Wave detects the first pickup, it stops proceeding down the routing list, whether or not anyone has actually answered the mobile phone. For this reason, when forwarding calls to a mobile phone, always check **Prompt recipient to accept or decline call**. Wave then relies on user input to signal a connection. Wave proceeds down the routing list unless someone explicitly accepts the forwarded call.

Call forwarding and voicemail

If a forwarded call is not answered, it is sent to the user's voicemail.

To completely transfer a user's calls to another user's phone, so that the other user receives voicemail as well as the calls themselves, do not use call forwarding. Instead, use ViewPoint to create a routing list whose final (and only) action is Transfer to Extension, and make it the user's active routing list. See *Vertical Wave User's Guide.*

Forwarding calls over Centrex/PBX trunks

In certain circumstances you can use the option **Attempt Centrex/PBX transfer** when forwarding calls to external numbers, which economizes Wave trunk usage. You can use this option if your ISM has either of the following:

- Centrex trunks
- ISDN trunks with Two B-Channel Transfer enabled
- A connection to an external PBX
- A connection to a SIP / PSTN Gateway device

If this option is checked when a trunk call would be forwarded to an external number, Wave attempts to have the carrier create a direct transfer from the origin number to the external forwarding number, thus saving two Wave trunks.

If the requirements for Centrex / PBX transfer are not present—for example, on a normal analog trunks—Wave forwards the call to the external number in the usual way, using a second trunk.

Note: When a call is routed out using a Centrex / PBX transfer, Wave loses control of it and cannot send it to subsequent steps on the user's routing list. For example, after a call is transferred using Centrex / PBX, it does not go to voicemail.

Note: Centrex / PBX transfer is never used in the following situations: supervised transfers, transferring a conference call, routing from a workgroup, or transfers involving call center agents.

This option is also available when specifying external phone numbers in a user's routing list. See *Vertical Wave User's Guide.*

The Phone \ Automatic Log Out tab

This tab applies to all phone types (analog internal and external stations, and digital phones).

If the user has logged in at another user's workstation—using either ViewPoint or the telephone commands—the setting on the User dialog box's Phone \ Automatic Log Out tab determines how much inactive time elapses before the user is automatically logged out and the station is reset to its default user. This feature is useful if a roaming user walks away from a phone without logging out. Enter the number of minutes in **Automatically log out of other user's stations after __ minutes of inactivity.**

All calls are written to the Call Log according to the user logged in at the station, so a user can log in anywhere in the office and make calls that are logged correctly under his or her name. Calls from the station continue to be logged under the visiting user's name until one of the following happens:

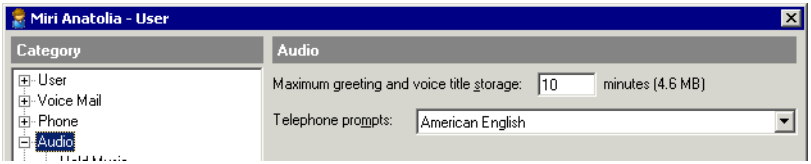
- The visiting user logs out, either by pressing ***00** at the dial tone or by choosing **File > Exit and Log Off** in ViewPoint. This resets the station to its default user.
- Another user logs in to the station using ViewPoint or telephone commands. This resets the station to the new user.
- The amount of time specified in **Automatically log out of other user's stations after __ minutes of inactivity** is exceeded. This resets the station to the default user. Inactivity is defined as any time except during active calls (inbound or outbound) and when telephone commands are used that require entering a password (for example, logging into the phone to listen to voicemail). All other station activity, such as picking up the phone and dialing *14, or using ViewPoint to play a voice message over the station, count as inactivity.

Note: Incoming calls for other users, such as calls forwarded to the station, do not count as activity even if they are answered.

Uncheck **Automatically log out of other user's stations after __ minutes of inactivity** to prevent resetting the station after any amount of inactivity.

The Audio tab

Choose **File > New > User**, then click the Audio tab.



Setting the storage size for greetings and voice titles

In the **Maximum greeting and voice title storage** field, enter how many minutes worth of audio files this user can store for greetings and voice titles. These voice file types include the following:

- **Greetings.** All greetings displayed in ViewPoint's Greetings view, plus the user's grab-and-hold greeting.
- **Voice titles.** The user's own voice title plus all voice titles for the user's contacts.

The default setting of 10 minutes requires 4.6 MB of storage. The Administrator opens a warning message if the total allotment of voice message and greeting space for all users exceeds the available disk space on the Wave ISM.

Choosing a language for telephone prompts

From the **Telephone prompts** dropdown list, choose the language that Wave system prompts will play in for this user. When the user logs on or is identified on the telephone, Wave automatically switches to this language for all subsequent system prompts during the call. The language can be also be set in ViewPoint. This setting does not affect any prompts that other callers or users hear.

The list shows the languages currently installed. You must reinstall the Wave ISM to add other languages. See *Vertical Wave Installation Guide*.

The Audio \ Hold Music, Voice Title, and Disk Usage tabs

Expand the Audio tab category to select the Audio \ Hold Music, Audio \ Voice Title, and Audio \ Disk Usage tabs.

Setting the user's hold music

Users can have individualized hold music that is different from the default system hold music. A user's hold music is heard by callers whenever the user puts them on hold. A user's hold music can come from any station that you have set up as a music-on-hold device.

To customize hold music for a user:

1. Expand the Audio tab category and select the Hold Music tab.
2. From the **Music on hold** drop-down list, select the music-on-hold source.

Recording the user's voice title

Expand the Audio tab category to select the Voice Title tab, where you can record the user's voice title.

A user's voice title is a short recording consisting only of the user's name. Wave uses the voice title in several prompts, for example, the call screening prompt when the user calls another user (the user receiving the call hears "Call from <voice title>"). Users can record their voice titles themselves in their own voices, using either the telephone commands or ViewPoint. However, since the voice title is a critical part of the Wave system (for example, users without a voice title are not listed in the dial-by-name directory), it is recommended that you record them, after which those users who want to re-record them can do so.

To record the voice title, use the audio controls.

Viewing the user's disk usage

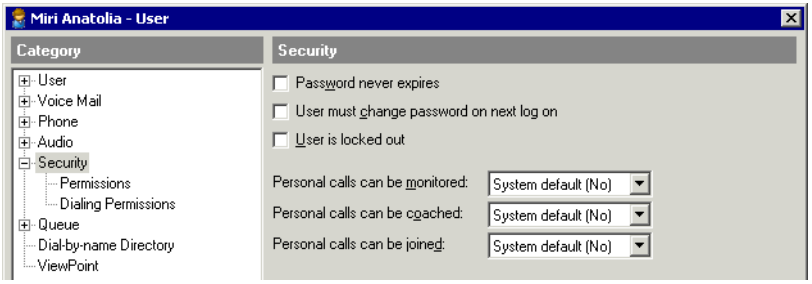
Expand the Audio tab category to select the Disk Usage tab, which displays how much space the user's audio files are taking up. The percentage of allocated space is also displayed.

To avoid slowing the opening and scrolling of the Users view, Wave does not dynamically recalculate these totals. Totals are recalculated once a day at 1:00 a.m. You can also recalculate the totals at any time by choosing **Tools > Recalculate Disk Usage**.

To configure space for the user's voice messages, see "The Voice Mail tab" on page 11-18. To configure space for the user's greetings and voice titles, see "The Audio tab" on page 11-36.

The Security tab

Choose **File > New > User**, then click **Security** in the tree pane. Use the Security tab to configure the user's password settings and whether the user's calls can be supervised.



Configuring password expiration

Use the options on the Security tab to protect the user's account and your Wave system from unauthorized access and toll fraud. For more information about toll fraud, see Appendix A.

The following security options are available:

- **Password never expires.** If checked, the user's password does not expire, although you can always manually change it or force the user to change it. If unchecked, the user's password may expire as determined by your system settings.

  Note: Checking this field is a security risk, as long-standing passwords are easier to guess.

  Note: You should check this field for users of IP phones that use PLAR, because a changed password prevents the phone from working.

- **User must change password on next logon.** If checked, the system requires the user to change his or her password the next time he or she logs on to any workstation application or by using the telephone commands.
- **User is locked out.** If checked, the account cannot log on to the system, even with the correct username and password. Depending on your system settings, lockout can occur automatically if someone repeatedly tried and failed to log on to the account. Uncheck the field to unlock the account and permit normal logging on.

Configuring whether the user's calls can be supervised

You can choose whether the user's personal calls can be supervised by other users with permission to do so. These settings do not apply to call center queue calls or ACD workgroup calls. Supervision of call center queue calls is controlled separately by agent permissions.

In each of the following fields choose "Yes," "No," or "System Default":

- **Personal calls can be monitored.** Any user with the "Allow monitoring user calls" permission can listen to this user's personal (not queue) calls without this user knowing.
- **Personal calls can be coached.** Any user with the "Allow coaching user calls" permission can add himself or herself to this user's personal (not queue) call and be heard by this user, but not by the caller.
- **Personal calls can be joined.** Any user with the "Allow joining user calls" permission can add himself or herself to this user's personal (not queue) call as a full participant.

Note: To coach a call between two users, the user being coached must allow coaching *and* the other user must allow monitoring. This is because coaching the first user automatically involves hearing (monitoring) the other user. If your supervisors will be coaching calls between users, you should set up users to allow monitoring as well as coaching.

The Security \ Permissions tab

The Security \ Permissions tab lets you define permissions and roles for the user.

For an explanation of all the user permissions, see "Wave permissions" on page 11-49.

Before assigning permissions

Before assigning permissions and roles to users, set up the roles the way you want (see “Managing roles” on page 11-45). A role is a template enabling you to apply the same group or collection of permissions to multiple users, so by setting up roles in advance, you can save time in giving each user the permissions he or she needs.

Assigning a user’s permissions

A user’s permissions determine which Wave views and features he or she can use. To assign permissions, do the following:

1 Assign the user to a role if necessary. A role is a collection of permissions. By default, new users belong to the Users role. To assign the user to a new or different role, click **Change**. See the next section for instructions.

Note: A quicker way to assign batches of users to a role is to edit the role. See “Assigning users to a role” on page 11-46.

You can assign a user to more than one role. If the roles’ permissions conflict, the most permissive setting is used. For example, users who belong to both the Users role and the Administrators role have their permission for **Place external calls when logged on via a trunk** set to Allow, which is the permission level for the Administrators role.

2 If you want to give the user unique permissions, different from those of the roles to which he or she belongs, edit the user’s permissions using the **Permissions** pane. The user’s **Permissions** pane settings override all role settings.

To adjust an individual permission for a user, click the **Value** column for that permission in the **Permissions** pane. Select one of the following from the dropdown list:

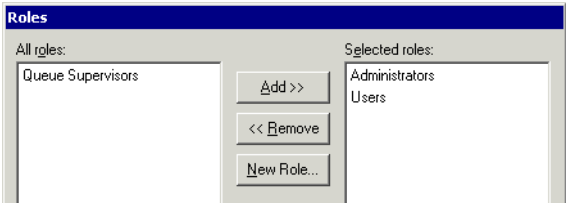
- **Use roles (value).** Permission for this item is determined by the user’s role memberships (described in the following section). The actual value of the permission is displayed in parentheses.
- **Allow.** The listed feature (for example, exporting Contacts) is available to the user.
- **Disallow.** The function is not available to the user.
- **View and Edit.** The specified tab or folder (such as the Phone settings tab or the Call Log folder) can be viewed and edited by the user.
- **View only.** The user can view the folder or tab, but cannot change it.

- **No access.** The folder or tab cannot be used or viewed by the user.

Changing the user's roles

- To change the roles to which the user is assigned, do the following:

1 Click **Change** on the Permissions tab. The Roles dialog box opens.



2 Use **Add** and **Remove** to place the roles to which the user should belong in the **Selected roles** list.

To create a new role, click **New Role**. See "Creating a new role" on page 11-46 for instructions.

3 Click **OK**.

Note: If the user belongs to no roles, by default the user's permissions are all set to deny access.

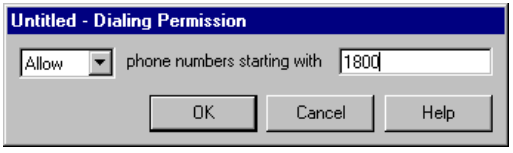
The Security \ Dialing Permissions tab

The Security \ Dialing Permissions tab lets you control which numbers the user is permitted to dial.

Note: It is recommended that you set dialing permissions at the Role or dialing service level, and set permission at the user level only for special exceptions. In cases of conflict, the more individual setting applies. See "Dialing permissions hierarchy" on page 11-58 for more information.

To set dialing permissions:

1. Use the **Default permission** list to specify how to set the user's dialing permissions. Choose one of the following options:
   - **Use Role permissions.** Applies the dialing permissions set up for the role to which the user belongs. This is the easiest way to set up dialing permissions for users. See "Managing roles" on page 11-45 for more information.
   - **Use Role permissions except the following.** Applies the dialing permissions set up for the role, except for the numbers allowed or disallowed in the **Exception permissions** list. The listed settings override the role's settings.
   - **Allow all numbers except the following (ignore Role permissions).** Allows the user to dial all numbers except those disallowed in the list.
   - **Disallow all numbers except the following (ignore Role permissions).** Prevents the user from dialing any numbers except those allowed in the list.
2. Under **Exception permissions**, click **Add** to add a new exception permission to the list. Click **Edit** to modify an existing exception permission. The Dialing Permission dialog box opens.



3. In the Dialing Permission dialog box, choose to **Allow** or **Disallow** calls, and then enter the digits. Enter a phone number or the initial digits of a phone number. Be sure to include 1 before the number if it is normally be dialed as part of the number, for example, 1800.
4. Click **OK**. The exception permission appears in the **Exception permissions** list and is applied whenever the user dials a number beginning with the digits.

The Dial-by-name Directory tab

Use the Dial-by-name Directory tab to specify whether the user can looked up by name by callers who don't know his or her extension.

To include a user's name in the dial-by-name directory that callers can search, check **List in dial-by-name directory**, and make sure that the user has a voice title recorded.

To play a user's extension along with the user's name when callers choose the user from the dial-by-name directory, check **Play extension to the caller**.

The ViewPoint tab

This tab contains the following fields:

- **Use Navigation Pane**. If checked, the user's ViewPoint application displays the Navigation pane on the left side. If unchecked, ViewPoint displays the view bar instead.
- **Show Welcome Wizard.** If checked, the ViewPoint Welcome Wizard starts when the user starts ViewPoint, offering a step-by-step guide to recording his or her voice mail greeting and voice title and entering personal phone numbers. It also leads him or her to the Wave Quick Tour and online Help for more information.
- **Show Tip of the Day.** If checked, the Tip of the Day window opens whenever the user starts ViewPoint, showing different tips on using Wave.

Enabling automatic logon for users

You can configure a user's Home, Home2, or Mobile number to be 'authenticated' whenever the user calls Wave from that number. This way users can call Wave from their remote numbers and be connected immediately to their account menu, where they can check voice mail and perform other account operations. They are not prompted for extension or password. To authenticate one or more of a user's numbers, edit the user's "My Numbers" in the Administrator and check **Use to Authenticate** (see "The User \ Numbers tab" on page 11-16 for instructions). You can then set up automatic logon in either of the following ways:

- **Per user.** If you enable automatic logon at the user level, every call Wave receives from the user's authenticated numbers is automatically authenticated, regardless of whether the auto attendant has automatic logon enabled. To use this method, check **Authenticate trunk calls via Caller ID** on the User \ Numbers tab of the User dialog box (see "The User \ Numbers tab" on page 11-16).
- **Per auto attendant.** If you enable automatic logon at the auto attendant level, every call that auto attendant receives from the user's authenticated numbers is automatically authenticated, regardless of whether user has automatic logon enabled. At other auto attendants, the user cannot automatically log on unless they have the per-user setting checked. To use this method, check **Authenticate trunk calls via Caller ID** for the auto attendant (see "Creating a new auto attendant" on page 13-3).

Adding a user at the telephone

You can add a new user at an unassigned Wave station by picking up the phone and pressing ****0**. You are prompted to enter an extension and password for the user, and the phone's station ID is automatically assigned to the user. You can also record the user's voice title and change user preferences. The user is automatically assigned user settings from the default user template and phone settings from the default phone template for his or her phone type.

New users created at the telephone are given a first name of "New" and a last name of "User X," where X is the user's extension. For example, a user created at the telephone with extension 117 is named "New User 117." To change the name, use the Administrator.

When creating a batch of users, you can use the ****0** command as a time-saving way to assign stations to users, without knowing the station ID of each Wave phone. Do the following:

1. Create your users in the Administrator, assigning their names and extensions and other details but giving each user a station ID of 0.
2. Go to each phone that will belong to a new user. At each phone, press ****0**. When prompted for an extension, enter the appropriate user's extension. The phone's station ID is assigned to the user. If the extension you enter doesn't exist, Wave creates a new user.

For example, use the Administrator to create a user named Amy Smith, with an extension of 117 and station ID 0. Then go to Amy Smith's phone, press ****0**, and enter 117 when prompted for an extension. That phone's station ID is assigned to Amy Smith.

Modifying a user's ViewPoint settings

There are times when you may need to troubleshoot aspects of a user's account that can only be accessed using ViewPoint. For example, with ViewPoint you can modify the user's voicemail greetings.

Wave lets you modify a user's ViewPoint-based settings directly from the Administrator, without your having to know the user's password. Private aspects such as the user's voice messages are not accessible.

You must have ViewPoint installed to use this feature.

To modify a user's ViewPoint-based settings from the Administrator:

1 In the Users view, select the user whose ViewPoint settings you want to edit.

2 Choose **Users > Edit All ViewPoint Settings**.

A limited version of ViewPoint opens with the selected user logged in. You can access all ViewPoint-based features except for the following:

- The user's voicemail
- The user's Call Monitor

To change those features—for example, to share the user's calls or voicemail to another user—you must start ViewPoint and log in as that user.

To modify many ViewPoint-based settings, choose **Tools > Options**. For complete instructions on using ViewPoint, see *Vertical Wave User's Guide*.

Managing roles

Roles are templates that enable you to apply the same set of permissions to multiple users. You can create as many different roles as you want, to represent different groups of users who have similar permissions. Roles appear in the Users view in bold.

When a user belongs to a role, he or she inherits the role's permissions. A user can belong to more than one role, in which case the most permissive settings apply in cases of conflict.

You can grant a user individual permission settings that override those of the role, by adjusting his or her permissions individually on the Permissions tab of the User dialog box. See "The Security \ Permissions tab" on page 11-39.

Wave comes with the following two roles:

- **Administrators.** You cannot delete this role, but you can edit some of its settings. By default the role has full permissions. You can disallow only the following permissions:
  - Place external calls when logged on via a trunk
  - Place external calls from a station
  - Forward or route calls to external numbers

- Return calls when logged on via a trunk

The Admin user belongs to the Administrators role by default and cannot be removed.

- **Users.** By default new users belong to this role.

Assigning users to a role

The quickest way to assign a batch of users to a role is to edit the role and add the users. See “Creating a new role” on page 11-46.

You can also assign a user to a role by editing the user. See “The Security tab” on page 11-38.

Editing a role

To edit an existing role, double-click it in the Users view. For further instructions, see the next section.

When editing a role, be aware of the following:

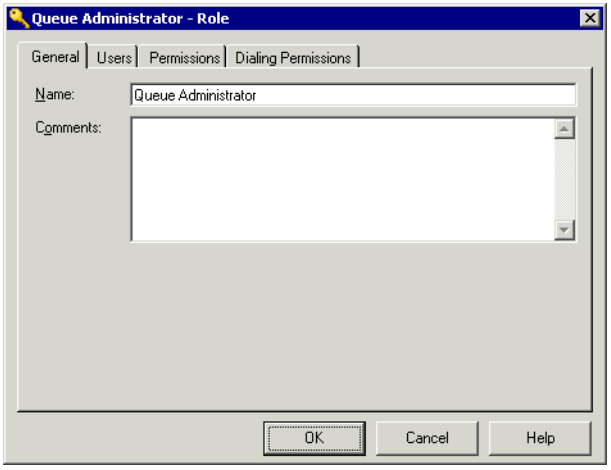
- When you change a role’s permissions, those permissions change for all users belonging to the role, except where a user’s individual permission setting overrides the role, or where a user’s other role provides a more permissive setting.
- When you remove a user from a role, the user loses all permissions granted by that role.
- The Administrators role can only be edited in limited ways.

Creating a new role

You can create a new role, for example Admin Assistant, for a group of users that require the same or similar permissions. All users that you assign to this role are automatically granted its permissions, except where their individual permission settings override roles.

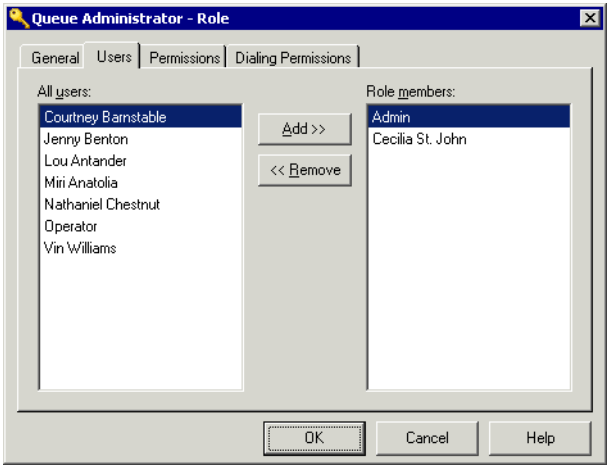
To create a new role:

1 Choose **File > New > Role**. The Role dialog box opens.



2 Enter the name of the role and any comments about its function.

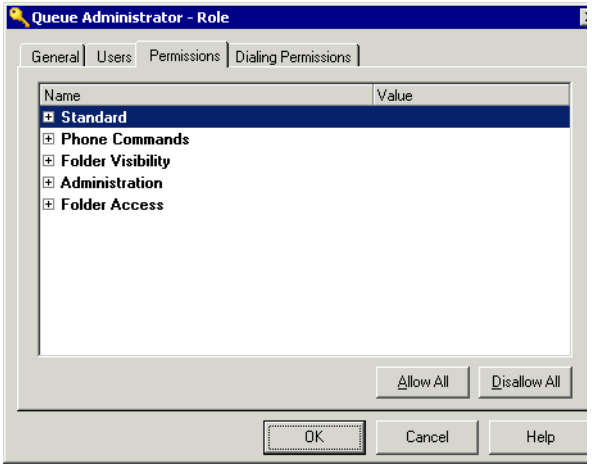
3 Click the Users tab to assign users to the role.



To add users to the role, select them in the **All users** list and click **Add**. To select several users at once, hold down SHIFT or CTRL as you click.

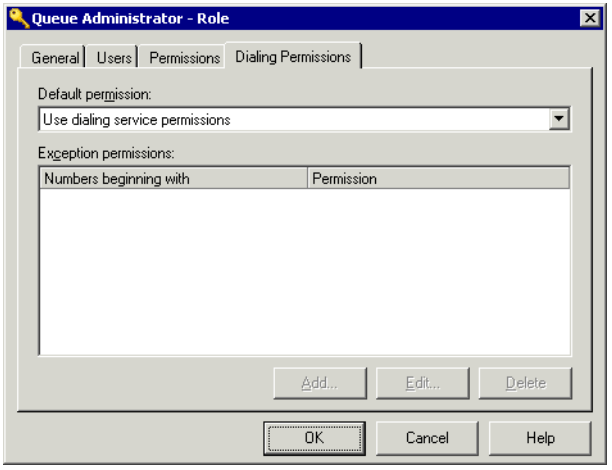
To remove a user from the role, select the user and click **Remove**.

4 Click the Permissions tab to choose the role's permission settings.



To set a permission, click its **Value** column and select the setting you want.

5 Click the Dialing Permissions tab to specify which numbers can be dialed by users belonging to this role. A disallowed number prevents the dialing of any number beginning with those digits.



Note: You can set dialing permissions globally for each Phone Number dialing service, and also individually for each user. In cases of conflict, the more individual setting applies. See "Dialing permissions hierarchy" on page 11-58.

6 Use the Default permission list to specify how to set the role's dialing permissions. Choose one of the following options:

- **Use dialing service permissions.** The role applies no dialing permissions or restrictions to users belonging to it. Users' dialing is controlled by the permissions of the dialing service they use, and any individual exceptions they have.
- **Use dialing service permissions except the following.** The exceptions you enter here override dialing services' permissions for users belonging to this role.
- **Allow all numbers except the following (ignore dialing service permissions).** Users belonging to this role can dial all numbers except what you disallow here, regardless of dialing service permissions. Users are also prohibited from dialing any numbers disallowed at the individual level.
- **Disallow all numbers except the following (ignore Role permissions).** Users belonging to this role cannot dial any numbers except what you allow here, regardless of dialing service permissions. Users are also permitted to dial any numbers allowed at the individual level.

7 Under **Exception permissions**, click **Add** to add exception permissions to the list. For instructions, see page 42.

8 When you are finished defining dialing permissions, click **OK** to close the Role dialog box.

Wave permissions

A user's access to Wave features is controlled by permissions. There are three types of Wave permissions:

- **General user permissions.** These control what ViewPoint views and Wave commands the user can use. See the next section.
- **Dialing permissions.** These control what phone numbers the user can dial. See "Dialing permissions" on page 11-57.
- **Call center agent permissions.** These apply to agents in a call center queue only, and control what queue features the agent can use.

Users inherit general permissions and dialing permissions from the *roles* to which they belong. Roles are collections of permissions that you set up to define jobs or roles in your office. See "Managing roles" on page 11-45. Users can also have individual permissions that override the permissions of the roles to which they belong.

General user permissions

To assign permissions to a role, see “Creating a new role” on page 11-46. To assign individual permissions to a user, see “The Security tab” on page 11-38. You can assign the permissions in the following table:

Wave General User Permissions

Permission	Controls the ability to...
	Standard
Access Tools menu in ViewPoint	Use the Tools menu in ViewPoint, which includes access to call forwarding, personal status, the Call Center Reporter, and more. See *Vertical Wave User’s Guide*.
Access call center reporter	Use the call center reporter to run reports.
Access system call log via API	Use the Wave Client API’s System.GetSystemCallHistory method to get call log data on any call in the system. This applies to API developers only.
Add parties when replying to voicemail	Send voicemail replies to additional users as well as the sender. Applies only to using ViewPoint.
Allow coaching/joining/ monitoring user calls	Monitor, coach, or join other users’ calls. The target user must be set up to permit call supervising (see “Configuring whether the user’s calls can be supervised” on page 11-39).
Place external calls when logged on via a trunk	Dial in to Wave from a remote location and place external calls through the ISM that get billed to the ISM. See also **Forward or route calls to external numbers**.
Place external calls from a station	Place outbound calls on Wave trunks.

Wave General User Permissions

Permission	Controls the ability to...
Change Personal Status	Change the user's own personal status. You might disallow this for agents in a call center queue, to ensure that they take calls during their shifts.
Change the personal status of any user	Change their own or another user's personal status, using the **Apply Personal Status** command in ViewPoint. The user must still enter the other user's password to change his or her personal status.
ViewPoint call control	Use the ViewPoint Call Monitor to handle calls.
Delete Call Log entries	Use the Edit > Delete command in ViewPoint's or the Administrator's Call Log.
Export data	Export contacts, extensions, or the Call Log, using ViewPoint. Does not affect exporting audio files or using export commands in the Administrator.
Forward or route calls to external numbers	Specify an external number when forwarding calls or setting up routing lists.
Forward voicemail	Forward voice messages to one or more users.
Lock/unlock the layout of ViewPoint views	Use ViewPoint's **View > Lock the layout** command to lock the current layout in place and unlock it.
Log on to ViewPoint Web Access	Use ViewPoint Web Access.
Log on to ViewPoint	Use Wave ViewPoint.
Log on via IP trunk	Log on when making an Internet call to Wave .

Wave General User Permissions

Permission	Controls the ability to...
Log on via station	Log on by pressing # at a station.
Log on via trunk	Log on when calling from a remote location, either via the auto attendant or by pressing 9 at a voicemail greeting.
Change password	Change the user's own Wave password.
Off-hook page	Use the *15 telephone command to place pages or intercom calls.
Pick up other ringing call	Use the *91 or *99 commands to answer one ringing station from another.
Play audio into call	Use the Call Monitor's **Play audio into call** command to insert recorded audio into a call.
Record calls	Record calls using the Call Monitor.
Reply to voicemail	Send voice messages as replies to voice messages received.
Report on all call logs	Run the Call Log report on the Call Log of any user or queue. When set to Disallow (the default), the report can be run only on the Call Log of the user logged in to the Reporter. For instructions on running reports.
Return external calls when logged in on a trunk	Use the **43** or **44** commands to call back a voice message from an external number, when calling in from a remote location.
Send voicemail	Record and send new voice messages directly to users' voice mailboxes.

Wave General User Permissions

Permission	Controls the ability to...
Show 'All' tab in ViewPoint Extensions view	See a tab in ViewPoint's Extensions view that shows all extensions in the system. With this tab turned off, the user can still see the filtered tabs, such as tabs for workgroup or call center queue extensions.
Show menu bar in ViewPoint	See ViewPoint's menu bar, from which all commands can be chosen.
View call history	See the History pane in the Device Monitor or the Call Log (Administrator or ViewPoint).
Access...	View and use the specified features in ViewPoint's Options dialog box (Tools > Options). Note: **Access external station settings** also controls the **6 9** telephone command to set a new remote phone as an external station.
Access call forwarding options	Forward calls, using ViewPoint, Administrator, or telephone commands.
Access voice title	Record the user's own voice title, using ViewPoint, Administrator, or telephone commands. Does not affect the ability to record or capture voice titles for contacts.
Phone Commands	
Access saved messages	Press 2 after logging on to access voice messages in the Saved folder.
Call back last incoming call	Dial *69 to return the most recent incoming call.
Dial by name	Dial *93 to use the Wave dial-by-name directory.

Wave General User Permissions

Permission	Controls the ability to...
Disable call waiting	Dial *70 to disable call waiting on the next call.
Enter account code	Dial *11 to enter an account code for the current call.
Manage account settings	Use the 6 command from the voicemail / Account menu to manage account preferences.
Manage calls on hold	Dial *95 to manage calls on hold.
Redial	Dial *66 to redial the last call placed.
Disconnect (remote)	Dial *96 to log off from a remote Wave session.
Send message to all	Option to send a voice message to 8888#, sending it to all users.
Set 'calling as'	Dial *14 to mark subsequent outbound calls as originating from a queue.
Set personal status...	Set that personal status by logging in and pressing 6 1 *x*. The permissions for Available, Available (Queue Only) and Available (Non-Queue) control the ability to dial *50-*52 to set that personal status.
Start a new call via #	Press # for dial tone to dial a new call from either the voicemail / Account menu (after logging on) or the Call Handling menu (after pressing Flash).
Toggle hands-free	Dial *10 to turn hands-free answering on or off.
Toggle voice-first	Dial *12 to turn voice-first answering on or off.

Wave General User Permissions

Permission	Controls the ability to...
Universal pickup	Dial *91 to answer another ringing phone.
Unpark	Dial *92 to retrieve a parked call.
Workgroup pickup	Dial *99 to answer another ringing phone within a workgroup.
Folder Visibility	
View...	These permissions control whether or not the specified view or folder appears when the user logs into the Wave ViewPoint or ViewPoint Web Access. To make a folder visible but not editable, use the **Folder Access** section.
Administration	
Access...	View and be able to use the specified features in the Administrator.
Edit all ViewPoint settings	Use the **Edit all ViewPoint Settings** button to edit a user's ViewPoint settings from the Administrator.
Export Call Log	Export the Call Log using the Administrator. Does not affect exporting the Call Log using ViewPoint.
Export system prompt text	Export system prompts to a text file using the Administrator.
Select a specific trunk for outbound call	Dial **88** followed by a trunk number and a phone number to place a call on a specific trunk.
Backup and restore the database	Perform database backups and restores.

Wave General User Permissions

Permission	Controls the ability to...
Edit system settings in Wave settings editor	Use the TVSettings.exe application to modify registry settings.
Start and stop the Server	Use the Administrator or Device Monitor commands to start and stop the Wave ISM.
Access...folder	These permissions control the degree of access the user has to the specified Administrator view or folder. The choices are the same as for **Folder Access** below. Note that the permission **Access Queues folder** enables users to sign agents in and out of any queue, including themselves if they are non-observer agents. It overrides the per-queue permission **Queue sign in/out**. The objects shown in the Dial Plan view are edited using the permissions for other folders (Users, Queues, etc.), so the permission **Access Dial Plan folder** has an Allow/Disallow choice.

Folder Access

Wave General User Permissions

Permission	Controls the ability to...
Access...	These permissions control the degree of access the user has to the specified ViewPoint view or folder. The choices are as follows: **No access** - the view or folder does not appear. **View only** - the user can view but not edit or delete the folder's items. **View and Edit** - the user has full access to the view or folder. Note that a **No access** setting prevents the user from accessing the folder even using the Wave API. Disallowing a folder using the **Folder Visibility** permission removes it from ViewPoint, but still permits access via the API.

Dialing permissions

Dialing permissions determine what phone numbers can be dialed by Wave users. By default, all numbers are allowed. You can use dialing permissions to disallow certain numbers, either globally, by role, or on a per-user basis. You can decide whether to permit all numbers except for a few, or disallow all numbers except for a few.

A user who dials a disallowed number hears the message, "I'm sorry, you do not have permission to dial that number." A user cannot include a disallowed number in a routing list or forward calls to a disallowed number.

A disallowed number means that the user cannot dial any number beginning with those digits. Commonly disallowed numbers include the following:

Prefix	Disallows
1	Long-distance calls. Be aware that in some areas this may block local calls as well.
011	International calls.
1550	Group conversation lines.
1554	Adult information services.
1900	Long-distance programs.
1976	General information programs.

Dialing permissions hierarchy

You can set dialing permissions separately for the following:

- **Phone Number dialing services.** Use this setting to create global dialing restrictions that affect everyone using the dialing service.
- **Roles.** Use this setting to apply the same dialing restrictions to a group of users. See “Managing roles” on page 11-45.
- **Users.** Use this setting to give individual users exceptions to the more general dialing permissions. See “The Security \ Dialing Permissions tab” on page 11-41.

In cases where dialing permissions conflict, the more individual setting applies. User settings override role settings, and role settings in turn override dialing service settings. For example, if a dialing service disallows 011 numbers, and a role allows them, users belonging to the role can dial them. However, if a user has 011 numbers disallowed at the individual level, that user cannot dial them.

Managing Workgroups

CHAPTER CONTENTS

About Workgroups

A workgroup is a group of related extensions or contacts. With Wave workgroups you can do the following:

- Place or pick up calls to a group of users. You can direct calls to a workgroup so that all phones (including external stations) in the workgroup ring simultaneously, and the first to answer receives the call. Users in a workgroup can also use the ***99** telephone command to answer any ringing phone in their workgroup.

  Note: For a different method to call a group of users, use station hunt groups. See "Creating a Station hunt group" on page 10-24.

  workgroups using methods other than simultaneous ring, create a user with a routing list that calls the members of the workgroup using top down, round robin, or other methods.

- Organize groups of extensions for display in ViewPoint's Extensions view, making it easier for users to locate an extension for calling or transferring calls.

See *Vertical Wave User's Guide* for instructions on placing calls, routing calls to workgroups, and using the Extensions view.

Public and personal workgroups

Wave provides two types of workgroups: public and personal.

Public workgroups are visible to all Wave users. Only public workgroups can have extensions, so they can be dialed from any phone. Administrators and users with the appropriate permissions can create public workgroups. Public workgroups are managed in the User / Workgroup Management applet.

Personal workgroups created by users to easily locate a group of related extensions in ViewPoint's Extensions list. A personal workgroup is visible only to the user who created it and cannot have an extension. Personal workgroups do not have extensions. Personal workgroups are managed in ViewPoint (see *Vertical Wave User's Guide*).

Benefits of using workgroups

Wave workgroups offer the following benefits:

- The process of finding an individual to take calls or to join a conference call is easier, because the Extensions view in ViewPoint can be filtered by workgroup.
- Auto attendants, queues, contacts, or IVR Plug-ins can be added to a workgroup (for informational purposes) and viewed in the Extensions view.
- Calls to a workgroup simultaneously ring the phones (including external stations) of all the users who are members of that workgroup. IVR Plug-ins, auto attendants, queues, and contacts who are members of that workgroup are not called. Public workgroups can be called by their extension numbers or via ViewPoint. Private workgroups can only be called via ViewPoint.
- When workgroup members set their personal statuses to Do Not Disturb (see *Vertical Wave User's Guide*) their phones do not ring when the workgroup is called.

  Note: The Wave Advanced Setting **Server\UseGroupMemberDNDSetting** governs workgroup call behavior to shared stations: whether one user's Do Not Disturb setting prevents workgroup calls to that user only, or the station as a whole. For more information, see Appendix J of *Vertical Wave Installation Guide*.

- When workgroup members forward their calls internally (see *Vertical Wave User's Guide*), calls to the workgroup ring at the number to which calls are being forwarded.

The Workgroups view

Use the Workgroups view in the Wave Global Administratror to add, edit, and delete public workgroups. To open it, do the following:

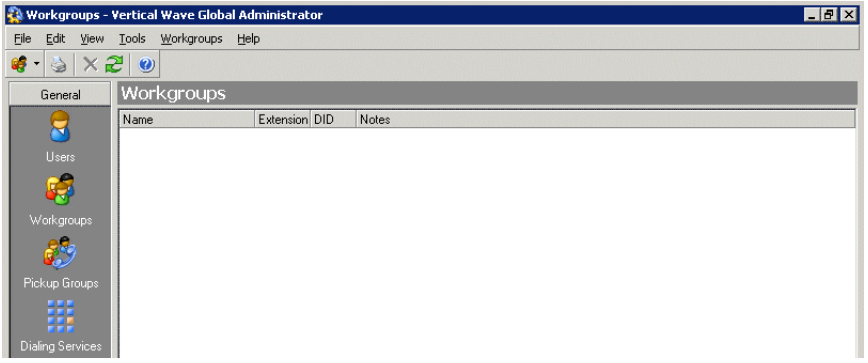
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the **User/Workgroup Management** icon, located in the PBX Administration section of the Management Console.

3 Log on to the User / Workgroup Management applet, which opens in a remote access window. For information on navigating in the User / Workgroup Management applet, see "Using the User / Workgroup Management applet" on page 2-9.

4 Click **Workgroups** in the view bar to open the Workgroups view:

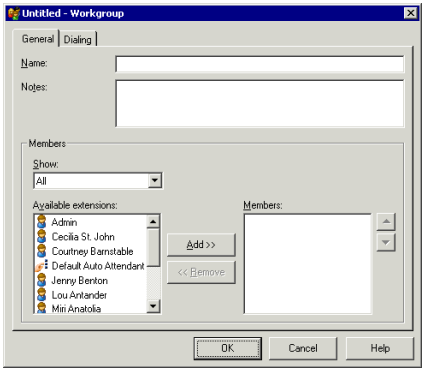


Creating a Workgroup

To create a public workgroup, choose **File > New > Workgroup** and enter information on the tabs in the Workgroup dialog box, as follows:

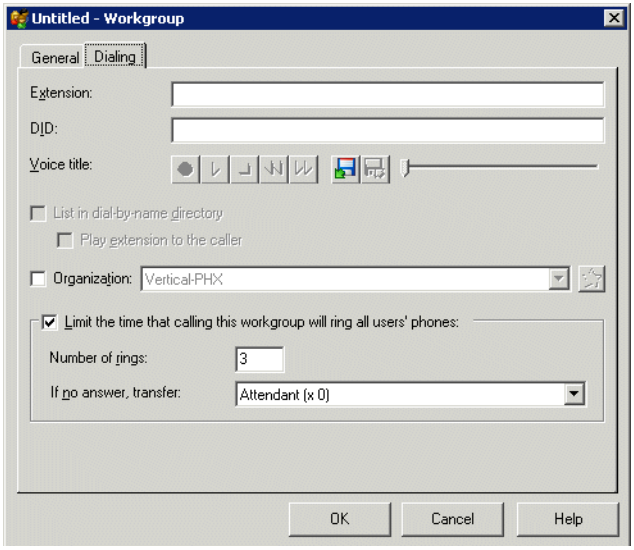
1 On the General tab, enter the **Name** of the workgroup and at least one member. You can optionally add a note about the workgroup in the **Notes** field.

2 To add members to the workgroup, select names from the list of **Available extensions** and click **Add**. To select multiple names, hold down CTRL while clicking.



3 Use the arrows next to the **Members** list to arrange the order of the members. The order in which the names appear can be used in conjunction with a user who has a routing list that calls the members of this workgroup in a “top down” or “round robin” sequence (for more information about routing lists, see *Vertical Wave User’s Guide*). You can also use the **Remove** button to delete members from the list

4 To give the workgroup a number so that it can be dialed using the telephone, click the Dialing tab. All of the information on the Dialing tab is optional. Use the following sections to configure dialing for this workgroup.



Calling, paging, or picking up calls from workgroups

Assign an **Extension** number that callers can dial to reach the workgroup. For more information about extension requirements and restrictions, see “Assigning an extension” on page 11-11.

When no extension number is entered, the workgroup can be called using ViewPoint, but not from the auto attendant or telephone, and users cannot use the paging option (*15).

Assigning a DID number to a workgroup

You can assign a **DID number** to a workgroup from the block of numbers provided by your telephone company. When Wave recognizes this number as the final digits on an inbound call, the caller is automatically connected to this workgroup, bypassing the main auto attendant.

To assign multiple DID numbers to a workgroup, separate each number by a comma (,).

Recording a voice title for a workgroup

You can give the workgroup a voice title, which is played to callers whenever they select the workgroup from the dial-by-name directory. The voice title should be recording of just the workgroup's name, for example, "Sales Department." See "Using the audio controls" on page 2-15.

Listing the workgroup in the dial-by-name directory

If you have recorded a voice title, check **List in dial-by-name directory** to list the workgroup in your company's dial-by-name directory and play the workgroup's extension when the extension number is dialed after the time limit has expired for the phone to ring.

When no one answers a call to a workgroup

Calls to the workgroup's extension ring the phones of all users in the workgroup. As an option, you can set a time limit for how long such calls can ring unanswered. If the time limit is exceeded, Wave transfers the call to an extension of your choice. If you do not choose this option, calls to the workgroup continue to ring all users' phones until the call is answered or the caller gives up.

To set a time limit for ringing on calls to the workgroup:

1. Check **Limit the time that calling this workgroup will ring all users' phones.**
2. In **Number of rings**, enter how many times calls can ring unanswered before being transferred.

   Note: In **If no answer, transfer**, select the extension to which Wave transfers unanswered calls.

   Note: The extension you specify is also the workgroup's personal Operator. If the workgroup is used for dial restrictions in an auto attendant, callers who dial 0 at the auto attendant are transferred to the **If no answer, transfer** extension.

Configuring Auto Attendants

CHAPTER CONTENTS

This chapter provides step-by-step procedures for configuring an auto attendant.

About Auto Attendants

Configure an auto attendant if you plan to have the inbound calls on your company's main telephone number answered automatically. The auto attendant usually consists of a recorded greeting followed by a menu of choices. For example, your main auto attendant might say: "Welcome to Barchetta Industries. You may dial an extension at any time. For Sales, press 1. For Customer Support, press 2. To hear a recorded message about our special offers, press 3. To speak to the Operator, please hold."

What callers can do at an auto attendant

You can set up an auto attendant to let callers do any of the following:

- Dial an extension
- Dial a user by name in the dial-by-name directory
- Log in using a Wave extension and password
- Hear a recorded message
- Transfer to a user, queue, workgroup, or IVR Plug-in
- Transfer directly to a voice mailbox to leave a message
- Transfer to another menu (another auto attendant)
- You can also specify an automatic action to take if callers do nothing.

The Default Auto Attendant

When Wave is installed, you must assign all trunk groups associated with trunks to the default auto attendant at extension 560. Whenever you add a trunk group, you must also assign it to an auto attendant. You can change assignments at any time

The Default Auto Attendant plays a greeting and offers the caller the following options:

- Dial any Wave extension.
- Press 9 to access a dial-by-name directory.
- Press 0 to transfer to the Operator.
- Press # to log in to Wave.

If three seconds pass after the greeting has played without the caller pressing a key, the call is transferred to the Operator.

Configuring an auto attendant

Configuring an auto attendant consists of the following procedures:

- “Creating a new auto attendant” on page 13-3
- “Defining menu choices” on page 13-4
- “Scheduling transfers and greetings” on page 13-11

- "Setting up an auto attendant's hold music" on page 13-14
- Configure the Trunk Group to define the Auto Attendant destination

Creating a new auto attendant

To create an auto attendant:

1 If necessary, click the Administration tab of the Management Console.

Click

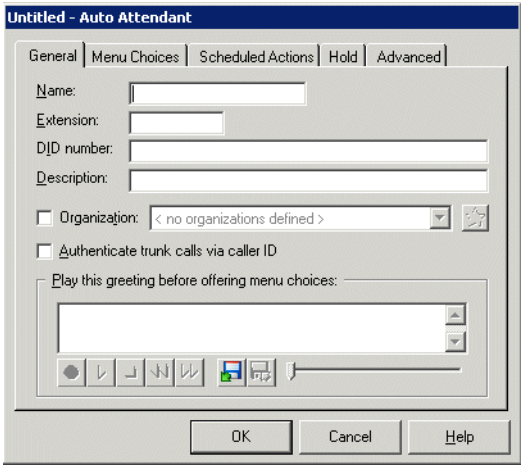
2 Click the **User/Workgroup Management** icon, located in the PBX Administration section of the Management Console.

3 Log on to the User / Workgroup Management applet, which opens in a remote access window. For information on navigating in the User / Workgroup Management applet, see "Using the User / Workgroup Management applet" on page 2-9.

4 Click the **Auto Attendants** icon in the view bar. The Auto Attendants view opens, showing all auto attendants that have been created so far.

The Default auto attendant is automatically provided.

5 Choose **File > New > Auto Attendant**. The Auto Attendant dialog box opens.



6 Enter the following information:

- **Name** (required). Descriptive name for the new auto attendant, for example, "Sales auto attendant."

- **Extension** (required). Extension used to reach the auto attendant from an internal phone.

  To test the auto attendant, dial the auto attendant's extension. The default auto attendant is assigned an extension of 560.
- **DID number.** This field is read-only.
- **Description.** Information that describes the auto attendant.
- **Organization.** Check this field and select an Organization to have calls to this auto attendant logged with that Organization. Calls must end at the auto attendant to be logged with the selected Organization. If the call proceeds to a user, it will be logged with the user's Organization. For information about Organizations, see "Using Organizations" on page 21-2.
- **Authenticate trunk calls via Caller ID.** Check this field to enable automatic logon for the auto attendant. Whenever a user calls it from a number with **Use to authenticate** checked (see "The User \ Numbers tab" on page 11-16), the user is automatically authenticated and can access his or her account without being prompted for a password. See "Enabling the user for automatic login" on page 11-17.

7 To attach a greeting to the auto attendant, that plays when callers first reach it, you must record the greeting and save it as a .wav file elsewhere. Then click the **Import Audio** icon in the audio controls to import it. A typical greeting is, "Thank you for calling Barchetta Industries. If you know your party's extension, you can enter it at any time."

8 Click **OK** or proceed to the next section.

Defining menu choices

An auto attendant can present a series of menu choices to callers. For example, callers might press 1 to transfer to the Sales department, 2 to transfer to the Customer Service department, etc. When a caller reaches an auto attendant, its greeting plays, followed by its menu choice prompts in the order you specify.

Caution: *If your auto attendant supports extension dialing, make sure that its menu choices do not conflict with extension numbers. For example, if you assign the 2 key to a menu choice, make sure there are no extensions beginning with 2. Otherwise callers trying to dial the extension will select the menu choice instead. See "Assigning an extension" on page 6-12.*

Each menu choice can contain the following:

- **Prompt.** A recorded message that explains the option to the caller. For example, “For Sales, press 1.”
- **Key.** The telephone key callers must press to select the option.
- **Action.** The action the system takes when the key is pressed.
- **Language.** The language for subsequent system prompts. When callers enter the key associated with this menu choice, all subsequent prompts are in the specified language. Your system supports the languages that were installed with the Wave ISM.
- **Custom data.** Extra information attached to the call. Whenever a caller selects the menu choice, you can attach a custom data variable or agent skill with the value(s) you define. That value can be seen by users or used to automate call handling.

Menu choice actions

The following table lists the actions that you can choose.

Table 13-1

Action	Description
Transfer to user	Transfers the call to a user.
Send to voicemail	Transfers the call to a user’s voice mailbox.
Play message	Plays a message that you record.
User login	Lets callers log into the system.
Dial by name	Offers callers the dial-by-name directory.
Jump to auto attendant	Transfers the call to another auto attendant (see the Note following this table).
Transfer to IVR Plug-in	Transfers the call to an IVR Plug-in for processing.

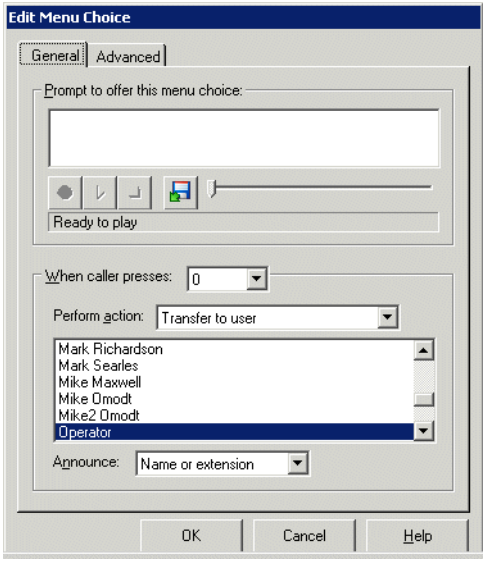
Table 13-1

Action	Description
Transfer to Queue	Transfers the call to a contact center queue.
Transfer to workgroup	Transfers the call to a workgroup. The workgroup phones ring simultaneously, and the first workgroup member to answer the call is connected to it.
Transfer to Hunt Group	Transfers the call to a hunt group. See “Configuring hunt groups of extensions” on page 10-20.

Note: The system automatically disconnects calls if callers do not press a key during three consecutive jumps between auto attendants (for example, if you set up an auto attendant to jump to itself for the “nothing” menu choice action). Callers are presumed to have hung up.

Adding a menu choice

1 On the Menu Choices tab of the Auto Attendant dialog box, click **Add** to create a new menu choice. Click **Edit** to modify the selected menu choice. The Edit Menu Choice dialog box opens.



2 On the General tab, type the text of the Prompt to offer this menu choice, for example, “For Sales, press 1.” Use the audio controls to import the .wav file containing the prompt.

3 In **When caller presses**, select the key that callers must press to select the menu choice. Valid keys are 0-9, *, or #.

4 In the **Perform action** dropdown list, select the action to perform when callers press the key.

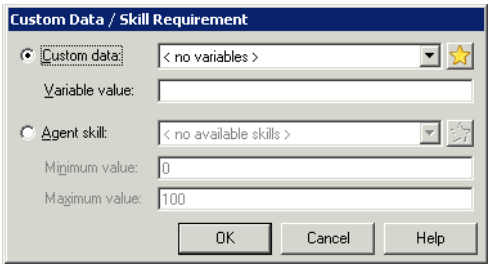
For transfers to a user, IVR Plug-in, or queue, select an optional Announce prompt, that determines what callers hear when they select this menu choice:

- **Nothing.** The call is transferred with no announcement.
- **Name or extension.** Announces the name of the user, IVR Plug-in, or queue, using the voice title if available. If no voice title is available, the auto attendant announces the extension to which the call is transferring.
- **One moment please.** Announces “One moment please” as the call is transferred.

5 Click the Advanced tab.

6 To change the language of subsequent prompts, check **Change the caller's telephone prompts to**. Then select another language from the dropdown list. When callers press the key for this menu choice, all subsequent prompts are in the language you specify here.

7 To set the value for one or more custom data variables or call center queue skill requirements whenever this menu choice is selected, click **Add**. The Custom Data / Skill Requirement dialog box opens.



8 To set a custom data variable, click **Custom data**, select the variable from the dropdown list, then enter the value to be assigned to the variable when the menu choice is selected.

9 Click **OK** to return to the Edit Menu Choice dialog box.

10 Click **OK** to save the menu choice and return to the Auto Attendant dialog box.

11 On the Menu Choices tab, use the arrows to change the order in which menu choices are presented to callers.

12 Add more menu choices or click **OK** to save the auto attendant.

Setting general menu options

1 In the Auto Attendant dialog box, click the Menu Choices tab.

2 In **Number of seconds before performing 'nothing' menu choice**, enter the number of seconds that the auto attendant will wait without a menu choice being selected, before performing the action associated with the **Nothing** menu choice. The wait begins after the final menu choice prompt finishes playing. You can choose the action for the Nothing menu choice using the following steps.

3 To permit callers to dial extensions from this auto attendant, leave the **Process all other digits as user extensions** field checked.

Note: Auto attendant extensions (for example, 8001) cannot be dialed at an auto attendant.

4 To disable type-ahead for this auto attendant, check **Prevent type-ahead**.

Type-ahead enables users to enter a sequence of commands together. For example, with a series of auto attendants set up as submenus, a caller could press 123 to choose menu choice 1, menu choice 2 from the submenu, and menu choice 3 from the final submenu. The problem with type-ahead is that if a caller enters a non-existent extension (for example, 123), the auto attendant processes the digits as type-ahead commands and sends the user to the appropriate menu or submenu. With type-ahead disabled, callers dialing non-existent extensions are never sent to menu choices. However, callers selecting menu choices must wait until they hear the prompts for each menu before entering commands for that menu.

5 To dedicate this auto attendant to a workgroup, so that only users in the workgroup can be dialed from it, check **Restrict dial-by-name and extension matching to members of**, and select the workgroup.

Customizing login behavior from auto attendants

By default, the **User login** menu choice prompts for extension and password, then sends users to Wave's voicemail / account menu (see Appendix A of *Vertical Wave User's Guide* for details). However, you can customize the user login destination, so that users who successfully log in are sent to any extension.

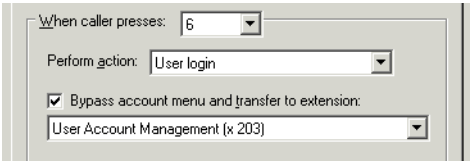
You can use this feature to provide quick access to an extension for verified users, for example, to an IVR Plug-in that gives them custom account information. Instead of having to log in from the auto attendant, press # for an internal dial tone, and dial the extension, the user simply logs in and is connected immediately to the extension.

Notes

- When sending login calls to a custom destination, the standard Wave alert prompts do not play, for example the prompts alerting the user to DND status, active call forwarding, and nearly full voice mailbox. However, the user still is prompted to change his or her password if that is required.
- Customizing user login changes the login behavior through this auto attendant only. Users logging in from a station's dial tone always have the default behavior.

To customize user login:

1. In the Auto Attendant dialog box, click the Menu Choices tab.
2. Click **Add**. The Edit Menu Choice dialog box opens.
3. From the **Perform action** dropdown menu, select **User login**.



4. Check **Bypass account menu and transfer to.**
5. Select the destination extension from the dropdown list.
6. Click **OK**.

Avoiding the auto attendant ambiguous dialing delay

By default, when a caller dials an ambiguous number at an auto attendant, there is a 3-second delay while the system waits to see if the number is complete. For example, if the auto attendant has a menu choice accessed by pressing 2, and an extension 200, a caller pressing 2 will experience the delay while the auto attendant waits to see if more digits are coming.

You can bypass or change the delay in the following ways:

- The caller can press # after dialing the number. This signals that the number is complete, and the caller is connected without delay.
- You can modify your dialing plan to eliminate ambiguous numbers.
- You can turn off extension dialing, if the auto attendant is meant to be used only for menu choices. To do so, uncheck **Process all other digits as user extensions** on the Menu Choices tab. This bypasses any ambiguities between menu choices and extension numbers, enabling menu choices to be dialed without the delay.
- You can modify the length of the delay by changing the Wave Advanced Setting `AutoAttendantInterdigitTimeout`. Be careful when modifying this setting if ambiguous numbers exist, because callers may find themselves connected to the wrong number.

Scheduling transfers and greetings

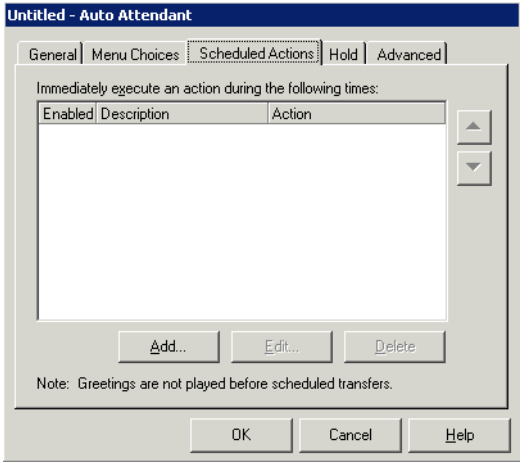
You can customize an auto attendant to automatically change its behavior based on time of day or on special dates. You can schedule the following actions:

- Playing of a different main greeting, which replaces the auto attendant's regular greeting. For example, you can schedule a "We're closed" greeting to be played to all callers after business hours and on weekends.
- A transfer to any other extension, including another auto attendant, user, queue, IVR Plug-in, or workgroup. For example, to provide extended customer support coverage, support calls that arrive after your California office closes in the evening can transfer automatically to the main auto attendant at your facility in New Zealand.

Note: If you have scheduled a greeting and a transfer to occur at the same time, the transfer always takes precedence and the greeting does not play. Also, if you have two greetings or two transfers scheduled for overlapping times, the top-most scheduled item always takes precedence.

To schedule transfers or greetings

1. In the Auto Attendants view, create a new auto attendant or double-click an existing auto attendant to edit it. The Auto Attendant dialog box opens.
2. Click the Scheduled Actions tab.

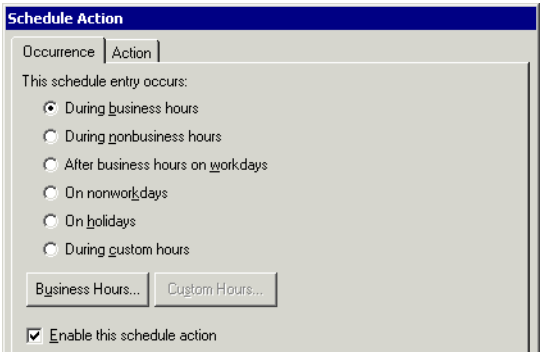


The following table shows the information that appears for each scheduled action already defined for this auto attendant.

Table 13-2

Column	Description
Enabled	If checked, the action will be performed as scheduled. If unchecked, the action is temporarily disabled.
Description	Time period during which the action will be performed.
Action	Action that will be performed.

3 Click **Add** to schedule a new action. Click **Edit** to modify the selected action. The Schedule Action dialog box opens.



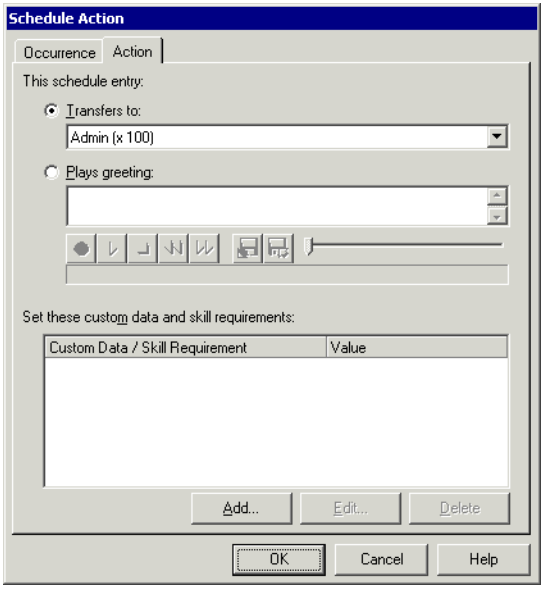
4 On the Occurrence tab, select one of the periods of time during which the action will occur.

Note: If your system uses several sets of business hours, click Business Hours before you click **OK** in the Schedule Action dialog box and verify that the action will take place according to the set of business hours that you want to use.

If you choose During custom hours, click Custom Hours and set your hours in the dialog box that opens.

5 Check **Enable this schedule action** to activate this action as soon as you save the auto attendant. If unchecked, the action is temporarily disabled.

6 Click the Action tab.



7 Under **This schedule entry**, select the action that the auto attendant will perform immediately when a call arrives during the period covered by the schedule entry:

- **Transfers to.** Immediately transfers callers to the extension that you select from the dropdown list during the scheduled time period.
- **Plays greeting.** Immediately plays the greeting that you record during the scheduled time period.

8 Using the **Set these custom data and skill requirements** section, you can have the auto attendant automatically attach custom data variables or apply skill requirements to all calls handled by the schedule rule.

9 Click **OK**. The Schedule Action dialog box closes.

10 On the Scheduled Actions tab in the Auto Attendant dialog box, use the arrows to move a scheduled transfer or greeting to a different position on the list. If you have two greetings or two transfers scheduled for overlapping times, the one that is at the top of the list will be used. If a greeting and a transfer are scheduled for the same time, the greeting is not played.

11 Click **OK** in the Auto Attendant dialog box to save your changes.

Setting up an auto attendant's hold music

Each auto attendant can play its own hold music. Callers hear an auto attendant's hold music while the auto attendant is transferring them to an extension, and they continue to hear it while on hold until they reach a part of the system that uses different hold music, such as a queue or another auto attendant that has different hold settings.

If you do not specify hold music for an auto attendant, the auto attendant uses the system default hold music.

To set up different hold music for an auto attendant

1. In the Auto Attendant dialog box, click the Hold tab.
2. Check **Music on hold** and select the music-on-hold source you want.
3. Click **OK**.

Viewing auto attendants in the Hunt Groups applet

If you create additional auto attendants besides the default auto attendant, they appear in the Hunt Groups list, where you can view or edit them.

To view or edit the Hunt Grop list

1. If necessary, click the Administration tab of the Management Console.

Click

2. Click the Hunt Groups icon, located in the PBX Administration section.
3. Click the Application tab.
4. All auto attendants you have created should appear in the list. You can click **Edit** to configure their hunt group behavior. See "Configuring hunt groups of extensions" on page 10-20.

Configuring the trunk group for the auto attendant extension

After creating auto attendants, or even if you are using only the default auto attendant, you must configure the Trunk Group to correctly route the auto attendant extension.

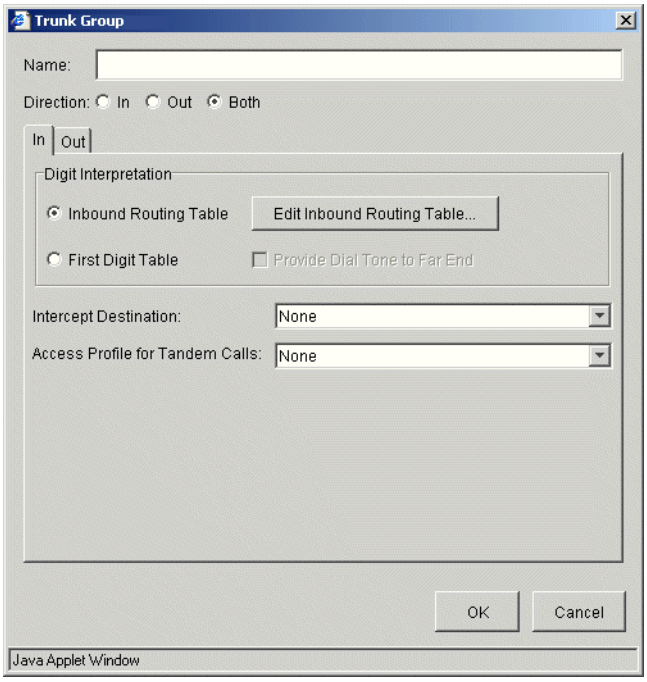
To configure the trunk group for an auto attendant

1 If necessary, click the Administration tab of the Management Console.

Click 

2 Click the Trunk Groups icon, located in the Trunk Administration section. The Trunk Groups dialog box opens.

3 Select **Voice Analog**, and click **Edit**. The Trunk Group dialog box opens with the In tab showing.



4 Choose one of the following methods to route calls to the auto attendant:

- For simple routing, set **Intercept Destination** to the auto attendant.
- For scheduled routing, click **Edit Inbound Routing Table**, click **Add**, and in the **Destination** cell enter the auto attendant's extension. Then use the other fields to set route calls according to the schedule you want.

For more information about the Inbound Routing table, see "Configuring inbound routing tables" on page 8-4.

5 Click **OK** until you return to the Management Console.

Data Networking Configuration

CHAPTER CONTENTS

This chapter provides information about configuring your Wave Integrated Services Manager (ISM) to connect to the Internet, assuming you have already completed the tasks in Chapter 5, Configuring Analog and Digital Trunks.

Ensuring that your T-1 serial interface is set correctly

When you connect an external router to your Wave ISM's T-1 module with a serial interface, you must:

- Assign channels of the T-1 trunk to the serial interface (see "Assigning digital channels to a serial interface" on page 5-22 for details)
- Ensure the serial interface is set correctly

Typically, you will not need to change the interface settings unless you have a non-standard configuration.

To ensure that the serial interface is set correctly:

1. If necessary, click the Administration tab of the Management Console.
2. Click the Trunk Configuration icon, located in the Trunk Administration section.

Click

3. Select the serial interface, labeled Serial I/F, and ensure that the settings are correct for your configuration.

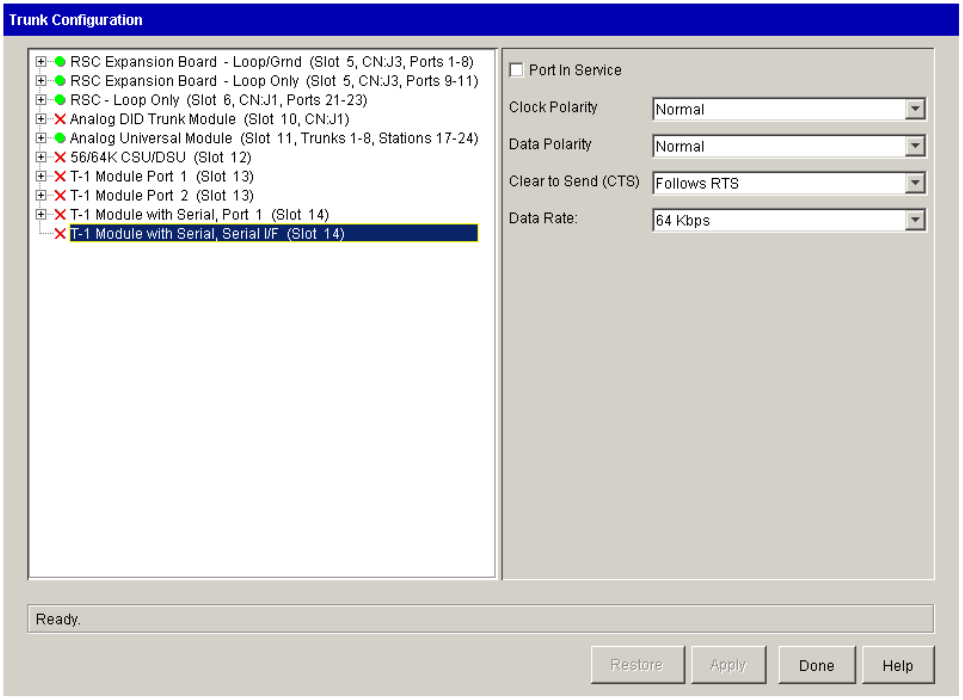


Figure 14-1 Trunk Configuration applet, showing serial interface settings

- Clock Polarity—Normal is the default. You might change this setting if there is a lot of latency between the Wave ISM and the external router, typically due to a long cable (more than 10 feet) between the two devices. The likelihood of this scenario is increased when more channels are used. If you see data errors, you might try inverting the clock.
- Data Polarity—Normal is the default. If you change this setting to Inverted, you must invert the data polarity on both ends of the connection.
- Clear to Send—Follow RTS (Request to Send) is the default. Set this to Always On, if the device at the other end of the connection is not driving RTS.
- Data Rate—64 Kbps is the default. Do not change this setting to 56 Kbps unless you know your connection's maximum data rate is 56 Kbps.

4 Click Apply to save your changes.

5 Click Done to return to the Management Console.

Initial System Administration

CHAPTER CONTENTS

This chapter guides you through the final tasks of initial configuration.

Backing up your system configuration

You should back up your system after completing your initial configuration and every time you make a configuration change. Back up your system whenever you perform a software upgrade or install third-party software. The System Backup / Restore applet backs up the following items.

- Vertical Wave configuration (database file and registry keys)
- RRAS configuration
- Voice Mail Greetings, Names, and Mailboxes directories
- Voice Mail messages and Music On Hold WAV files (optional)
- Call Navigator prompts (optional)

The System Backup / Restore applet does not back up the following items:

- Network Adapters and Settings (including host name / machine name, setting the TCP / IP domain, and IP Address / Subnet Mask / Gateway per adapter. Adapters include: Integrated Services Card, 10 / 100Base-T Ethernet)
- Password Administration settings (Wave account user names and passwords) (be sure to keep a secure record of user names and passwords)

- Date and Time settings
- RAID settings (Windows Disk Management)
- Windows Workgroup or Network Domain settings

Wave automatically backs up the system configuration database file every night at 2:00 AM to help you recover from situations where the database might be corrupted. Every time Wave restarts, the startup procedure checks the database for problems, and it is repaired or replaced with the backup if necessary.

Since the backup and restore procedure uses FTP, the client PC doing the backup must have an FTP program installed.

Note: Depending upon the number and size of your Voice Mail messages, the backup and restore procedure could each take up to 2 hours. For that reason, schedule backups during off-peak hours.

Note: You can only restore from a backup of a system of the same version number as your current system.

To back up Wave:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the System Backup / Restore icon, located in the General Administration section.

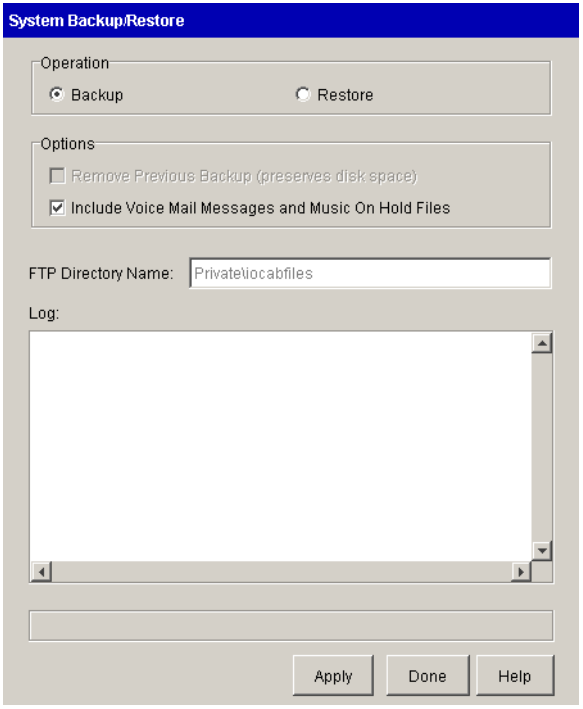


Figure 15-1 System Backup / Restore applet

3 If necessary, select Backup.

Note: Compression takes place only after a temporary full backup of the raw files has been created, so be sure that your Wave ISM's hard drive has enough space (up to 2 GB) to accommodate the temporary backup files.

4 If you wish to remove the previous backup file from Wave ISM hard drive, select Remove Previous Backup. (This option is dimmed if no previous backup is present.)

5 If you wish to back up Voice Mail messages and Music on Hold WAV files, select the Include Voice Mail Messages and Music On Hold Files options.

Recorded names and greetings are included in the standard backup operation and are not affected by this option.

6 If you use the Call Navigator application and wish to back up its prompt files, select the Include Call Navigator Prompts option. (If Call Navigator is not installed on the Wave ISM, this option does not appear.)

7 Click Apply.

Detailed results of the backup operation will appear in the Log field.

The system configuration cabinet (CAB) file is stored in the *C:\Inetpub\Ftproot\Private\Iocabfiles* directory.

Note: It is recommended that you transfer a copy of the CAB file to a different machine via FTP for safe storage.

8 Click Apply again.

9 Click Done to return to the Management Console.

Configuring the Fault Monitor

The Fault Monitor is an embedded processor that provides independent watchdog services for the overall system, collecting system error messages that help you determine why a fault has occurred. The fault monitor module stores a copy of a subset of the system traces that are stored by the system trace manager, specifically those that are flagged as severe or fatal errors.

The Fault Monitor module must be connected to an analog trunk (a dedicated analog trunk if you have a Integrated Services Card [ISC]) in order to use dial-in access and pager notification. For information on connecting the Fault Monitor module to a trunk, refer to the *Vertical Wave Installation Guide*. For a full discussion of using the Fault Monitor once it is configured, refer to the *Vertical Wave IP 2500 Hardware Reference Guide*.

The General Settings applet allows you to configure the Fault Monitor module on the Integrated Services Card to

- set the password for dial-in access for remote assessment of system error messages
- dial a pager on system failure

Note: The Fault Monitor modem on a Integrated Services Card (ISC) answers incoming calls only after 10 rings. If you have a Integrated Services Card (ISC), the modem answers after 5 or 6 rings.

To configure the Fault Monitor:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 Select the Fault Monitor tab.

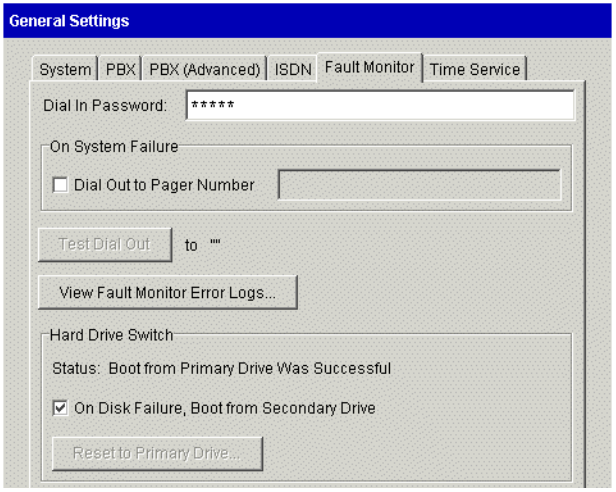


Figure 15-2 General Settings applet, showing the Fault Monitor tab

4 To specify a new password for dialing in for remote Fault Monitor assessment, enter a password between 1 and 16 alphanumeric characters long in the Dial In Password field.

Note: The password is case-sensitive.

Using the new password, you can dial in and view system error messages. See the *Vertical Wave IP 2500 Hardware Reference Guide* for details. If you don't specify a new password, anyone can dial in using the default password, which is admin.

5 If you want Wave to dial a page number in the event of a system failure, follow these steps:

a. Select the Dial Out to Pager Number option.

b. In the adjacent field, type the pager number to be dialed and a code to indicate which system has failed.

   For example, entering

   14085551212,,,12345#

   in the field would dial 1-408-555-1212, and display the code 12345 on the receiving pager. A 9 is not required in the digit string because the Fault Monitor dialer is independent of the Wave PBX.

c. Be sure that the person who will receive such pages knows the meaning of the code you assign.)

d. Click Test Dial Out to test the pager number and code saved in the Dial Out to Pager Number field.

6. Click Apply to save your changes.

7. Click Done to return to the Management Console.

Mirroring your hard drive

As the last step of the initial configuration you should mirror your redundant hard drive using Windows Disk Management. This procedure creates a backup of your Wave configuration that you can fall back on in case of hard drive failure.

Redundant Array of Independent Disks, or RAID, brings another level of fault tolerance to the Wave ISM. RAID is a set of disks (hard drives) that serve collectively as a single, logical storage device, providing data redundancy. The Disk Management application sets up disk mirroring, using one hard drive to mirror another with the same controller, so that an exact copy of the primary hard drive is stored on a secondary, mirrored hard drive.

Whenever you create a mirrored disk, you must use a hard drive of a size equal to or larger than the primary hard drive; the Disk Management application then creates a partition of the correct size automatically. It is best to use a new hard drive, preferably one that is identical to the primary hard drive. For consistency, obtain new hard drives from Vertical Communications.

Depending on the amount of data on the hard drive, it can take up to 30 minutes for Disk Management to mirror the Wave ISM C: drive.

Three scenarios are possible with Wave hard drives:

- A Wave ISM purchased with two hard drives is preconfigured for RAID-1. The second hard drive is mirrored for you.
- If you add a second hard drive after you purchase a Wave ISM, you need to configure RAID-1 on the second hard drive and mirror it. See the instructions that follow.
- If you need to recover a Wave system using a mirrored hard drive, you must break the mirror, power off the Wave ISM, install the mirrored drive in slot A and insert a new drive in slot B, restart, and then mirror the new hard drive. See "Recovering with RAID-1 Configuration" on page 24-30.

To mirror a new, blank hard drive:

1. Shut down the Wave ISM.
2. Insert the new hard drive in slot B.
3. Restart the Wave ISM.
4. Log on to the Management Console.
5. If necessary, click the Administration tab of the Management Console.
6. Click the RAID-1 Configuration icon, located in the General Administration section.

   Click

   For information about logging on using a remote connection, refer to "Remote Access Application applets" on page 2-5.

   The Disk Management application opens.

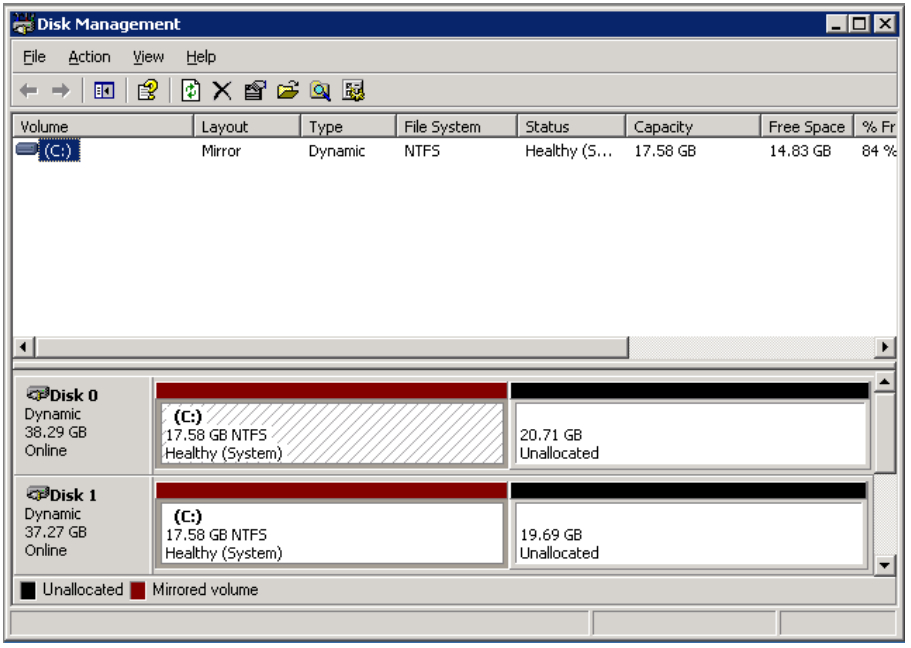


Figure 15-3 Disk Management application

The hard drive labelled Disk 1 should be blank, unformatted, and partitionless. If the hard drive has partitions, delete the partitions before mirroring it. See "Clearing an old hard drive" on page 24-27.

Note: To view SNMP alarms while you are mirroring the hard drive, open another browser window on your workstation, log onto the Management Console, click the Administration tab if necessary, and click the SNMP Alarms icon. The SNMP Alarms applet reports the SNMP traps as they occur.

7 In order to create a mirror of your hard drive, both disks must be dynamic disks. By default all drives are basic. To determine which format your disks are, look for either "Basic" or Dynamic" below the disk number.

8 To convert your disks to dynamic disks, select the disk or disks at the bottom of the screen and select **Action > All Tasks > Convert to Dynamic Disk**.

9 Select the disks you want to convert, then click **OK**.

If you are converting Disk 0, follow the prompts to reboot your system. Once the system has been rebooted, log into the Management Console and re-enter the RAID-1 applet. You should now see that the disks are dynamic disks.

10 Click the C: partition on Disk 0.

11 Select Action > All Tasks > Add Mirror.

If the command is dimmed, your new hard drive is not blank. Follow the instructions in "Clearing an old hard drive" on page 24-27, then return to step 7.

12 Select Disk 1, then click **Add Mirror**.

A new color indicates mirroring (the default color is purple).

Note: If the resulting mirrored partitions are of different sizes, then the primary and mirrored hard drives are physically incompatible. This should not happen if you received your hard drive from Vertical Communications. Contact technical support for assistance. While the mirroring will work, the mirrored hard drive will not boot if the primary hard drive fails; however, it will be recoverable from a separate machine.

The disks will now synchronize. Disk Management indicates initializing mirroring status with the following message:

RESYNCHING (percentage complete)

13 When mirroring is complete, Disk Management indicates healthy status with the following message:

HEALTHY

14 Exit Disk Management to return to the Management Console.

Note: If you remove the mirrored hard drive from the Wave ISM and are running Wave with just the primary hard drive installed, be sure to return to the RAID-1 Configuration applet and break the mirror so that the system does not expect to see two hard drives.

RAID cautions

The following cautions apply to all situations using RAID:

- Do not change the Wave partition size. This will break the mirror and will cause both recovery and mirroring problems in the future.

If the partition sizes are different after mirroring, the mirrored drive will not boot.

It is not necessary to use Microsoft Windows formatting and partitioning features before you use the Disk Management application; the application performs all necessary steps for you.

- Do not attempt to mirror an Wave primary hard drive in Slot A onto an Wave primary hard drive in slot B. Due to the cloning technique used in manufacturing Wave primary drives, the Disk Management application cannot distinguish between primary drives.

  An alternative is to use Disk Management to remove all partitions on the second Wave primary disk so the disk will be treated as a new drive.

- Once you mirror a hard drive, either leave the mirrored hard drive in the slot or take it out and put it somewhere safe until you need it. If you take out the mirrored drive and are running with just one hard drive, break the mirror so that the system does not expect to see two hard drives.

- Do not use the mirrored hard drive as a primary hard drive and then load both hard drives back into the Wave ISM. The system cannot distinguish between the two primary hard drives and cannot restart.

You cannot see any SNMP alarms during RAID-1 configuration unless trap destinations are configured in the SNMP Configuration applet; for instructions, see "Configuring SNMP agents" on page 24-16.

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Restart System icon, located in the General Administration section.

3 In the **Seconds before restart** field, specify how many seconds should elapse before the system restarts.

4 Click Restart to restart the Wave ISM.

5 Click Yes to confirm that you want to restart.

6 Click OK.

7 Close the browser window.

Running Microsoft Systems Management Server

If you run Microsoft Systems Management Server (SMS) on your company network, configure the SMS software to exclude all Wave ISMs from its control list.

Part 2

Advanced Configuration and Administration

Advanced Trunk and Channel Configuration

CHAPTER CONTENTS

This chapter provides information about configuring the advanced trunk and channel features.

Configuring advanced trunk settings

You can modify the advanced trunk settings for your T-1 trunk ports. You can find trunk Advanced Settings in the Trunk Configuration applet.

Caution: *Do not modify these settings unless you are an expert.*

To configure advanced trunk settings for a T-1 module:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Trunk Configuration icon, located in the Trunk Administration section.

3 Select the T-1 module.

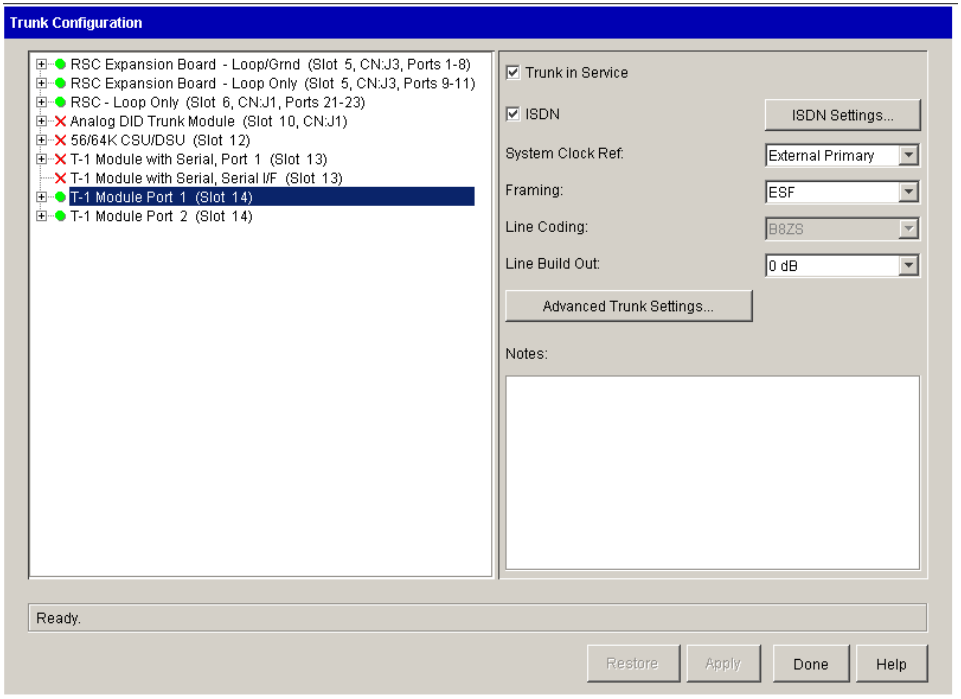


Figure 16-1 Trunk Configuration applet, showing T-1 module settings

4 Click Advanced Trunk Settings.

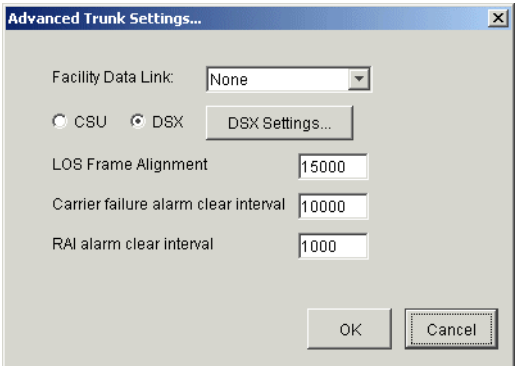


Figure 16-2 T-1 Advanced Trunk Settings dialog

5 **Set the** Facility Data Link **according to your Service Confirmation Letter.**

Two Facility Data Link (FDL) protocols are available. You may also either protocol, both, or none.

- T1.403—Sends Performance Report Messages. The service provider can maintain a continuous history of trunk performance. The service provider can also send test messages to the trunk, if needed.
- TR54016—Sends messages when it is queried by the central office. If the service provider wants to know the status of a particular trunk, it will ask for it, and the Wave ISM will send the information.
- T1.403 & TR54016
- None

This option is provided to allow the T-1 trunk to be tested and maintained by far-end equipment, for example, by the T-1 service provider's equipment.

Your trunk provisioning letter should include this information.

T-1 service providers try to guarantee the up time of the trunks they provide in two ways:

- They keep track of the physical layer errors in both directions, when possible, to proactively identify problems
- They send commands from their end of the T-1 to automatically loop T-1 trunks for error testing

You can view these messages in the trace log by using the Trace Monitor diagnostic applet in the Remote Diagnostics Console.

If you are configuring FDL on a public network, refer to the T-1 service provider's provisioning letter for information about the type of FDL support the service provider supports. If nothing is mentioned, select None.

If you are configuring FDL on a private network, you will typically select None. Since you control both of the T-1 endpoints, you can monitor statistics at each end.

If one trunk endpoint is not a Wave ISM, select either T1.403 or TTR54016 according to what the management equipment supports on the non-Wave endpoint.

6 Choose CSU or DSX.

When connecting to the PSTN, the FCC only allows the CSU setting.

Use DSX mode only if you are connecting a Wave ISM to another Wave ISM using this trunk. In DSX mode, you have full control of all the possible signal strength and shape parameters that can be configured for the T-1 trunk. Use DSX mode only for private networks.

Note: Even though CSU mode was developed for the PSTN, this mode generally works for private T-1 lines. Use DSX mode to set advanced signal strength and shape parameters.

- If you chose DSX mode, click DSX Settings in the Advanced Trunk Settings dialog box.

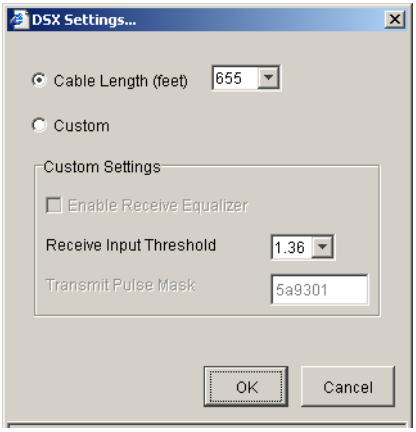


Figure 16-3 DSX Settings dialog

- Cable Length (feet)—Select the length of cable (in feet) to the other Wave ISM.

  Note: Signal power level changes can be significant for short cable lengths, but not as much for longer lengths. Therefore, several short distance choices, and not as many long distant choices have been provided.

- Custom—Specifies custom DSX settings. You should only change these settings if you are working with your service provider to determine the correct settings. Refer to “Customizing transmit and receive signal settings” on page 33-2 for more information on custom settings.

7 Click OK.

8 Modify the device timers settings, if appropriate, by typing new values in the text boxes.

The value ranges and maximum number of digits allowed for these settings are:

- LOS Frame Alignment—Default=15000; Range=1000-30000
- Carrier Failure Alarm Clear Interval—Default=10000; Range=1000-15000
- RAI Alarm Clear Interval—Default=1000; Range=500-10000

9 Click Apply to save your changes.

10 Click Done to return to the Management Console.

Setting trunk timing values

Caution: *Do not modify these settings unless you are an expert.*

Setting digital timer values

Timer values are classified as either inbound or outbound, depending on the direction of the call to which the timer applies. For more information about trunk timing values, see “Trunk timing values” on page 33-4.

To set the timing values for a digital trunk:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Trunk Configuration icon, located in the Trunk Administration section.

3 Display and select the channel(s) you want to configure.

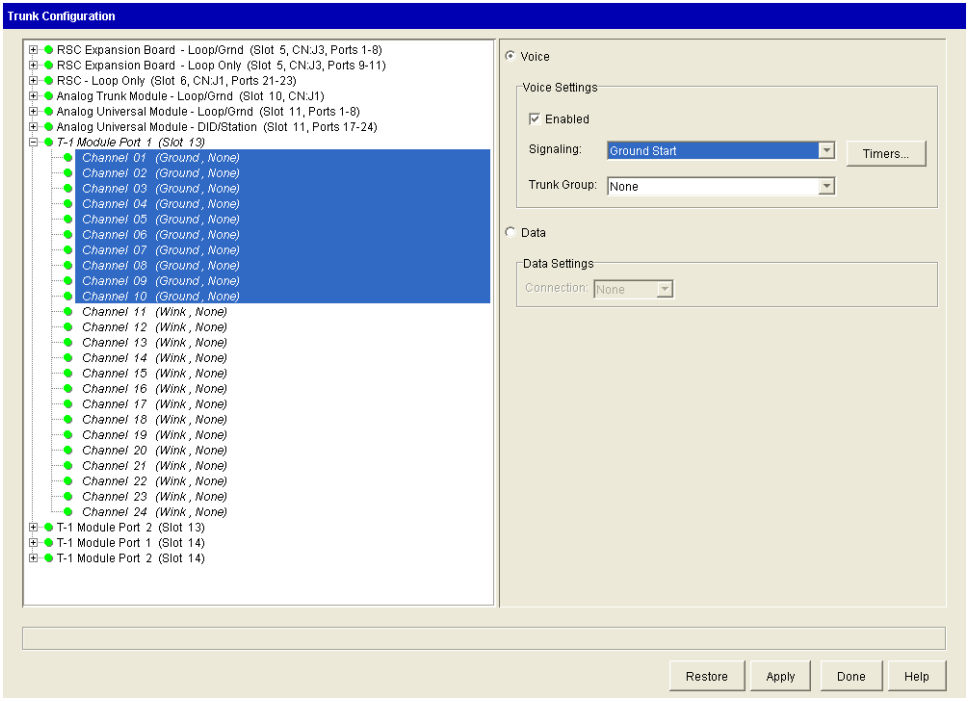


Figure 16-4 Trunk Configuration applet, with channel settings displayed

4 Click Timers.

Depending on the channel settings, you will see one of the following:

- The T-1 E&M Immediate Start Timers dialog box (Figure 16-5)
- The T-1 E&M Wink Start Timers dialog box (Figure 16-6)
- The T-1 Ground Start Timers dialog box(Figure 16-7)
- The ISDN Timers dialog box (Figure 16-8)

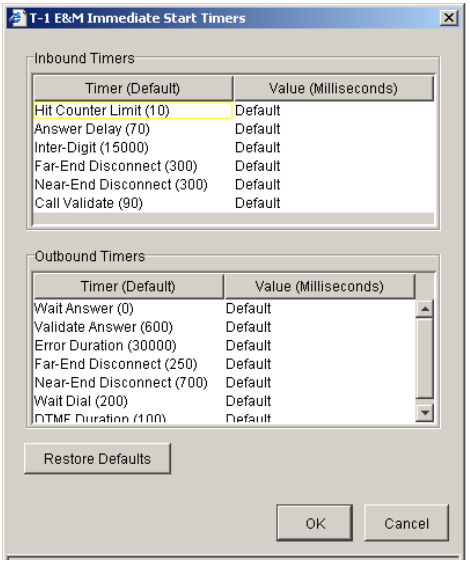


Figure 16-5 T-1 E & M Immediate Start Timers dialog

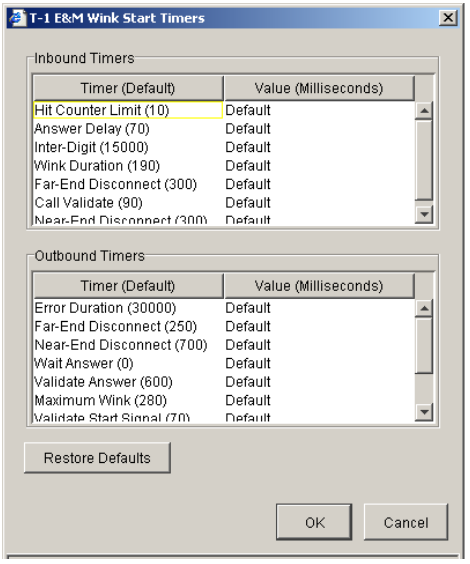


Figure 16-6 T-1 E & M Wink Start Timers dialog

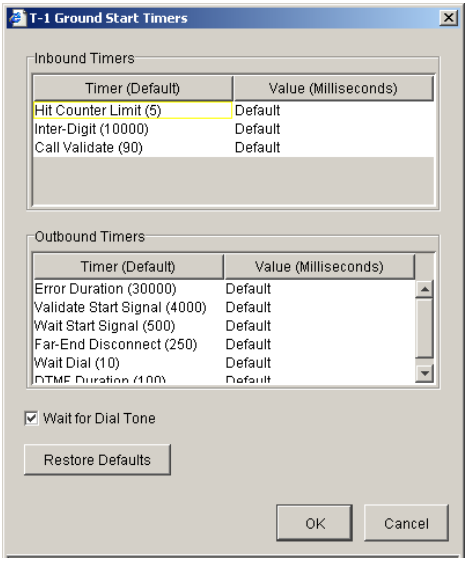


Figure 16-7 T-1 Ground Start Timers dialog

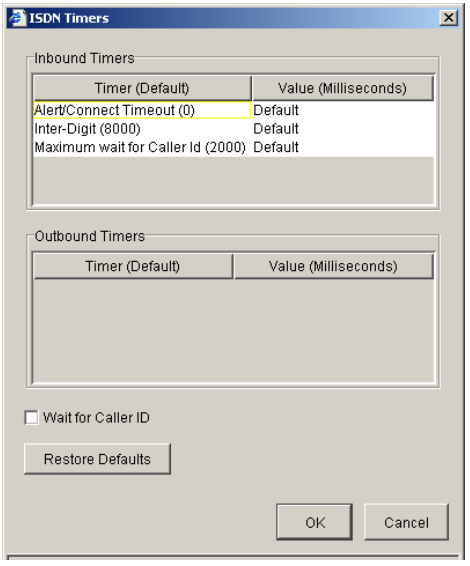


Figure 16-8 ISDN Timers dialog

5 Click the Value field of the timer that you want to edit.

A text box appears where you can type a new value.

For information about specific T-1 trunk timers, refer to the following tables:

- Table 33-2, Inbound T-1 trunk timers (E&M Wink Start and E&M Immediate Start), on page 4
- Table 33-3, Outbound T-1 trunk timers (E&M Wink Start and E&M Immediate Start), on page 5
- Table 33-4, Inbound T-1 trunk timers (ground start), on page 6
- Table 33-5, Outbound T-1 trunk timers (ground start), on page 6
- Table 33-6, Inbound T-1 trunk timers (ISDN PRI), on page 7

6 If the channel or channels you are editing are configured for Ground Start signaling, you can modify the Wait For Dial Tone setting by selecting or deselecting that check box.

This check box tells Wave whether or not to expect dial tone on the channel before dialing.

7 Click Apply to save your changes.

8 Click Done to return to the Management Console.

Setting analog timer values

Timer values are classified as either inbound or outbound, depending on the direction of the call to which the timer applies. For more information about trunk timing values, see “Trunk timing values” on page 33-4.

Caution: *Do not modify these settings unless you are an expert.*

To set the timing values an analog trunks:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Trunk Configuration icon, located in the Trunk Administration section.

3 Display and select the channel(s) you want to configure.

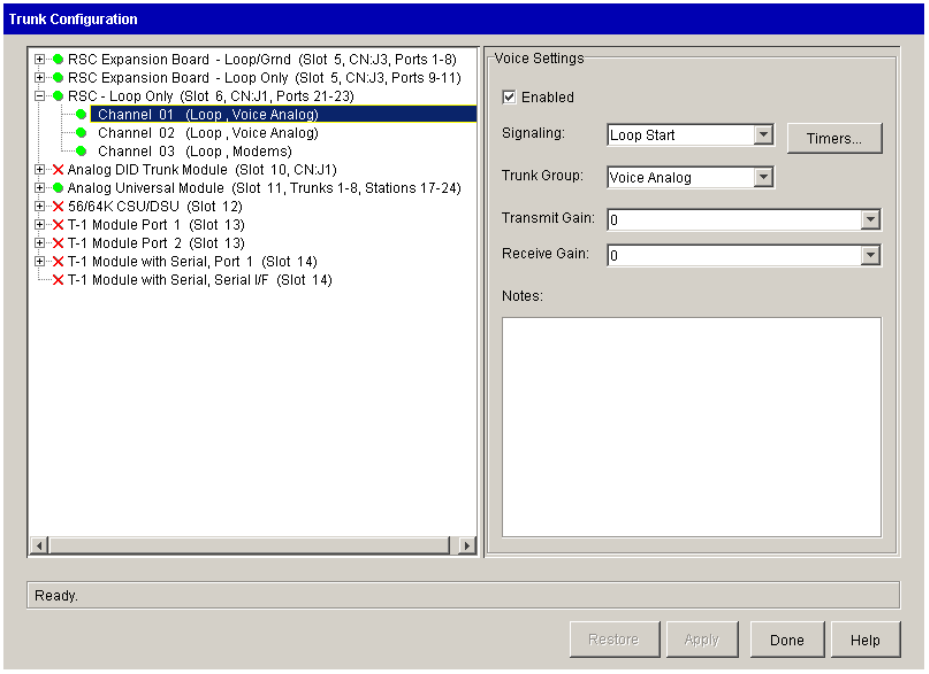


Figure 16-9 Trunk Configuration applet, with channel settings displayed

Note: You must select channels with the same Signaling configuration.

Depending on your signaling configuration for the selected trunks, you will see one of the following:

- The Analog Loop Start Timers dialog (Figure 16-10)
- The Analog Ground Start Timers dialog (Figure 16-11)

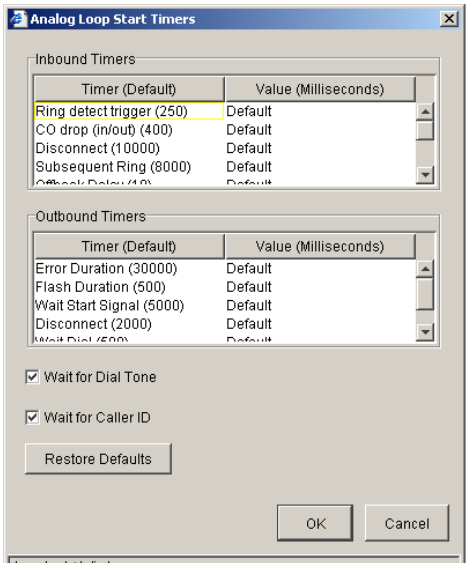


Figure 16-10 Analog Loop Start Timers dialog

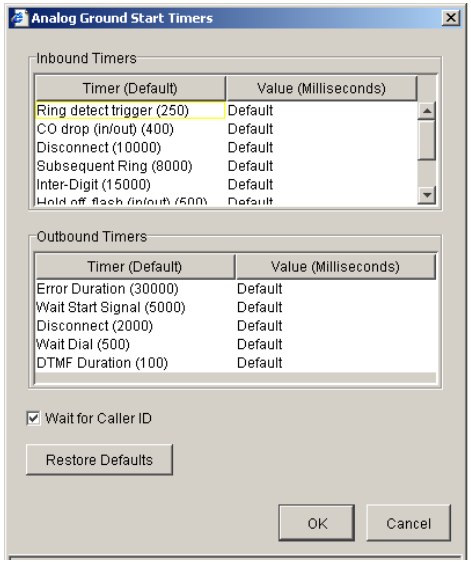


Figure 16-11 Analog Ground Start Timers dialog

4 Click the Value field of the timer that you want to edit.

A text box appears where you can type a new value.

5 Enter a new value for the timer.

For information about specific analog trunk timers, refer to the following tables:

- Table 33-7, Inbound analog trunk timers (loop start, ground start), on page 7
- Table 33-8, Outbound analog trunk timers (loop start, ground start), on page 8

6 If you are using Loop Start signaling, you can specify the Wait for Dial Tone setting by selecting or deselecting that check box.

This check box indicates whether Wave should expect a dial tone on the channel before dialing.

7 If you are using Loop Start signaling, select the Wait for Caller ID check box if you want to specify that the trunk should wait one ring for Caller ID information on an inbound call and answer on the second ring. (Caller ID information will come between the first and second rings.)

8 Click Apply to save your changes.

9 Click Done to return to the Management Console.

Configuring systemwide ISDN settings

Systemwide ISDN settings enable you to specify company-wide information about your ISDN channels, including how long-distance and international calls are dialed when using ISDN.

To set systemwide ISDN settings:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 Click the ISDN tab.

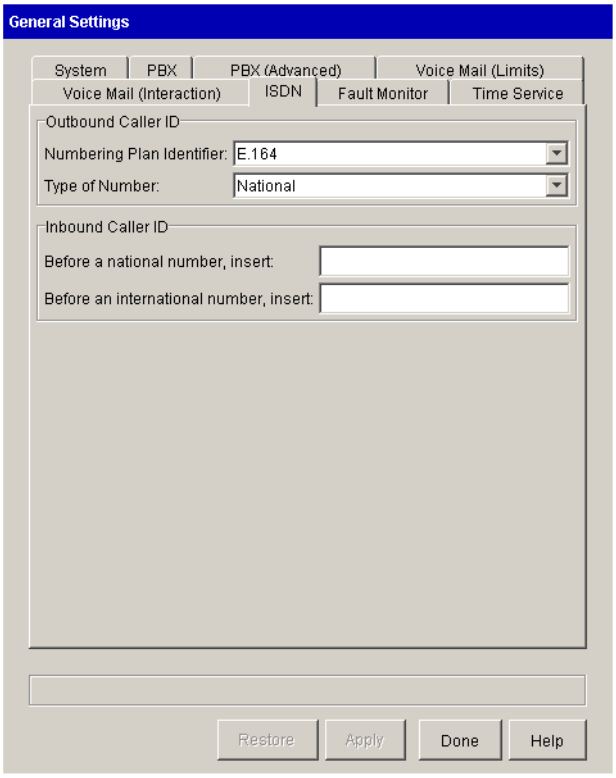


Figure 16-12 General Settings applet, with ISDN tab displayed

4 Specify the numbering plan identifier in the Numbering Plan Identifier drop-down list as specified in your Service Confirmation Letter.

The NPI is used to indicate the general way phone numbers are constructed within the Caller ID. The two most common numbering plans are E.164—the world-wide ISDN numbering standard—and Unknown, indicating that the sender does not want to specify a plan. Private indicates that the calling party may have a unique string of digits fro the calling party ID.

5 Specify a type of number in the Type of Number drop-down list as specified in your Service Confirmation Letter.

For example, the numbering plan you selected in step 2 may have four types of numbers: Unknown, Subscriber (local), National (long distance), and International.

Caution: *Do not modify this setting from the default value unless you are an expert.*

6 Specify any digits to insert prior to a national number.

For example, when Wave receives a call specified as National, it prepends a 1 in the Caller ID that is sent, so the receiver will know how to correctly return the call, if necessary.

7 Specify any digits to insert prior to an international number.

For example, when Wave receives a call specified as International, it prepends a 011 in the Caller ID that is sent, so the receiver will know how to correctly return the call, if necessary.

8 Click Apply to save your changes.

9 Click Done to return to the Management Console.

Outside Lines Configuration

CHAPTER CONTENTS

This chapter provides information about configuring call routing using Outside Lines.

Creating outside lines

An outside line is an entity that maps Outside Line keys on digital telephones directly to one or more trunks, simulating a key system for external telephone calls. Outside lines are configured in the Outside Lines applet. You must associate the outside line with a trunk in Trunk Configuration, and associate the outside line with keys on the digital telephones in the User Configuration (Templates) applet.

To create an outside line:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Outside Lines icon, located in the Trunk Administration section.

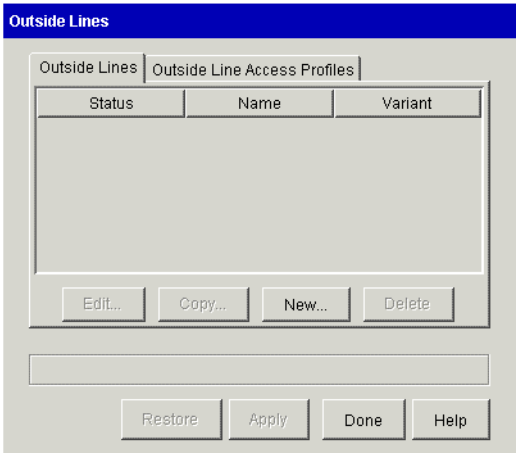


Figure 17-1 Outside Lines applet

3 Select the Outside Lines tab, and click New to open the Outside Line dialog box.

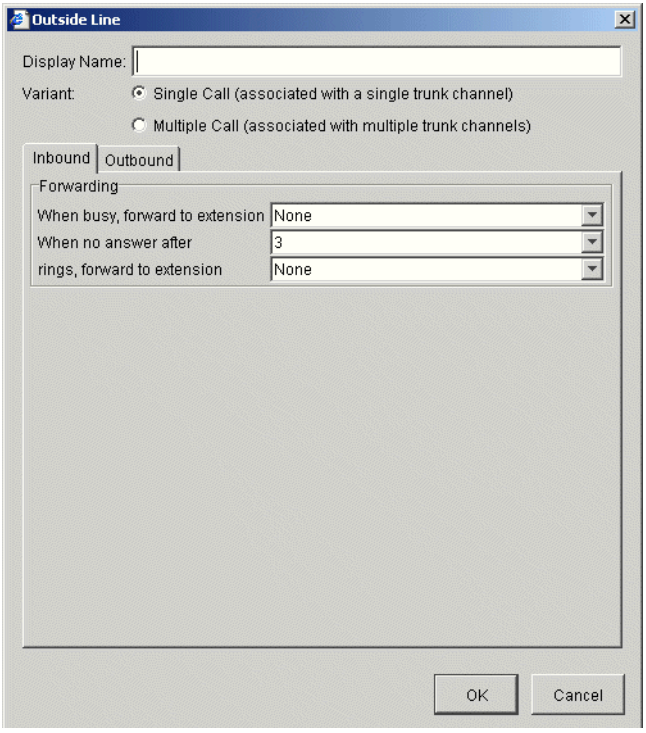


Figure 17-2 Outside Line dialog, showing Inbound tab

4 Enter a Display Name for the outside line.

This name will appear in the Trunk Configuration applet, so make the name easy to identify as an outside line.

Note: The Display Name field accepts up to 16 alphanumeric characters as well as the following special characters: ` ~ ! # $ % & * ( ) - = + | { } ; : " , . / < > ?

5 Choose the appropriate call variant.

- Single Call—allows you to associate this outside line with a single trunk in Trunk Configuration
- Multiple Call—allows you to associate this outside line with multiple trunks in Trunk Configuration

For a description of Single and Multiple Call variants see “Outside lines” on page 28-26.

6 Configure the Forwarding options in the Inbound tab.

   a Select a busy forwarding destination in the first drop-down list.

   b Select the number of rings before a call is forwarded in the second drop-down list.

   c Select the Ring No Answer destination in the third drop-down list.

7 Click the Outbound tab.

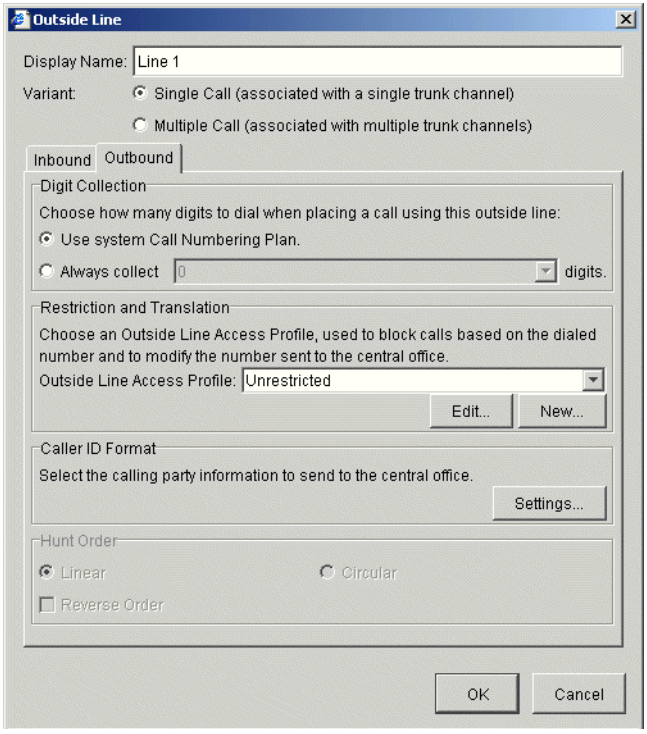


Figure 17-3 Outside Line dialog, showing Outbound tab

8 Configure the Digit Collection settings.

- Use system Call Numbering Plan—The system determines how many digits to wait for depending on the first digits dialed. For example, under the North American Numbering Plan, if a user dials a 1, the system waits for 10 more digits before sending the number to the central office.
- Always collect ***n*** digits—Requires users to enter the specified number of digits when using the outside line.

9 Choose an Outside Line Access Profile from the drop-down list.

Click Edit to edit an existing outside line access profile, or click New to create a new outside line access profile. See “Configuring outside line access profiles” on page 17-6 for instructions.

10 Configure the Caller ID format.

a Click Settings in the Caller ID Format group box.

The Caller ID Format dialog opens.

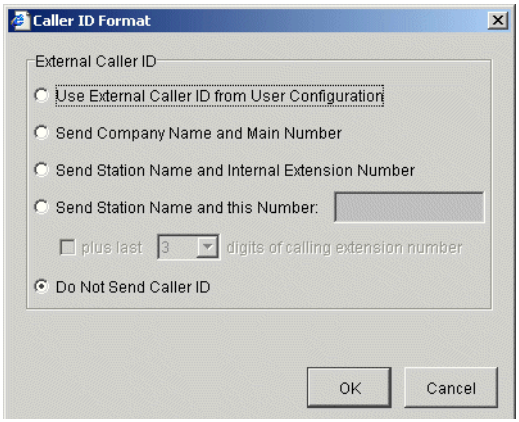


Figure 17-4 Caller ID Format dialog

b Select a Caller ID format.

c Click OK to close the Caller ID Format dialog box.

11 If you are configuring a Multiple Call Outside Line, select a trunk Hunt Order.

For information about trunk hunt order see “Trunk group hunt types” on page 26-7.

12 Click OK to close the Outside Line dialog box.

The new outside line appears in the Outside Lines table.

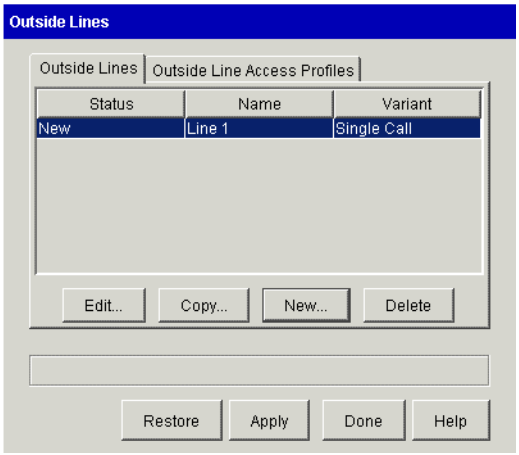


Figure 17-5 Outside Lines applet, showing new outside line

13 Click Apply to save your changes.

14 Click Done to return to the Management Console.

Configuring outside line access profiles

Configure outside line access profiles to create restriction and digit translation rules on outside lines.

To configure outside line access profiles:

1 If necessary, click the Administration tab of the Management Console.

Click 

2 Click the Outside Lines icon, located in the Trunk Administration section.

3 Click the Outside Line Access Profiles tab.

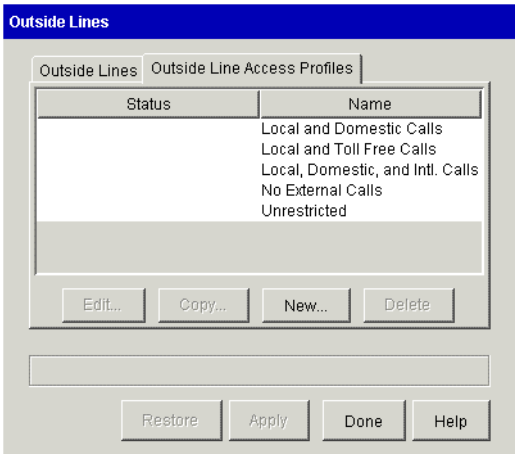


Figure 17-6 Outside Lines applet, showing Outside Line Access Profiles tab

4 To edit an access profile, select an access profile, and click Edit. To create a new access profile, click New.

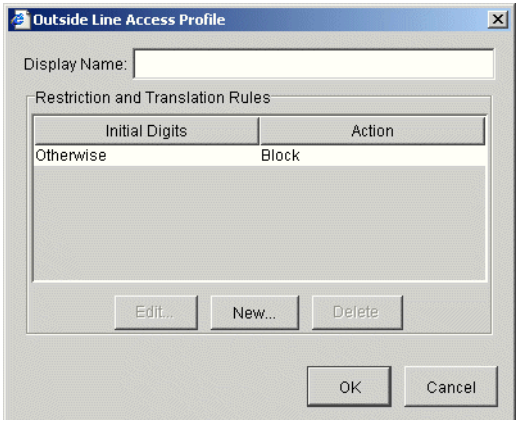


Figure 17-7 Outside Line Access Profile dialog

5 If you create a new outside line access profile, enter a unique Display Name.

6 Click New to create a new rule, or click Edit to alter an existing step.

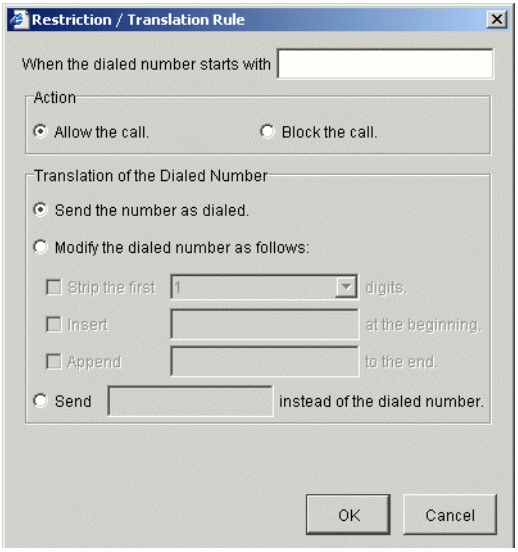


Figure 17-8 Restriction / Translation Rule dialog

7 If you are entering a new step, enter the initial digits for the reference telephone number in the When the dialed number starts with text box.

Use *x* as a variable digit.

8 Select an action:

- Allow the call
- Block the call

9 Specify digit translation if necessary.

If you choose to allow the call, there are digit translation rules you can apply to the dialed telephone number.

- If you want to send the telephone number exactly as it was dialed, select the Send the number as dialed option.
- If you want to strip digits from the beginning of the telephone number, select the Modify the dialed number as follows option, select the Strip check box, and specify how many digits to strip.
- If you want to insert digits at the beginning of the telephone number, select the Modify the dialed number as follows option, select the Insert check box, and specify the digits to add.

- If you want to add digits to the end of the telephone number, select the Modify the dialed number as follows option, select the Append check box, and specify the digits to add
- If you want to send a completely different telephone number, select the Send option and specify the telephone number to send

10 Click OK to close the Restriction / Translation Rule dialog box.

11 Click OK to close the Outside Line Access Profile dialog box.

12 Click Apply to save your changes.

13 Click Done to return to the Management Console.

Linking trunks with outside lines

The Trunk Configuration applet has a Trunk Group option where an outside line can be selected and associated with one or more trunks.

To associate an outside line with a trunk:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Trunk Configuration icon, located in the Trunk Administration section.

3 Configure your trunks according to “Configuring digital trunks and channels” on page 5-10.

4 Select the outside line from the Trunk Group drop down list.

OL| appears at the beginning of each outside line available.

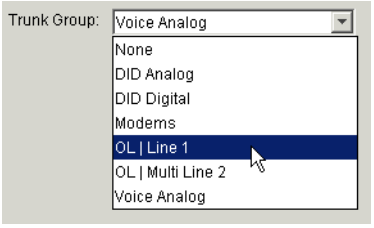


Figure 17-9 Trunk Groups in Trunk Configuration applet

5 Click Apply to save your changes.

6 Click Done to return to the Management Console.

Adding Outside Line keys to digital telephones

The User Configuration (Template) applet's digital telephone feature assignment dialog has an Outside Line button feature that requires an outside line and other parameters to be configured.

To create or edit a digital telephone template, refer to the instructions in "Configuring telephone templates" on page 10-1.

To include outside line keys on existing telephones, refer to the instructions in "Configuring telephone templates" on page 10-1.

To associate an outside line with a digital telephone key:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User Configuration (Templates) icon, located in the PBX Administration section.

3 Edit the digital telephone features.

You can select a user from the list and make changes to individual telephones from the Telephone tab, or select a digital telephone template, alter the template, and apply this template to multiple digital telephone users.

Figure 17-10 Telephone Template dialog, showing the Edge 100-12 telephone

4 Select a feature key from the digital telephone template dialog box.

5 Select Outside Line from the Feature drop-down list in the Feature Button Configuration dialog box.

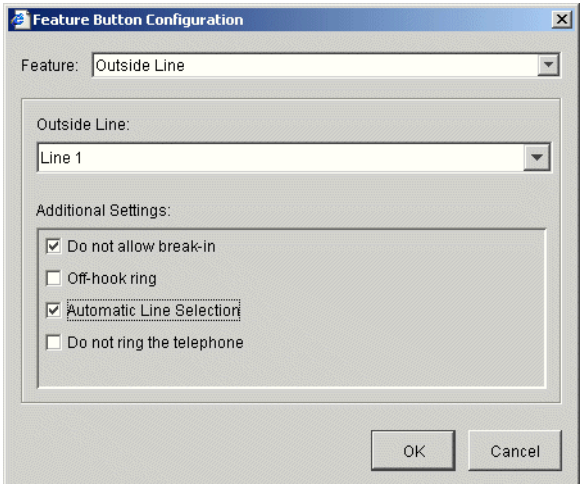


Figure 17-11 Feature Button Configuration dialog, showing Outside Line feature

6 Select an outside line from the drop-down list.

7 Configure any additional settings.

- Do not allow break-in—for the Single Call variant only, checking this setting allows you to deny break-in on any calls on this outside line key. This does not affect instances of the outside line on other telephones. Break-in is not supported on the Multiple Call variant of Outside Lines.
- Off-hook ring—checking this setting allows the telephone to ring when the handset is off-hook
- Automatic Line Selection—checking this setting allows this line to be selected for making calls automatically when an external access digit is dialed, or for answering calls when the telephone goes off-hook
- Do not ring the telephone—checking this setting is equivalent to a Do Not Disturb for this line. When a call comes in on the outside line the telephone will not ring, but the LED will flash amber.

8 Click OK to close the Feature Button Configuration dialog box.

9 Click OK to close the telephone template dialog box.

10 Click Apply to save your changes.

Click Done to return to the Management Console.

PBX Feature Configuration

CHAPTER CONTENTS

Authorization codes

Use the Authorization Codes applet to configure numeric passwords that allow users to place calls on telephones and telephone lines where call access is restricted.

Authorization codes can be used on analog telephones and Vertical Communications digital telephones. On Vertical Communications digital telephones, authorization codes can be used on primary and secondary line appearances and outside lines. Refer to the *Vertical Edge Digital Phone User's Guide* and the *Vertical Edge Digital Phone Quick Reference Guide* for information about using authorization codes.

Note: Authorization Codes cannot be used on IP telephones in this release.

To add authorization codes:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Authorization Codes icon, located in the PBX Administration section.

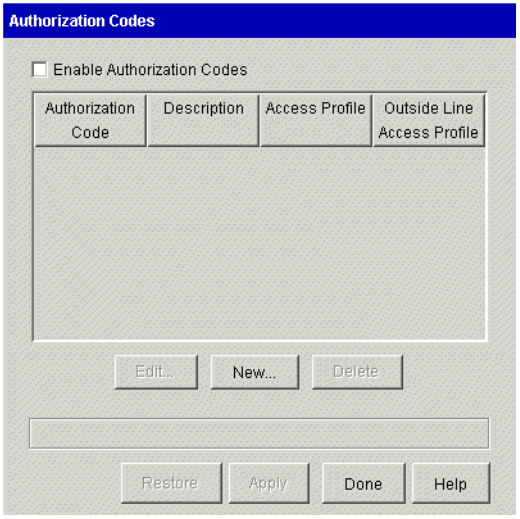


Figure 18-1 Authorization Codes applet

3 Click New to open the Authorization Code dialog box.

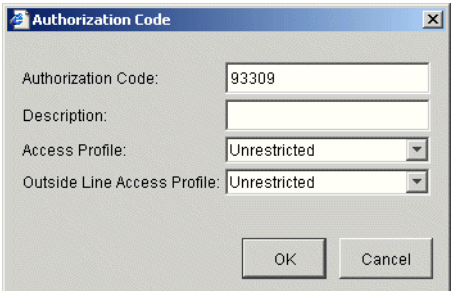


Figure 18-2 Authorization Code dialog

The Authorization Code field is automatically populated with a randomly selected unused 5-digit number. You may change this number to any 3- to 12-digit number.

4 Enter a Description.

5 Choose an Access Profile from the drop-down list.

The Access Profile determines what types of calls can be made on an Wave extension using this authorization code.

6 Choose an Outside Line Access Profile from the drop-down list.

The Outside Line Access Profile determines what types of calls can be made on an outside line using this authorization code.

7 Click OK to add the Authorization Code to the list.

8 Check the Enable Authorization Codes check box.

Authorization codes cannot be used until the Enable Authorization Codes check box is checked. When you are ready to enable authorization codes, check the Enable Authorization Codes check box.

9 Click Apply to save your changes.

10 Click Done to return to the Management Console.

Call Park options

Call Park places a call on an extension or in a system parking slot for retrieval from another telephone.

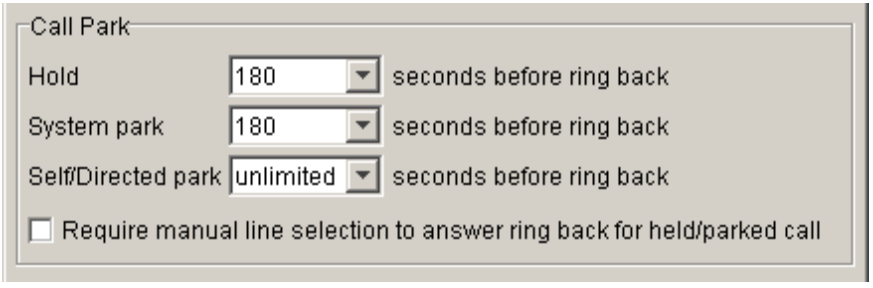


Figure 18-3 General Settings applet, Call Park options

In the General Setting applet, PBX (Advanced) tab, in the Call Park group box, specify the following call park settings:

- Hold *n* seconds before ring back.

  In the Hold drop-down list, select the number of seconds that Wave waits for a user to pick up a held call. If the call is not picked up within the specified time, Wave rings the extension from which the call was held.

If you specify unlimited seconds, then Wave does not ring back the extension.

- System park *n* seconds before ring back.

  In the System park drop-down list, *n* is the number of seconds that Wave waits for a user to pick up a parked call. If the call is not picked up within the specified time, Wave rings the extension from which the call was parked.

  If you specify unlimited seconds, Wave does not ring back the parking extension.

  An Enhanced Caller ID telephone or a digital telephone with a display is required to system park a call, but any telephone can be used to retrieve a system parked call.

- Self / Directed park *n* seconds before ring back.

  In the Self / Directed park drop-down list, select the number of seconds that Wave waits for a user to pick up a self-parked (or directed-parked) call. If the call is not picked up within the specified time, Wave rings the extension from which the call was parked.

  If you specify unlimited seconds, then Wave does not ring back the extension.

- Require manual line selection to answer ring back for held / parked call

  When you pick up the handset of a phone that has a call on hold or a parked call on the primary line, you can choose whether the phone connects you to the held / parked call or gives you dial tone on a different line to place a new call.

  - If checked, the phone provides dial tone when picked up. To connect to the held / parked call, you must select its line manually.
  - If unchecked, picking up the phone connects you to the held / parked call on the primary line.

Call pickup groups

You can configure call pickup groups—groups of extensions that can be answered by all the users in the group using the Group Pickup telephone feature—and add extensions to them in the User Configuration (Template) applet. An extension can belong to only one pickup group. There are two methods to pick up a call in a pickup group:

- Group—Any group member can answer the ringing extension of any other group member. Members in this group press the Group Pickup button on the digital telephone or dial ***74** to answer a call

- Extension—A user specifies which ringing telephone he or she wants to answer. The user presses the Extension Pickup button on the digital telephone, or dials ***75**+extension to pick up calls. Directed pickup works only for members of the same pickup group, or if neither extension is in a pickup group.

To create a pickup group

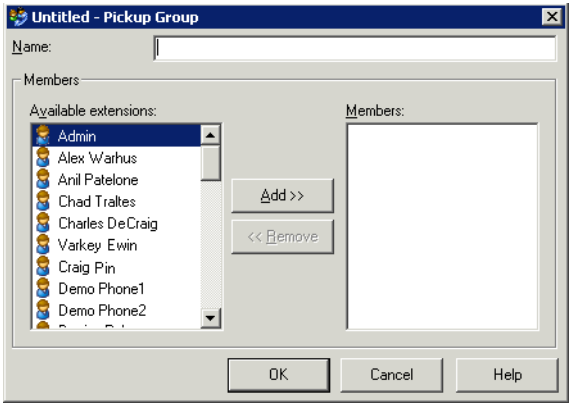
1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the **User/Workgroup Management** icon, located in the PBX Administration section of the Management Console.

3 Log on to the User / Workgroup Management applet, which opens in a remote access window. For information on navigating in the User / Workgroup Management applet, see “Using the User / Workgroup Management applet” on page 2-9.

4 Choose File > New > Pickup Group. The Pickup Group dialog box opens.



5 Enter a **Name** for the Pickup Group.

6 Select the users you want and move them into the Members list by clicking **Add**. Hold down the CTRL key as you click to select multiple users.

7 Click **OK**.

Pickup Groups you have defined appear in the Pickup Groups view. Click its icon in the view bar of the User / Workgroup Management applet to see and manage Pickup Groups.

Caller ID

Caller ID refers to the telephone number and name that identify a caller. There are thre classifications of Caller ID: external, internal, and inbound.

External Caller ID

External Caller ID refers to the name and number that identifies the caller when a call is sent by Wave over a trunk to the central office. External Caller ID can only be sent on an ISDN-PRI trunk. Wave does not send Caller ID on analog trunks, and if Caller ID is enabled on T-1 wink start or ground start trunks, the central office must be capable of receiving ANI/DNIS format.

In order to send a name with the Caller ID information, the call must be placed on an ISDN trunk, the Send Caller Name option must be selected in the trunk configuration, and the far end has to accept the name. See “Configuring digital trunks and channels” on page 5-10 for information about enabling Caller ID on digital trunks.

When an internal extension initiates a call, its external Caller ID is determined by the settings configured in the General Settings and the User dialog box, User\External Caller ID tab. When a trunk initiates an outbound call (a tandem call) the external Caller ID is the same as the received Caller ID (or it is the trunk group name if no Caller ID is received).

By default, Wave sends no Caller ID to the trunks. Outbound trunk groups, outside lines, and IP telephony call destinations are the gatekeepers of Caller ID. At this level Wave decides whether to send Caller ID to the trunk and in what format (see Figure 18-4).

To send Caller ID with outbound calls, you must perform the following tasks:

- Configure trunk-specific Caller ID settings (see “Configuring trunk-specific Caller ID settings” on page 18-9).
- Configure the systemwide Caller ID settings (see “Configuring systemwide Caller ID settings” on page 18-10).

By default, all internal extensions send the external Caller ID specified in the General Settings applet. For users with specific Caller ID requirements, configure the Caller ID settings in the User dialog box to override the General Settings Caller ID format (see “Configuring user-specific Caller ID settings” on page 18-12).

Hierarchy of external Caller ID settings

As shown in Figure 18-4, Caller ID information is configured at three different levels: trunk-specific, extension-specific, and systemwide. The systemwide Caller ID can be overridden by extension-specific settings, and the extension-specific settings can be overridden at the trunk-specific level.

For example, if at the systemwide level you choose to use the Company Name and Main Number, and at the extension level you choose to send no Caller ID, Caller ID will not be sent by that extension. However, if at the trunk level you choose to send the Company Name and Main Number, then the Company Name and the Company Main Number are sent even though the extension specified otherwise.

If you choose Use External Caller ID at the User dialog box level, and Use External Caller ID from General Settings at the extension level, all Caller ID information depends upon what is set at the systemwide level in the General Settings applet.

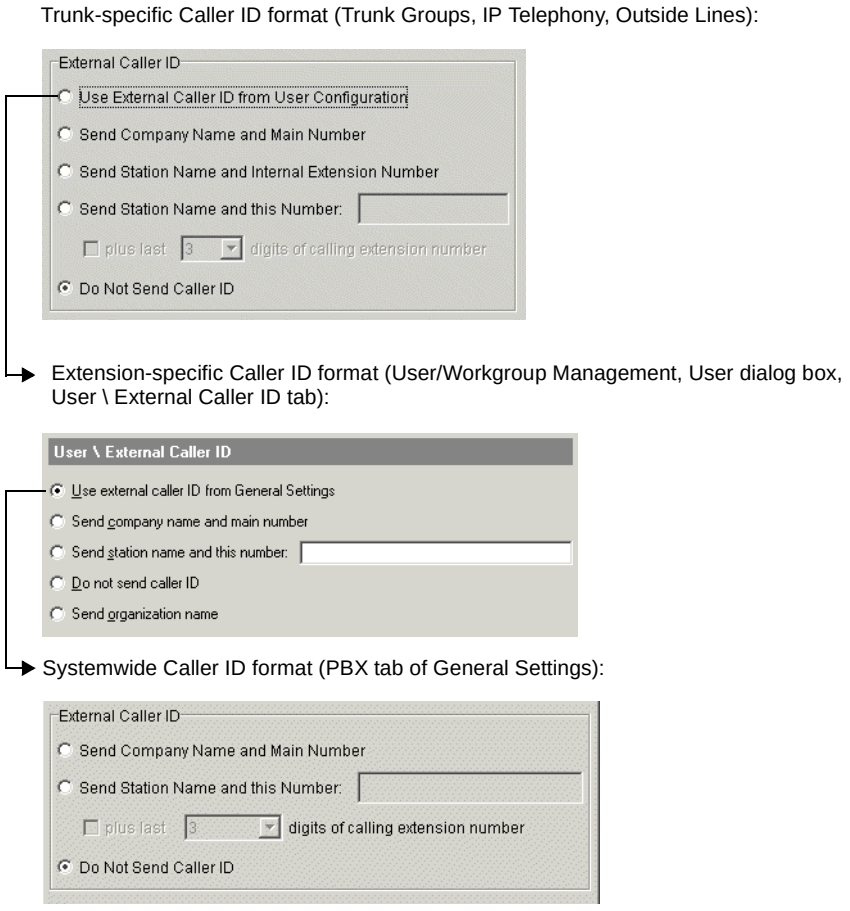


Figure 18-4 Caller ID format dependencies, showing system defaults

Internal Caller ID

Internal Caller ID refers to the name and number from an station-to-station call originating on the Wave ISM or a PBX connected to the Wave ISM. Internal Caller ID for extensions is always the Display Name and the extension number configured in the User dialog box.

Inbound Caller ID

Inbound Caller ID refers to the name and number received from an inbound call from an inbound trunk group, IP telephony source, or outside line. When a call arrives from a trunk (or IP telephony source), Wave might or might not receive Caller ID. If the Wave does receive Caller ID, this information is sent along with the call to its destination, whether it be internal or external.

If Caller ID is not received, Wave assigns Caller ID information to the call depending on the call source:

- **Inbound Trunk Group**—If the name is missing, the trunk group name (DID Digital, for example) is sent. If the number is missing, no number is sent.
- **IP Telephony**—If the name is missing, "IP Telephony" is sent. No number is sent with an IP telephony call.
- **Outside Line**—The name of the outside line is always sent. No number is sent on outside lines.

Configuring trunk-specific Caller ID settings

The trunk-specific Caller ID format determines whether Caller ID will be sent to the trunk and in what format. In the Trunk Groups, IP Telephony, and Outside Lines applets, you can configure the Caller ID values as they are supported by the trunks associated with the outbound trunk group, IP call destination, or outside line. Configuring Caller ID on a particular outbound trunk group affects all the trunks and digital channels associated with the trunk group.

Caution: *Check your service confirmation letter to determine whether Caller ID is supported on your trunks and in what format. Sending Caller ID to a trunk that doe not support it might cause your calls to fail.*

To configure trunk-specific Caller ID settings:

1 Navigate to the appropriate Caller ID settings for your application.
   - **Trunk group**—Open the Trunk Groups applet, edit a trunk group, and select the Out tab.
   - **IP call destination**—Open the IP Telephony applet, IP Call Destination panel, and edit a call destination.

- **Outside line**—Open the Outside Lines applet, edit an outside line, select the Outbound tab, and click Settings in the Caller ID Format group box.

2 Select a Caller ID setting (see Figure 18-4).

- Use External Caller ID from User Configuration—for calls initiated from stations, sends Caller ID (as it is specified in the User dialog box)
- Send Company Name and Main Number—sends the Company Name and Company Main Number
- Send Station Name and Internal Extension Number—for calls initiated from stations, sends the Display Name and extension number set in the User dialog box.

  Use this setting for trunks connected to other PBXs.
- Send Station Name and this Number—for calls initiated from stations, sends the call source Display Name and the number specified in the adjacent field

  If the check box is selected, the specified number of digits from the calling extension number are appended to the digits specified in the field.

  You can use this setting to provide the station name and DID number on outbound calls. It is recommended that you set this at the systemwide level in the General Settings applet.
- Do Not Send Caller ID—sends no Caller ID from this trunk group, IP call destination, or outside line

  Use this setting for trunks that do not support Caller ID, or for trunks where Caller ID should be blocked.

Configuring systemwide Caller ID settings

Configure the systemwide Caller ID settings for calls initiated by internal extensions in the General Settings applet. Remember that the external Caller ID is only sent to the central office if the trunk group is configured to send external Caller ID.

To configure systemwide Caller ID settings:

1 Enter the Company Name and Company Main Number in the General Settings applet, System tab.

The Company Name can include up to 16 alphanumeric characters. Caller ID cannot send more than 15 characters over ISDN.

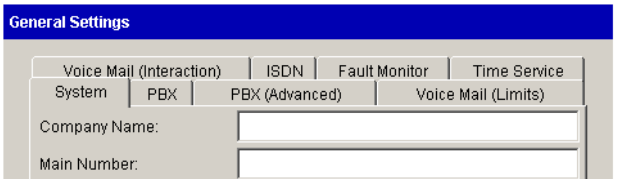


Figure 18-5 General Settings applet, System tab

2 Select a default External Caller ID setting for calls initiated by stations in the General Settings applet, PBX tab (see Figure 18-4).

- Send Company Name and Main Number—sends the Company Name and Company Main Number (entered in the General Settings System tab)

  Use this setting to provide some Caller ID information while keeping the actual calling extension number private.

- Send Station Name and this Number—sends the Station Name (entered in User Configuration (Templates)) followed by the digits entered in the adjacent field

  If the check box is selected, the specified number of digits from the calling extension number are appended to the digits specified in the field.

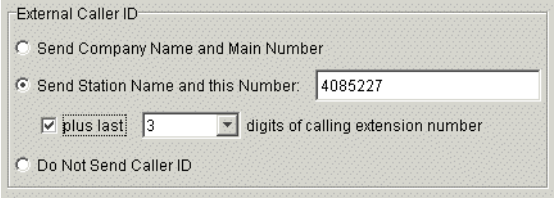


Figure 18-6 External Caller ID example sending a DID number

  For example, if you enter 4085227, and specify that the last 3 digits be added to the number, a call from extension 1234 will send the number 408-522-7234.

  Use this setting to provide the station name and DID number on outbound calls.

- Send Organization Name—sends the name of the Organization to which the calling user belongs. For more about Organizations, see “Using Organizations” on page 21-2.

- Do Not Send Caller ID—Wave will not provide External Caller ID.

Configuring user-specific Caller ID settings

By default all users send the external Caller ID format specified in the General Settings applet. To override the systemwide Caller ID settings for a specific user, see “The User \ External Caller ID tab” on page 11-15.

Dialing time-out

Configure the settings that determine how long Wave should wait after you finish dialing before placing the call.

Figure 18-7 General Settings applet, Dialing options

Click

In the General Setting applet, PBX (Advanced) tab, set When dialing, wait up to ***n*** seconds for next digit to be entered. This drop-down list sets the dialing timeout. If the specified time elapses before another digit is pressed, Wave will stop collecting digits and attempt to route the call based on the digits collected.

The dialing timeout is useful for dialing numbers of a length not expected by your dialing plan. For example, in North America, numbers are generally 7, 10, or 11 digits in length. If you are dialing an international number the length of the number will be longer than expected, or if you are dialing the local operator the number will be shorter. After you have finished dialing the number, Wave will wait the number of seconds specified in the drop-down list, and place the call as dialed.

Emergency dialing

By default, Wave is configured so that users must dial the external access code before dialing 911 to reach emergency services. This setting helps to prevent accidental calls to 911. If you want to allow users to dial 911 without having the dial the external access code, deselect the Require external access code to dial 911 (see Figure 18-7) check box in the General Setting applet, PBX (Advanced) tab.

Be sure that all users know whether they need to dial the external access code in an emergency.

External call routing restrictions

Any time a call comes in to the Wave ISM and is routed back out on another trunk (trunk-to-trunk), you must consider these external call routing restriction options. In this scenario a call is physically connected across two external trunks through the Wave ISM.

Scenarios include off-site call forwarding, off-site transferring, and conferencing where two or more parties is an external telephone number. These options can also affect your inbound call routing wherever you have an inbound call routed to an external destination.

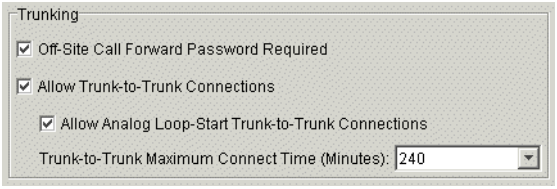


Figure 18-8 General Settings applet, Trunking settings

Click 

You can configure the following options in the General Setting applet, PBX (Advanced) tab, in the Trunking group box:

- Off-Site Call Forward Password Required—Select this check box if users must enter their Voice Mail passwords when forwarding their telephone calls to an external number.

  If you select this option, users must enter their Voice Mail passwords after specifying the external number when they forward their calls to an external telephone number. Instructions for off-site call forwarding are available in the *Vertical Edge Digital Phone User's Guide*.

  Note: this option does not apply if a user is forwarding their telephone to a Private Networking destination.

- Allow Trunk-to-Trunk Connections—To allow inbound calls to be routed to an external telephone number, through forwarding, transferring, or inbound routing, you must select this check box. Also, select this check box to allow conferences where two or more parties are external telephone numbers.
- Allow Analog Loop-Start Trunk-to-Trunk Connections—Select this check box to permit direct calls between analog loop-start trunks. Many connections of this type are left open, even after both parties hang up. If you select this check box,

you can specify a maximum connect time in the Trunk-to-Trunk Maximum Connect Time field to ensure that the connection is closed after a specified amount of time.

- Trunk-to-Trunk Maximum Connect Time (Minutes)—This setting causes Wave to disconnect any trunk-to-trunk calls after the specified time limit. Setting this option helps avoid a situation where a trunk-to-trunk call is in a loop (for instance, both sides are busy) where neither side knows to terminate the call. Select Unlimited to prevent Wave from automatically terminating a trunk-to-trunk call.

Music On Hold

To enable Music On Hold:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 Select the PBX tab.

4 Select a Music On Hold setting.

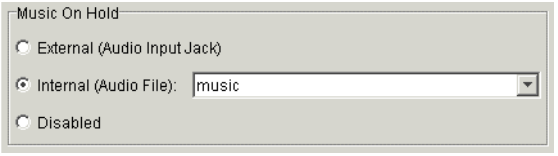


Figure 18-9 General Settings, Music On Hold settings

- External (Audio Input Jack)—Music On Hold from an external source requires third-party hardware as a music input source. Typically, CD players, radios, or specialized music-on-hold devices are used. Once it is installed, anyone who presses the telephone Flash or Hold button will hear music-on-hold. For a full discussion of external Music On Hold sources, see the *Vertical Wave IP 2500 Hardware Reference Guide*.
- Internal (Audio File)—This option is enabled if WAV files are present in the Wave C:\Inetpub\Ftproot\Options\Music directory. See the next section. Before you select this option, you must configure a system port in the Resource Management applet.

Click

a If necessary, click the Administration tab of the Management Console.

b Click the Resource Management icon, located in the PBX Administration section

c Expand the Application Resources folder.

d Expand the Music On Hold folder and select Wave Player.

e Select a port from the TAPI/WAVE Ports drop-down list (on the right side of the applet).

f Click Apply to save your changes, and click Done to close the Resource Management applet.

- Disabled—Disables Music On Hold.

Note: After you click Apply or Done, Music On Hold takes effect immediately. However, calls currently on hold without music will remain without music. If you switch from an Internal to an External hold music source, SIP calls currently on hold will continue to hear the Internal music.

Using custom audio files for system hold music

You can use your own .WAV audio files for system hold music by doing the following:

- Place the .WAV files in the following directory on the Wave ISM computer: C:\Inetpub\ftproot\Private\Options\Music
- For a .WAV file to play over SIP trunks and stations, you must also place codec files with the same filename as the .WAV file in the following directory on the Wave ISM computer: C:\Inetpub\ftproot\Private\Options\IpMOHMusic. For example, Name.wav, Name_3bit.g723, Name_5bit.g723, Name.g729.

Public Address

Public Address requires third-party hardware for amplification on an analog-only Wave system. If you have digital telephones, the speakers on the telephones act as a public address system and announcements are sent to digital telephone speakers as well as the overhead public address system.

To enable the public address system:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 Select the PBX tab.

4 Select the Enable Public Address check box.

Figure 18-10 General Settings applet, Enable Public Address setting

Once Public Address is enabled, users can make announcements over the public address system and digital telephone speakers by pressing the System Page key on digital telephones, or dialing ***11**. For more information about the System Page key see “Page” on page 14.

Night Answer

The Night Answer feature enables you to manually place Wave into a mode where inbound calls are redirected to predetermined destinations. You can configure any on- or off-premise telephone number as the destination.

On digital telephones, configure a Night Answer button to activate and deactivate Night Answer. When Night Answer is active, the LED flashes red. When Night Answer is not active, the LED is dark.

On telephones without a Night Answer button, dial *85 to activate Night Answer and *86 to deactivate Night Answer.

To configure Night Answer:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 In the PBX tab of the General Settings applet, select the Night Answer Mode check box and enter a destination in the Default Night Answer Destination field.

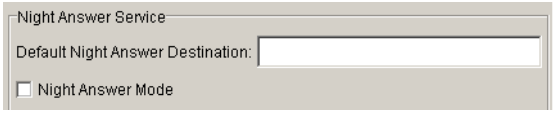


Figure 18-11 Night Answer Service group box

4 Edit your inbound trunk groups' Inbound Routing Tables to specify the correct night answer mode in the Night Answer Mode field.

- If you are configuring your incoming T-1 or analog trunks for Night Answer, open the Trunk Groups applet and edit your Inbound Routing Tables.
- If you are configuring your incoming IP Telephony calls for Night Answer, open the IP Telephony applet, select Default Inbound Routing from the Call Routing folder, and click the Edit Inbound Routing Table button.

The available Night Answer Modes are as follows:

- Not Used—disables the Night Answer Mode for this trunk group
- Use System Default—uses the Default Night Answer Destination specified in the General Settings applet

  Note: Select an Access Profile for Tandem Calls in the *Inbound Trunk Group* dialog and enable Allow Trunk-to-Trunk Connections in the General Settings (PBX (Advanced) tab) if the Default Night Answer Destination you specified in General Settings is an off-premise call and not routed using the Global Access outbound routing rules.

- User Defined—uses the destination that you enter in the Night Answer Destination field in the Inbound Routing Table and it overrides the system default specified in the General Settings applet

  Note: Select an Access Profile for Tandem Calls in the Inbound Trunk Group dialog and enable Allow Trunk-to-Trunk Connections in the General Settings (PBX (Advanced) tab) if the Night Answer Destination you specified is an off-premise call and not routed using the Global Access outbound routing rules.

Note: The night answer mode configuration is not allowed for the Modem trunk group.

5 If you want to configure digital telephones with a Night Answer button, change the configuration of the those telephones in the User Configuration (Templates) applet.

System Speed Dial

Use the System Speed Dial applet to assign three-digit speed dial numbers to telephone numbers that your organization uses frequently.

System speed dial numbers can be used on analog and digital telephones. Refer to the Vertical Communications *Vertical Edge Digital Phone User's Guide* and the *Vertical Edge Digital Phone Quick Reference Guide* for information about using system speed dial.

Find System Speed Dial information in the following sections:

- Adding speed dial numbers
- Setting the System Speed Dial password
- Adding speed dial numbers using the telephone

Adding speed dial numbers

To add speed dial numbers in the System Speed Dial applet:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the System Speed Dial icon, located in the PBX Administration section.

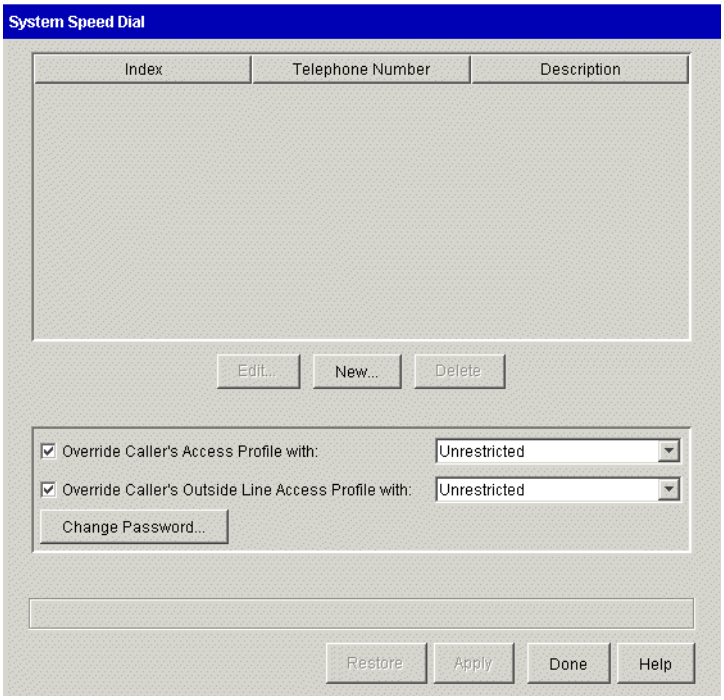


Figure 18-12 System Speed Dial applet

3 Click New to open the Add New Index dialog box.

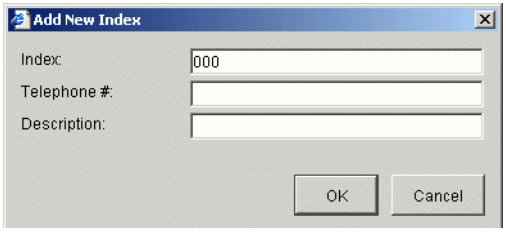


Figure 18-13 Add New Index dialog

4 Enter the speed dial number in the Index field.

The Index field is automatically filled in with the next available index number. You can enter any number in the range 000-999.

5 Enter the telephone number in the Telephone # field.

A telephone number can be any digit sequence up to 32 digits in length. Be sure to include the external access code if necessary.

Note: Telephone numbers for external calls must include the first digit defined in the First Digit Table applet for external dialing access. These external speed dial numbers can be dialed using primary lines, secondary line appearances, and outside lines.

6 Enter a description for the speed dial number.

A description can be any character sequence up to 32 characters in length.

7 Click OK to close the Add New Index dialog box.

8 Click Apply to save your changes.

9 Click Done to return to the Management Console.

Setting the System Speed Dial password

The System Speed Dial password applies to all speed dial numbers.

To set the System Speed Dial password:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the System Speed Dial icon, located in the PBX Administration section.

3 Click Change Password.

Figure 18-14 Change Password dialog

4 Enter a five-digit password in the Enter New Password field.

5 Enter the password again in the Confirm Password field.

6 Click OK.

7 Click Apply to save your changes.

8 Click Done to return to the Management Console.

Adding speed dial numbers using the telephone

To add speed dial numbers using the telephone:

1 From any telephone on Wave, dial *88.

2 Enter the five-digit System Speed Dial password.

3 Enter the three-digit speed dial index number.

4 Enter the telephone number.

A telephone number can be any digit sequence up to 32 digits in length. Include the trunk access code (for example, 9) for external calls.

5 Press # to save the number.

For example:

```
*88 + [password] + [index] + [telephone number] + #
```

For example, you might enter:

```
*88 12345 123 914085551212 #
```

If the password is correct, Wave responds with two beeps indicating that the speed dial number was created. The number will overwrite any number previously stored at that index.

If the password is incorrect, Wave responds with a fast-busy tone.

A description is entered in the System Speed Dial table indicating the extension number from which the speed dial number was entered. You can open the System Speed Dial applet to edit the description.

Overriding access profiles

By default, Wave will not override an access profile assigned to a line appearance or an outside line in order to route a call initiated with a system speed dial number. For example, if an extension does not have permission in its access profile to dial long distance numbers (a extension's telephone line appearances or outside lines might have Local Only access profiles assigned to them), a user cannot use the system speed dial numbers that correspond to long distance telephone numbers on that extension.

If you want users with restrictive access profiles to be able to use system speed dial numbers that require a higher level access profile, you must override the user's access profile in the System Speed Dial applet.

To override user access profiles when using System Speed Dial:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the System Speed Dial icon, located in the PBX Administration section.

3 Check the appropriate override options.

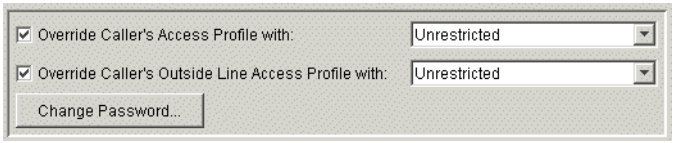


Figure 18-15 System Speed Dial access profile options

- **Override Caller's Access Profile**—allows Wave to override a line appearance access profile with the specified access profile when a user dials any system speed dial number on a Wave extension.
- Override Caller's Outside Line Access Profile—allows Wave to override outside line access profiles with the specified access profile when a user dials any system speed dial number on an outside line.

4 Select the appropriate access profiles from the drop-down lists.

Note: Access profiles for line appearances are configured in the Outbound Routing applet; refer to "Configuring specific access profiles" on page 9-10. Access profiles for outside lines are configured in the Outside Lines applet; refer to Chapter 17, Outside Lines Configuration.

5 Click Apply to save your changes.

6 Click Done to return to the Management Console.

Virtual extensions

Configure virtual extensions for users who do not need a physical telephone, but require an office extension. These users might be employees who work on the road with a cell phone, but who need to have an office extension listed in the Voice Mail Names Directory (see Chapter 13, Configuring Auto Attendants).

To configure virtual extensions:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the User / Workgroup management icon, located in the PBX Administration section. Log in to the User / Workgroup Management applet when it opens in the remote session window.

3 Click **File > New User** to open the User dialog box.

4 Enter appropriate name information.

5 Enter an **Extension** number.

6 Under **Associated device**, use the **Slot:port** section to select **No Slot Selected** and **No Port Selected** from the drop-down lists.

7 Select **Analog** from the **Telephone type** list.

8 On the User \ External Caller ID tab, select **Do Not Send Caller ID**.

9 Configure other user options as needed.

10 Click **OK** to close the Configure User dialog box.

Zone paging groups

Zone paging groups allow you to page a group of digital telephones simultaneously. Zone paging groups are configured in the Zone Paging Groups applet.

Note: The Wave system has a maximum of 20 groups, including hunt groups, trunk groups, and zone paging groups.

If you have an overhead public address system connected to the Wave ISM, it will not be included in any zone paging group. See “Public Address” on page 18-15.

To create a zone paging group:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Zone Paging Groups icon, located in the PBX Administration section.

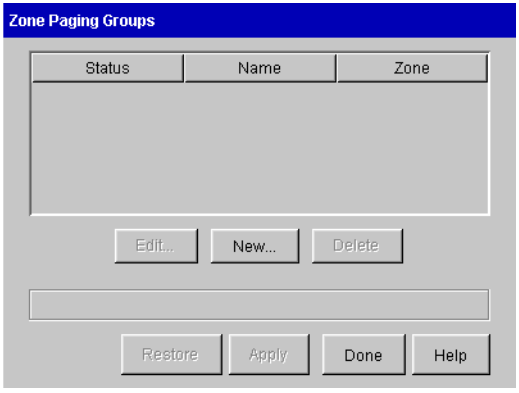


Figure 18-16 Zone Paging applet

3 Click New to open the Zone Paging Group dialog box.

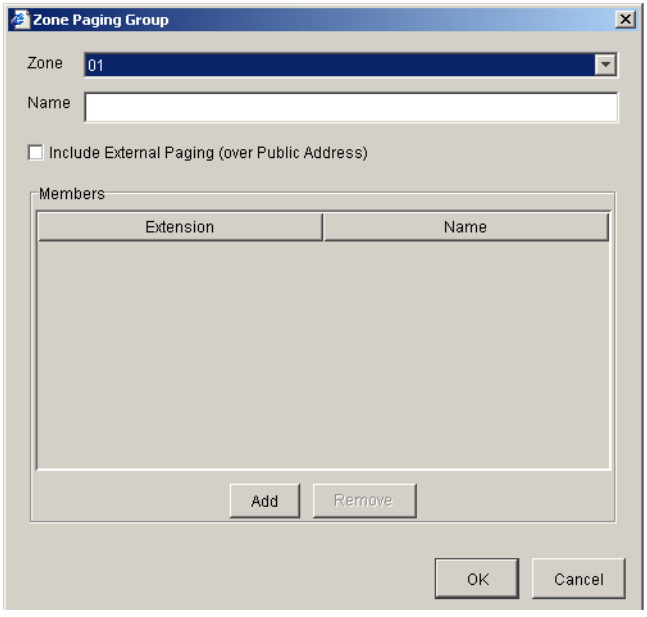


Figure 18-17 Zone Paging Group dialog

4 Select a zone number from the Zone drop-down list.

5 Enter a descriptive name for the zone paging group in the Name field.

6 Click Add to open the Add Zone Paging Group Members dialog box.

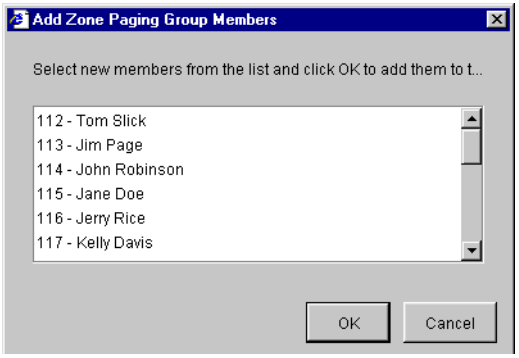


Figure 18-18 Add Zone Paging Group Members dialog

Note: Only digital telephones, configured in the User Configuration (Templates) applet, appear in the list.

7 Select members from the list for the zone paging group.

8 Click OK.

The Members list is populated with the members you selected.

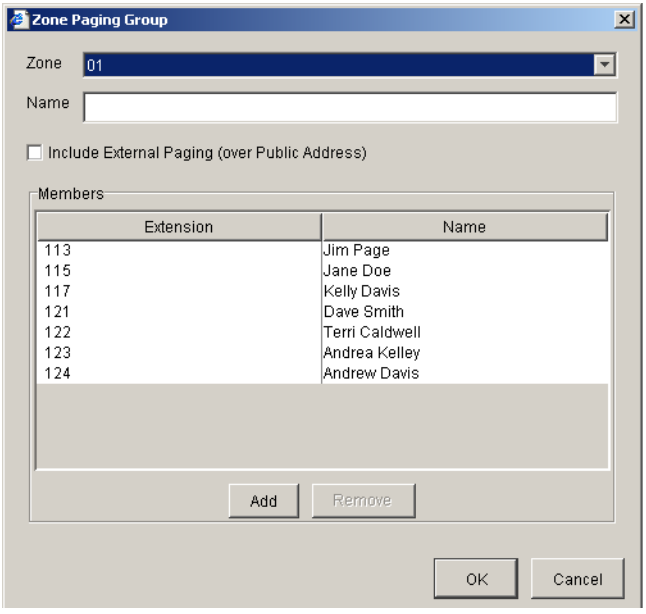


Figure 18-19 Zone Paging Group dialog, showing group members

9 Click OK.

The new zone paging group appears in the Zone Paging Groups applet.

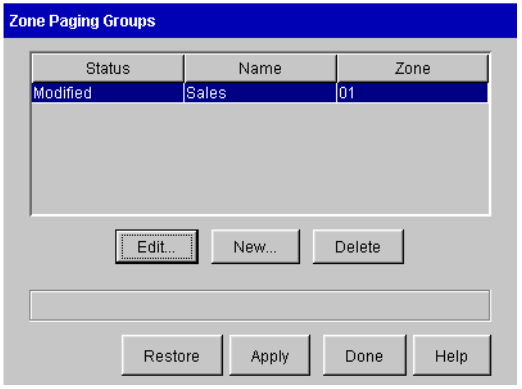


Figure 18-20 Zone Paging Groups applet, showing a zone paging group

10 Click Apply to save your changes, and click Done to close the Zone Paging applet.

Refer to the *Vertical Edge Digital Phone User's Guide* and the *Vertical Edge Digital Phone Quick Reference Guide* for information about using the Page feature.

Managing System Prompts and Audio

CHAPTER CONTENTS

About system prompts and audio

System prompts are audio prompts that Wave plays to callers and users. System prompts offer callers menu choices and provide menus and instructions to users. This chapter explains how to play and rerecord the system prompts used throughout Wave.You can use the standard prompts included with the system or record over them to create customized prompts.

The chapter also describes how to set up hold music, which enables callers to hear music whenever they are put on hold by a user or the system.

Setting general system prompt options

This section describes general system-wide options you can set for system prompt behavior.

Setting the system prompt language

You can choose which language system prompts play in by default. Individual users can select a different language for prompts that are played to users and callers navigating their accounts.

To set the default system prompt language:

1. From the Management Console, click the icon for **User/Workgroup Management**, located in the PBX Administration section. The User / Workgroup Management

   applet opens. See "Using the User / Workgroup Management applet" on page 2-9 for information about navigating in the User / Workgroup Management applet.
2. Choose **Tools > System Settings**. The System Settings dialog box opens.
3. Choose the Audio tab.
4. From the **Default system prompts** dropdown list, select the language you want.
5. Click **OK**.

Presenting a confirmation prompt before voicemail

You can choose whether or not callers hear the prompt, "To leave a message press 1, or press * to return to the menu" after they hear a user's voicemail greeting. See "Setting general ISM settings" on page 4-4.

The System Prompts view

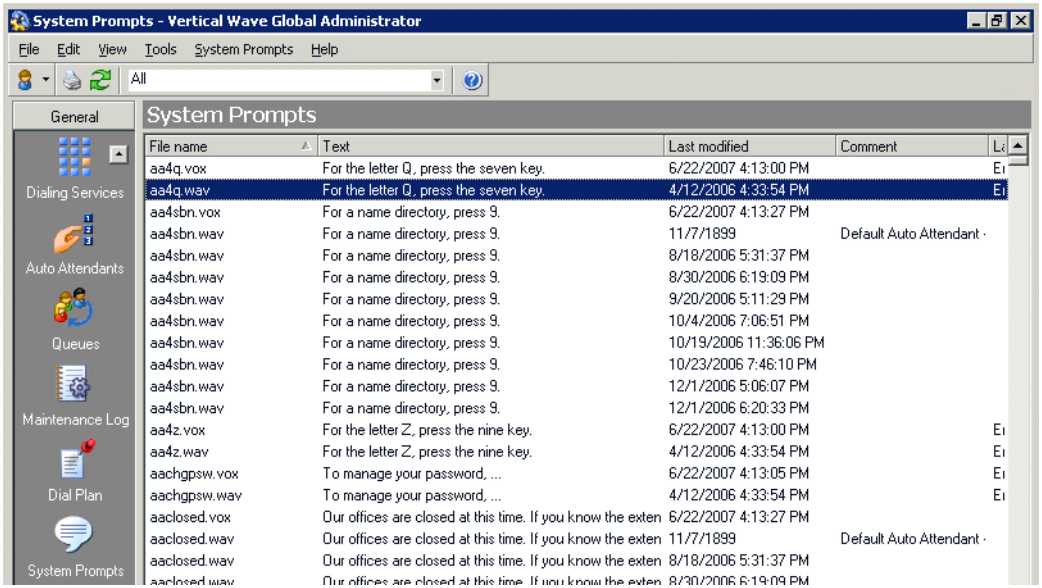
The System Prompts view in the User / Workgroup Management applet allows you to listen to and change the recordings used for standard system prompts and auto attendants. For example, when you are setting up your Wave system, you typically go to this view to change the default Greeting prompt so that it contains your company name.

To display the System Prompts view:

1 From the Management Console, click the icon for **User/Workgroup Management**, located in the PBX Administration section. The User / Workgroup Management

applet opens. See “Using the User / Workgroup Management applet” on page 2-9 for information about navigating in the User / Workgroup Management applet.

2 Click the System Prompts button in the view bar to open the System Prompts view.



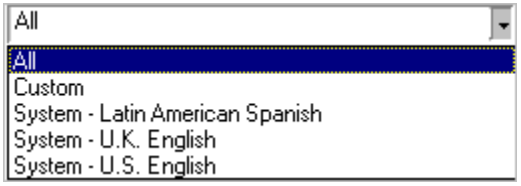
Each system prompt appears as a row in the view. The information in the following table is displayed for each system prompt.

Column	Description
File name	File name of the prompt.
Text	Contents of the file in text form. The text displayed here is accurate only if it is updated each time the file is changed. If you are unsure of the accuracy of the text, play the file to confirm what it says.

Column	Description
Last modified	Last time that the file was modified.
Comment	How the prompt is used in Wave. Applies to custom prompts and auto attendant prompts only. The column is blank for all other prompts.
Language	The set of language prompts to which this system prompt belongs. User-recorded prompts such as auto attendant prompts have this column blank.

Controlling the prompt display

By default the System Prompts view displays all system prompts on the Wave ISM. Use the control on the toolbar if you want to display only the custom prompts you have recorded or only the prompts for a single language.



Note: To install additional language prompts, you must run the Wave ISM installation again and select the languages you want.

Managing system prompts

This section explains the following aspects of managing system prompts:

- "Playing system prompts"
- "Exporting system prompt text" (page 19-5)
- "Exporting and importing system prompt audio files" (page 19-6)

Playing system prompts

You can play system prompts to confirm that they contain the correct information. System prompts play over the telephone or through your computer speakers. If you choose to play a prompt over the telephone, your phone rings and the prompt plays when you answer. See “Using the audio controls” on page 2-15 for more information.

To play a system prompt:

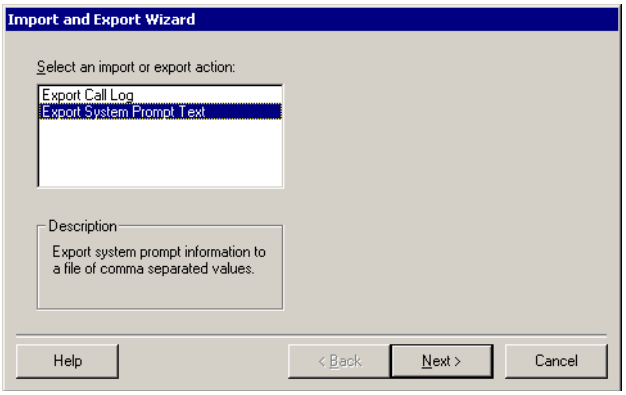
1. Select the name of the prompt that you want to play.
2. Choose **System Prompts > Play**.

Exporting system prompt text

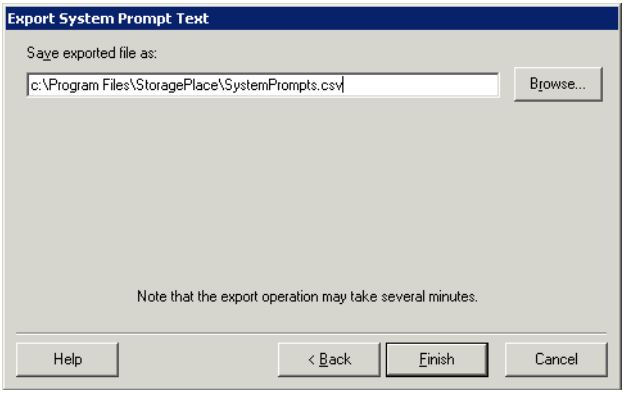
Use the following procedure to export system prompt text into a .CSV file for processing by a professional recording studio or for maintenance purposes.

To export system prompt text:

1 Choose **File > Import and Export**. The Import and Export Wizard opens.



2 Select **Export System Prompt Text** and click **Next**.



3 Under **Save exported file as**, accept the suggested location and file name or click **Browse** and choose a different location and enter a file name.

4 Click **Finish**. The file is exported.

Exporting and importing system prompt audio files

You can export a system prompt from your ISM for use on another Wave ISM. You also can import an existing sound file and use it as a system prompt. For more information, see “Importing and exporting voice files” on page 2-15.

Recording over system prompts

You may want to record over system prompts for some of the following reasons:

- You want your custom prompts and system prompts to be recorded with the same voice.
- You want to change the message text of a prompt, for example, the Welcome message.
- You have access to voice talent that you prefer over the existing Wave voices.
- You have localized the telephone commands for a language not provided with Wave (see "Localizing the telephone commands" on page 19-14) and want to record all of the prompts in that language as well.

Recording options

You can record system prompts in either of the following ways:

- "Recording system prompts professionally" (page 19-8)
- "Recording over system prompts yourself" (page 19-10)

The sentence file

The sentence file is a text file that contains all the voice prompts and the sentences they form. The American English sentence file is located in:

C:\Program Files\Wave Server\TVLEN00.INI

Note: "EN00" identifies American English files. Wave includes two other sets of system prompts. EN10 identifies British English files. ES00 identifies Latin American Spanish files.

The .WAP and .WAV files

Wave prompts are contained in the .WAP file, an indexed file containing individual .WAV recordings of variable information. Variable information, for example, numbers and dates, is used to build more complex prompts.

The .WAP files are used together to produce the complete prompts that callers and users hear. For example, in the sentence prompt, “You have three new messages, and twelve saved messages”, the words “three” and “twelve” come from the .WAP file.

The American English .WAP files are located in:

C:\Program Files\Wave Server\Vfiles\EN00

The American English .WAP file is called TVLEN00.WAP.

The recording process

To record a complete set of system prompts, you must do the following:

- Record the .WAP file.
- Build the indexed .WAP file.
- Test the new prompts.
- Deploy the new prompts.

Recording system prompts professionally

If you choose to obtain professional recordings, you should choose a voice vendor with experience in telephony recording, and then:

- Select a voice
- Provide the appropriate files to the vendor in formats they can use
- Test the new prompts for voice quality, usability, file-naming accuracy, and indexing accuracy
- Deploy the new prompts

Selecting a voice

The vendor will often provide you with 44kHz, full-bandwidth voice samples from which to choose. Ask your vendor to provide voice samples that have been re-sampled or recorded as MuLaw PCM Mono 8 kHz, which is the format used in Wave. This will ensure that your selection is based on how the voice will actually sound when used in your Wave system.

Keep in mind that high-pitched voices and high-frequency sounds degrade more as a result of this type of re-sampling, which may result in considerable change in higher frequency sounds at telephony bandwidth.

Using the standard Wave voices

To add or modify prompts using one of the standard Wave voices, contact Marketing Messages as shown in the following table. They provided the original set of prompts. Marketing Messages can record new voice files using the standard voices.

Language	Voice
U.S. English	"Ellen"
Latin American Spanish	"Claudia"
U. K. English	"Helen"
French Parisian	"Sylvie"
French Canadian	"Gisele"
German	"Anneli"

Contact Marketing Messages as follows:

Marketing Messages
51 Winchester Street
Newton, MA, U.S.A. 02461

800-486-4237 (phone)
617-527-3728 (fax)

http://www.marketingmessages.com

Providing files to the vendor

After you have selected a voice, you must provide your vendor with the list of prompt files and the text of each prompt to be recorded. The list of prompt files is available in the System Prompts and Prompts section of the TVLEN00.INI file.

You also need to provide your vendor with the TVLEN00.WAP file, so that your voice vendor can match the indexing of the new .WAP file to the existing file.

Testing the new prompts

It is important that you thoroughly test all voice files that you receive from the vendor to ensure:

- Accuracy of file names
- Synchronization of written and spoken prompt content
- Quality of voice recording
- Accuracy of index order and format of the .WAP file

See "Testing system prompts" on page 19-12 for information about using the Sentence Tester to assist with some of these tasks.

Deploying the new prompts

After all files are tested, you can replace the existing prompt files with the new ones. Place all new .WAV files and the .WAP file in the following directory:

C:\Program Files\Wave Server\Vfiles\User

The following auto attendant prompts must also be copied to the User directory.

- AACLOSED.WAV
- AAHI.WAV
- AA4SBN.WAV
- AAOPORWT.WAV

The default location is `C:\Program Files\TeleVantage Server\Voice Files\EN00`.

Recording over system prompts yourself

When you record over system prompts yourself, you can record all of the .WAV files as well as the.WAP file, as with professional recording, or record just the .WAV files and use the .WAP file included with Wave.

If you do not record over all the files, be aware that since prompts are combined with other prompts when presented to callers or users, recording some but not all prompts may result in a mismatch of voices.

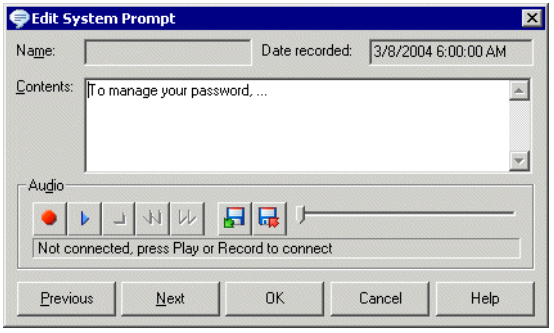
Recording over .WAV files

You use the User / Workgroup Management applet to record over these files (see the next procedure).

To record over a prompt:

1 In the System Prompts view, double-click the prompt. The Edit System Prompt dialog box opens.

2 Under **Contents**, enter the text of the new prompt. Use this text as a script when you record the prompt.



3 Record the prompt. See “Using the audio controls” on page 2-15 for instructions.

4 Click **OK** to save the new version of the prompt.

Recording over the .WAP file

You can record over the .WAP file by using a variety of recording tools and WAP tools. If you do not already have such a tool, you should consider VFEdit, which is available on the Internet.

Testing and deploying the new prompts

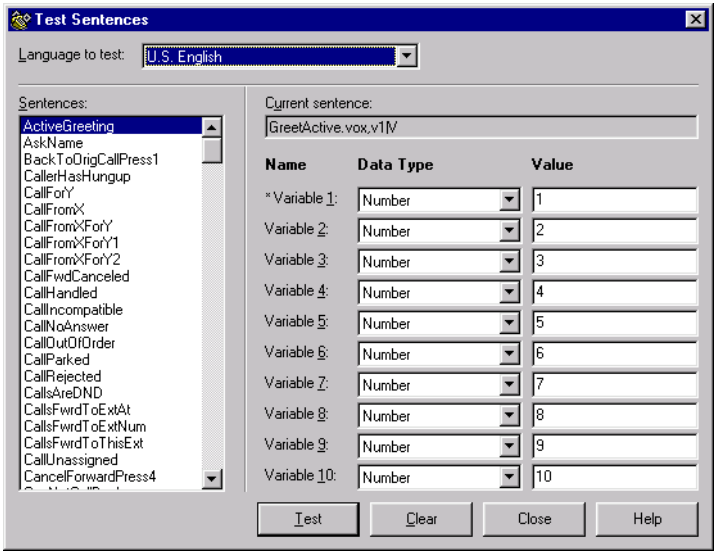
Use the Sentence Tester to test the new prompts. See “Testing system prompts” on page 19-12. For information about deploying the new prompts, see “Deploying the new prompts” on page 19-10.

Testing system prompts

You can test system prompts by listening to them in context over your telephone. By joining individual prompts into sentences and playing them as they are used in Wave, you can evaluate intonation, emphasis, and consistency.

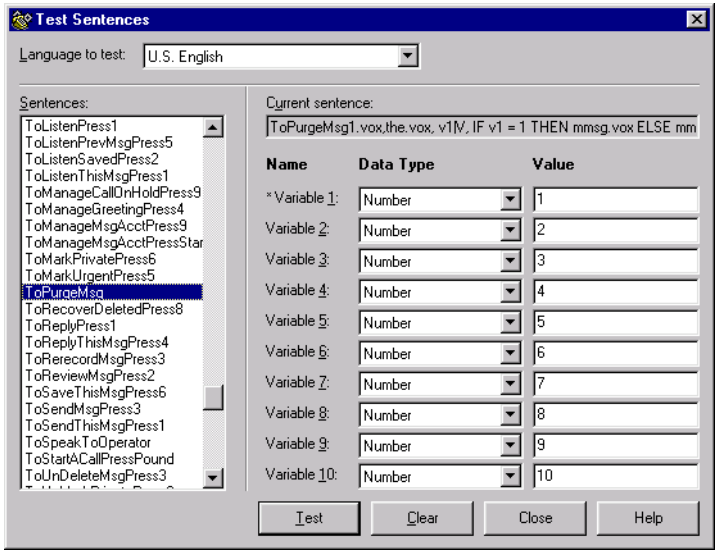
To test system prompts:

1. Start the User / Workgroup Management applet using the `/sentence` command line option.
2. Choose **Tools > Test Sentences**. The Test Sentences dialog box opens.



3. In **Language to test**, select the language of the prompts that you want to test.

4 Under **Sentences**, select a sentence from the list.



The **Current sentence** box displays how that sentence is described in the sentences.ini file. Many sentences consist of a single .WAV file. Other sentences are made up of several joined .WAV files, and may contain variables as well.

5 You can double click a sentence to test it, or select it and press **Test.** When your phone rings, pick it up and listen to the sentence in the language you selected. You can continue to play messages, and even change languages, without hanging up your phone.

6 If the sentence contains variables, they are indicated in the **Name** column with an asterisk. You can enter a new **Value** for a variable, and optionally select a different variable **Data Type**.

For example, by default the sentence ToPurgeMsg sentence plays as:

> "To permanently delete the 1 message in your ViewPoint's Deleted folder, press 3. Otherwise, press 4."

By changing the **Value** of Variable 1 to 6, the sentence plays as:

> "To permanently delete the 6 messages in your ViewPoint's Deleted folder, press 3. Otherwise, press 4."

Click **Clear** to return all **Values** to their original settings.

Localizing the telephone commands

The Wave Localization Kit is available if you want to localize and record the telephone commands in another language. The Localization Kit includes all the necessary documentation and tools for localization.

Although the process for recording system prompts is the same for localized system prompts, the localization process requires several more steps, which are described in the Localization Kit.

For more about the Wave Localization Kit, contact your Wave provider.

Changing the offhook alert audio

When a Wave station is left offhook for too long, it plays the prompt "Please hang up and try your call again," followed by a loud reorder tone for two minutes, similar to the tone played by telephone companies. To change the offhook audio, change the following files:

- **HangUp.WAV.** The verbal prompt.
- **OffhookAlert.** The reorder tone.

Recording All Wave Calls

CHAPTER CONTENTS

About recording calls

You can have Wave automatically record all calls handled by the system, while exempting the individuals, roles, or queues of your choice. For example, you could record all calls except for those belonging to users in the Administrators role. You can also exempt internal (station-to-station) calls.

Note: Users can also record their own calls manually (see *Vertical Wave User's Guide*), and you can configure call center queues to automatically record calls (see the *Vertical Wave Contact Center Administrator's Guide*).

System call recordings are stored in a voice mailbox of your choice. You can manage them exactly as you would manage voice messages. For instructions on playing and managing voice messages using the phone or ViewPoint, or managing archived recordings using the Wave Archived Recording Browser, see Appendix E of *Vertical Wave User's Guide*.

Caution: *If you record all calls or even a significant portion of calls, or if you have users with thousands of saved voice messages and large maximum mailbox sizes, disk space on the Wave ISM can quickly fill up with voice messages and call recordings. In addition, ViewPoint performance will significantly degrade while a user searches for*

and acts on thousands of recordings, or when recordings are being delivered to the user in quick succession. See "Offloading call recording voice files from your Wave ISM" on page 20-3 for how to manage many recordings properly.

What parts of the call are recorded

Call recordings include only calls with two or more parties, and only the portion of the call from time the parties are connected to the end of the call. The following parts of a call are not recorded:

- hold music
- auto attendant messages
- voicemail greetings
- voicemail messages
- telephone commands or prompts
- IVR Plug-in prompts
- consultation calls during supervised transfers

When a call is transferred, the various conversations are included in a single call recording.

Exempting queue calls

Call centers usually comprise a large portion of a system's total phone traffic. If your site uses Wave call center queues, it is recommended that you exempt your queues from system call recording, and use the queue's own recording features to record queue calls (see the *Vertical Wave Contact Center Administrator's Guide*). Otherwise, a needless duplication of recordings can result.

Privacy

Some states require that you announce to callers that their calls may be recorded. Wave includes a system prompt, MayBeMonitored.vox, that says, "Your call may be monitored or recorded," which you can play as needed (for example, by using an auto attendant or call center queue greeting). In addition, Wave allows you to play a regular

"reminder beep" while recording calls which alerts users and callers that their calls are being recorded (see "Including a beep on call recordings" on page 20-7). It is the license-holder's responsibility to comply with any Federal or other applicable statutes regarding the recording of phone calls. Vertical Communications, Inc. disclaims any responsibility for failing to comply with such regulations.

Preparing to record all calls

Recording all Wave calls can use significant amounts of disk space and can consume many voice resources. Including regular reminder beeps on recorded calls also requires additional conference resources. Before beginning to record calls, you should plan for how to store the resulting voice files and manage the demand for voice and conference resources. See "Call recordings and voice resources" on page 20-5 for information on managing voice resources for call recording needs.

Offloading call recording voice files from your Wave ISM

Each minute of call recording consumes .46 MB of disk space. If you store all call recordings on the Wave ISM computer, it can rapidly consume your available hard disk space and interfere with phone system performance and users' ability to receive voice messages. Therefore, it is highly recommended that you automatically offload call recordings from the Wave ISM computer. The following are two ways to do so.

Automatically archiving recordings

The recommended approach to archiving is to have Wave automatically archive all recordings of a certain age. You can choose which users are subject to automatic archiving and you can specify the network location of your choice for archive files. Users with permission can then search, manage and listen to the archived recordings using the Wave Archived Recording Browser. See "Archiving call recordings and voice mail" on page 23-34. Recordings are archived in .VOX, .WAV or .MP3 format with detailed Call Log information about the call.

Moving recordings to any e-mail address

As an alternative to automatic archiving, you can use Wave e-mail notification to automatically move call recordings to any e-mail address. To do so:

1. Create a placeholder user (named, for example, “Recorded Calls”) to whom you send all call recordings. For instructions on creating a user, see “About users” on page 11-2.
2. Set up e-mail notification for the user with the following selections:
   - **Send e-mail for all messages**
   - **Attach voice message and delete from Inbox**

   For instructions on setting up e-mail notification, see “Setting e-mail notification” on page 11-22.

With these settings, the call recording files are moved to your e-mail server in the form of e-mail attachments, with detailed Call Log information, and are deleted from the Wave ISM computer as soon as they arrive, so that no extra disk space is consumed.

When you offload call recording files via e-mail notification, you will have a large number of e-mails in the e-mail account to which they are sent—one e-mail for each recorded call. Wave automatically puts information about the call into the e-mail’s subject and body, so that you can use your e-mail program’s Search capability to find a particular call recording. The e-mail’s subject holds information in the following format:

SysRec: TrunkX / NAME->Station Y / User Y

where `->` indicates the direction of the call, `Trunk X` indicates the trunk number involved and the Caller ID name (where available), `Station Y` indicates the station ID of the station involved, and `User Y` indicates the extension of the user involved.

The e-mail body also includes the following Call Log information that further describes what was recorded (example data used):

```
Notes:
Trunk 1/ Unknown -> Station 2/ Queue 500

CustomData:
CustProp1=Value of Custom Property 1;CustProp2=Value of Custom
Property 2;

--- Call Recording Details ---
Direction: Inbound
From: Unknown
To: Queue 500
Answered By: User 2
From Number: 6172344500
To Number: 500
From Code: <None>
```

```
To Code: <None>
From Device: Trunk 1
To Device: Station 2
Duration: 01:07
Start Time: 8/31/2005 11:17:55
Stop Time: 8/31/2005 11:19:02
Wait Time: 00:07
Parties: 2
Caller ID Name: <None>
Organization: <None>
Call Log ID: 04010000002119

Wave Code:1207:1010:1
```

Storing call recordings on the Wave ISM

If you decide to store call recordings on the Wave ISM instead of offloading them, you should choose the amount of disk space that you want to devote to storing call recording files. Even if you configure Wave to automatically archive call recordings daily you still need enough disk space to hold 24 hours of recordings before they are archived. When this space is filled, you can have Wave automatically make room for the newest call recordings by deleting the oldest. To set this up:

1. Limit the size of the placeholder user's voice mailbox to the amount of disk space you want to devote to call recordings. Use the formula 1 minute = .46MB. For example, to devote 1 GB to call recordings, set the user's voice mailbox to 2185 minutes. See "Configuring the user's voice mailbox" on page 11-18.
2. Configure system call recording to automatically delete the oldest call recording when the mailbox is full. See "Recording all calls" on page 20-6.

Call recordings and voice resources

Call recording involves one additional voice resource for each call being recorded. For example, if your system has 5 trunk calls and 8 internal calls occurring at the moment, 13 extra voice resources are required to allow for call recording. Including a reminder beep on call recordings also uses one voice resource shared across all calls.

Note: Wave does not use dedicated trunk voice resources for system call recording.

Before beginning to record all calls, you should make sure that your hardware configuration includes enough voice resources to meet the increased demand. For a more in-depth discussion of voice resource usage, see *Installing Intel Telephony Components*.

Call recordings beeps and conference resources

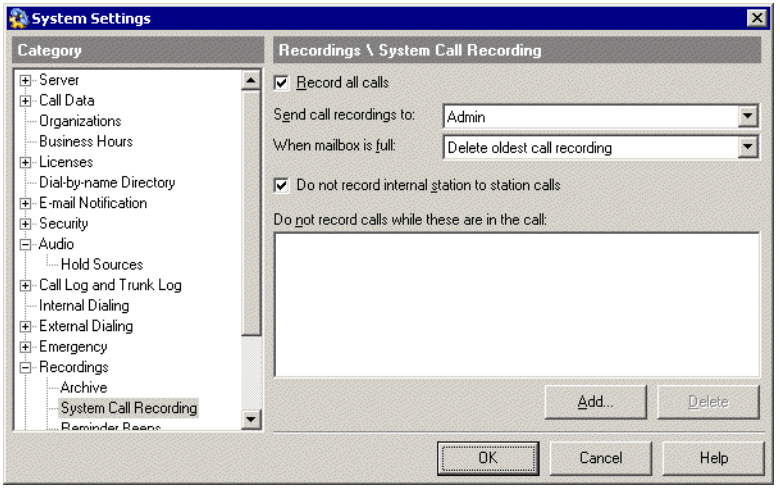
Adding reminder beeps to a two-party call requires three conference resources: one for each party, and one for the reminder beep. This can significantly increase conference resource usage.

Recording all calls

Use the following procedure to set up the automatic recording of all Wave calls, and specify exemptions for calls that you do not want to record:

1 Choose **Tools > System Settings**. The System Settings dialog box opens.

2 Choose the Recordings \ System Call Recording tab.



3 Check **Record all calls** to have Wave automatically record system calls according to the settings you make here. If unchecked, Wave does not record system calls.

4 From the **Send call recordings to** dropdown list, select the voice mailbox to which system call recordings are sent.

5 From the **When mailbox is full** dropdown list, choose one of the following options:

- **Discard new call recording.** Wave deletes the new call recording instead of storing it. Selecting this will cause call recordings to stop when the mailbox is full.
- **Delete oldest call recording.** Wave deletes the oldest call recording in the mailbox to make room for the new recording. Only call recordings can be deleted by this method. Wave never deletes voice messages in this way.

6 To exempt internal calls, so that only calls involving a trunk are recorded, check **Do not record internal station to station calls**. If unchecked, both internal calls and calls involving a trunk are recorded.

7 Use the **Do not record calls while these are in the call** list to exempt users or roles from system call recording. You can exempt any of the following entities:

- **Users.** The system does not record any call while an exempted user is a participant.

  If an exempted user joins a conference call that is being recorded, the recording pauses as long as the exempted user is in the call. If the exempted user leaves the conference, the recording resumes.
- **Roles.** The system does not record any call while a member of the role is a participant.
- **Queues.** The system does not record any queue call.

  When a queue call is transferred to a user who is not an agent in the queue, it ceases being a queue call and recording of it begins.

To exempt a user, role, or queue from system call recording, click **Add**. Make your selection in the System Call Recording Exclusion dialog box and click **OK**.

8 When you are finished adding exemptions, click **OK**.

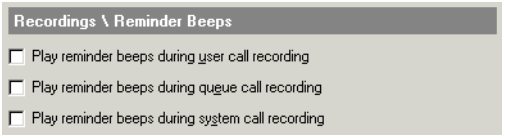
Including a beep on call recordings

You can include a regular “reminder” beep on Wave call recordings. If enabled, the reminder beep is heard by all parties in the call and is included in the recording. You can enable or disable recording beeps for each type of Wave call recording.

To include a reminder beep:

1 Choose **Tools > System Settings**. The System Settings dialog box opens.

2 Choose the Recordings \ Reminder Beeps tab.



3 Check the appropriate box to include a beep with each type of recorded call as follows:

- **User call recording.** Call recordings made manually by users using the *16 telephone command or ViewPoint's Call Monitor commands.
- **Queue call recording.** Automatic call recordings set up in a call center queue. These include queue call recordings and agent call recordings.
- **System call recording**. Call recordings set up in System Settings, Recordings \ System Call Recording tab, as described in this chapter.

4 Click **OK**.

Archiving call recordings

To save space on the ISM and improve ViewPoint performance, you can archive call recordings to a location of your choice, and access them using the Wave Archived Recording Browser. See "Archiving call recordings and voice mail" on page 23-34.

Tracking and Distinguishing Calls

CHAPTER CONTENTS

About tracking and distinguishing calls

Wave provides several ways to track groups of similar calls for purposes of record-keeping, billing, or automated call handling. The most basic way to track related calls is by sorting the Call Log (see "Using the Call Log view" on page 23-5), and by running reports using the Wave Call Center Reporter (see the *Vertical Wave Contact Center Administrator's Guide*). This chapter describes the following more advanced methods of tracking and distinguishing calls:

- **Using Organizations.** Organizations enable two or more separate businesses or contractors share a Wave ISM and trunks, yet be independent of each other in terms of caller experience and internal billing. See the next section.
- **Using account codes.** With user-entered account codes you can distinguish any group of calls for reporting and accounting purposes. For example, if your office contains employees or contractors whom you bill separately for their phone use, you can use account codes to mark calls by the user they belong to. Other uses of account codes include marketing campaigns, case and issue tracking, and more. See page 6
- **Defining custom data variables.** Custom data variables enable you to attach any information to incoming calls, for example, the name of the product that the caller is calling about. Users can view custom data variables in their Call Monitors, and you can set up automatic call handling based on custom data values. You can also report on calls involving custom data variables. See page 14.

Using Organizations

With Organizations, two or more separate businesses or other groups can share a Wave ISM, yet remain independent. Callers dialing a user in one Organization would never know that other businesses exist there, and internal billing can be kept strictly separate.

Once you define one or more Organizations, and assign each user to the appropriate Organization, you can do the following:

- Log calls by Organization for purposes of tracking or billing.
- Restrict callers at the auto attendant to dialing only the extensions of users in the Organization they're calling.
- Distribute outbound trunk use between Organizations.

This section covers the following aspects of using Organizations:

Defining an Organization

To use Organizations, you must first define them.

1. In the User / Workgroup Management applet, choose **Tools > System Settings**. The System Settings dialog box opens.
2. Choose the Organizations tab, which lists the Organizations you have defined so far.

   To edit or delete an existing Organization, click the Organization, then click **Edit** or **Delete**.

3 To add a new Organization, click **Add**. The Organization dialog box opens.

4 Enter the name of the Organization, for example, the name of the company that is sharing the Wave ISM.

5 Click **OK** to return to the Organizations dialog box.

6 When you are done adding Organizations, click **OK** to close the System Settings dialog box.

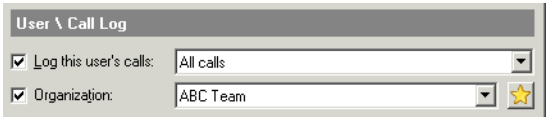
Assigning users to Organizations

Once you have defined Organizations, you can mark calls by which Organization they belong to. You can view a call's Organization using the Organization column in the Call Log, and Wave reports, and easily sort by Organization for tracking or accounting purposes. You can also display a call's Organization in ViewPoint's Call Monitor.

Note: Users in different Organizations cannot have identical extensions. Every Wave user must still have a unique extension.

To assign a user to an Organization:

1 In the User / Workgroup Management applet, double-click the user in the Users view to open the User dialog box, and choose the User \ Call Log tab.



2 Check **Organization**, and select the Organization to which the user should belong. Click  to create a new Organization. See "Defining an Organization" on page 21-2.

3 Click **OK**.

See Chapter 11 for complete information about setting up a user's account.

How calls are logged by Organization

The Organization column in the Call Log displays the Organization for each call that is associated with one. Outbound calls are logged with the Organization of the user who placed the call. Inbound calls are logged with the Organization of the user who answered the call (the user who appears in the Call Log's **Answered By** field.

Note: If a call center queue agent places calls as the queue, the call is still logged with the Organization of the agent, not the Organization of the queue.

Conference calls are logged with the Organization of the user who started the conference call.

Creating an auto attendant for each Organization

Assuming that each Organization has its own phone number, you can define a separate auto attendant for each Organization. Callers will then hear a greeting and menu choices specific to the Organization they're calling, and they will be unable to accidentally dial users in other Organizations, either by extension or dial-by-name.

To create an auto attendant for an Organization:

1. Create a public workgroup containing the same users that are the members of the Organization. For instructions see "Creating a Workgroup" on page 12-3.
2. Define an auto attendant as described in "Configuring an auto attendant" on page 13-2. Check **Restrict dial-by-name and extension matching to members of** on the Menu Choices tab, and select the workgroup.
3. Route the trunk(s) corresponding to the Organization's phone number to the auto attendant. Alternately, edit the auto attendant to give it the appropriate DID number. See "Creating a new auto attendant" on page 13-3.

Configuring Operators for multiple Organizations

At several places in the Wave system, callers can press 0 to transfer to an Operator. With multiple Organizations, you might want to have a different Operator for each Organization. To set up multiple Operators and make sure that callers reach the right Operator for the Organization they are calling, do the following:

1. Decide which extensions will be the Operators for the different Organizations. For example, 101 for Company ABC, and 102 for company YYZ. These examples are used in the following steps.

2. Edit each user. On the User \ Details tab use the **Operator** field to select the Operator extension appropriate to the user's Organization. For example, if a user belongs to Organization ABC, select extension 101. This ensures that callers pressing 0 while leaving a user voicemail are handled correctly.

   For full instructions, see "The User \ Details tab" on page 11-13.

3. If you have restricted one or more auto attendants by workgroup (see "Creating an auto attendant for each Organization" on page 21-4), edit each workgroup specified by an auto attendant. On the Dialing tab under **If no answer, transfer**, select the Operator extension appropriate to the Organization. For example, if the workgroup holds the members of Organization YYZ, select extension 102. This ensures that callers pressing 0 at an auto attendant are handled correctly.

   For full instructions, see "When no one answers a call to a workgroup" on page 12-6.

4. If you are using Wave call center queues, edit each queue. On the General tab under **Operator**, select the extension appropriate to the queue's Organization. For example, if the queue belongs to Organization ABC, select extension 101. This ensures that callers pressing 0 while leaving the queue voicemail are handled correctly.

   See the *Vertical Wave Contact Center Administrator's Guide* for complete information on creating and using a call center.

5. You can set up the default Operator at extension 0 to automatically transfer calls to the correct custom Operator based on who is calling. To do so, you must have created a workgroup for each Organization, containing all the users in that Organization. Edit the default Operator in ViewPoint. For each Organization, create a call rule that activates for that Organization's workgroup, and sends calls to the appropriate custom routing list. For each Organization, define a custom routing list to have no steps, only a final action that transfers the call to that Organization's custom Operator. For example, the call rule that activates for workgroup ABC would send calls to a routing list that transfers them to extension 101.

   See *Vertical Wave User's Guide* for instructions on creating call rules and routing lists.

Using account codes

Wave allows you to track your phone traffic by either forcing or optionally allowing users to enter an account code for each call. Account codes can represent any aspect of your phone traffic—customer number, product line, department, and so forth—that you want to track. You can define the available account codes and tell your users the codes that they should or must enter under specific circumstances.

Some of the ways you can use account codes are as follows:

- **For billing clients.** With account codes you can track calls to various customers whom you bill for the phone time you spend with them. You can associate account codes with contacts for automatic customer tracking.
- **For internal accounting.** If phone bills are a significant part of your company's expenses, you can use account codes to perform detailed expense analyses. For example, you can track phone use by department.
- **For marketing campaigns.** By setting up an account code for the campaign and having agents use it whenever they place or receive campaign calls, you can track the time, resources, and results of the campaign.

Account code information appears in the Call Log (see "Using the Call Log view" on page 23-5), and you can generate reports using the Wave Call Center Reporter that show calls by account code. For information about the Call Center Reporter, see *Vertical Wave Contact Center Administrator's Guide*.

Example: Your office is working on the Gould case and the Avellanos case. You give the Gould case an account code of 88 and the Avellanos case an account code of 55. Whenever users place or receive calls relating to the Gould case, they enter 88. Whenever they place or receive calls relating to the Avellanos case, they enter 55. You can then run a report that sorts calls by account code and see the phone traffic for the Gould and Avellanos cases separately. You can also run a report that sorts by user, so that you can see how much phone time a specific user spent on each case.

Account code modes

On a per-user basis, you can set account code entry to be voluntary or required. You can also choose to have the system verify account codes against a list of valid account codes.

The following account code modes are available:

- **Optional non-verified.** The user is not prompted to enter account codes, but can enter one if desired. If the user does enter an account code, it is not checked against the list of valid account codes.
- **Optional verified.** The user is not prompted to enter account codes. If the user does enter an account code, it is checked against the list of valid account codes. If the account code is invalid, the user is prompted to enter it again.
- **Forced non-verified.** The user is required and prompted to enter an account code when placing an external call. The account code is not checked against the list of valid account codes. This option is not available for inbound or internal calls.
- **Forced verified.** The user is required and prompted to enter an account code when placing an external call, and the account code is checked against the list of valid account codes. If the account code is invalid, the user is prompted to enter it again in order to make an external call. This option is not available for inbound or internal calls.

Setting general account code options

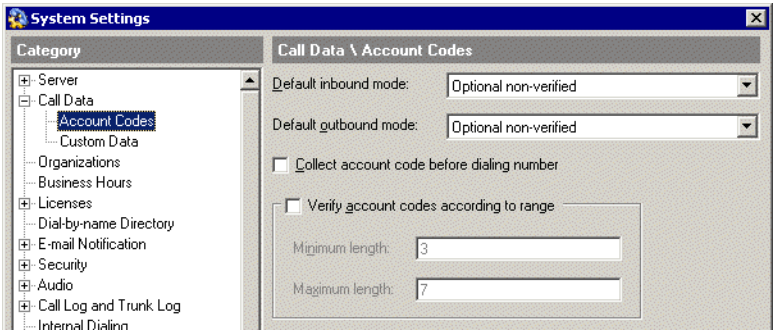
Before setting up account code modes for individual users, you should configure the system-wide account code options as follows:

1 From the Management Console, click the icon for **User/Workgroup Management**, located in the PBX Administration section. The User / Workgroup Management

applet opens. See “Using the User / Workgroup Management applet” on page 2-9 for information about navigating in the User / Workgroup Management applet.

2 Choose **Tools > System Settings**. The System Settings dialog box opens.

3 Choose the Call Data \ Account Codes tab.



4 Under **Default inbound mode** and **Default outbound mode**, choose the account code modes that you want to be active at stations to which a user has not been assigned. For an explanation of the modes, see "Account code modes" on page 21-6.

5 Check **Collect account code before dialing number** to prompt users for an account code immediately after they dial a dialing service access code (for example, 9). Uncheck the box to prompt users for an account code after they have finished dialing the entire phone number.

6 Check **Verify account code according to range** to have the system verify account codes by length. If an account code contains too many digits or too few digits, users are prompted to enter it again. Under **Minimum length** and **Maximum length**, specify the acceptable range for account code length. For example, if account codes in your system can be two, three, or four digits, enter a **Minimum length** of 2 and a **Maximum length** of 4.

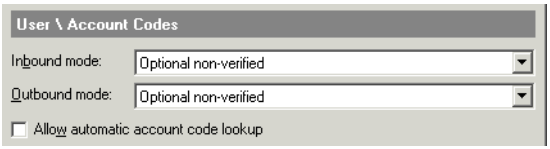
Note: It is more efficient to set **Minimum length** and **Maximum length** to the same number and use account codes that are all the same length. When set up this way, the system immediately recognizes when users finish entering an account code, so they do not need to press # at the end of the account code. When account codes are of variable length, users must press # to end the account code or there will be a slight pause while the system waits for more digits.

If **Minimum length** and **Maximum length** are both set to 0, account codes will not be verified by length.

7 Click **OK**.

Setting a user's account code modes

For each user, you can define whether account code entry is voluntary or forced, and whether the system verifies entered account codes against a list of valid account codes.



To set a user's account code modes:

1 From the Management Console, click the icon for **User/Workgroup Management**, located in the PBX Administration section. The User / Workgroup Management

applet opens. See "Using the User / Workgroup Management applet" on page 2-9 for information about navigating in the User / Workgroup Management applet.

2 Double-click a user in the Users view. The User dialog box opens. You can also set account code modes when you create a new user.

3 Click the User \ Account Codes tab.

4 Use the **Inbound mode** and **Outbound mode** dropdown lists to select the user's account code modes for inbound and outbound calls. See "Account code modes" on page 21-6.

5 Check **Allow automatic account code lookup** to enable automatic association of account codes with contacts for this user. If enabled, the user can enter an account code for each contact, and the system automatically applies the account code to calls to and from the contact. See *Vertical Wave User's Guide* for more information about using contacts.

6 Click **OK**.

For complete instructions on defining a user, see Chapter 11.

How users enter account codes

You should tell users what account codes to enter in which circumstances, and how they will be expected to enter them. Users can enter account codes for calls in the following ways:

- **When prompted by the system while placing an outbound call.** Only users forced to enter account codes encounter this prompt. Exactly where the prompt occurs in the dialing sequence depends on whether you checked **Collect account code before dialing number** (see "Setting general account code options" on page 21-7).

  By default the account code prompt is a beep. To change it, see "Using a verbal account code prompt" on page 21-13.

- **Automatically when placing a call to a contact.** When a user places a call from ViewPoint to a contact with an associated account code, the account code is automatically entered for the call. You can enter account codes for public contacts, and users can enter them for private contacts. For more about contacts, see Chapter 16 of *Vertical Wave User's Guide*.

- **During a call.** On an inbound or outbound call, users can press **Flash** to put a caller on hold, then ***11** to enter an account code for the current call. In ViewPoint, they can right-click the call in the Call Monitor and choose **Enter account code** from the shortcut menu. Users can use this command as many times as they want during a call to change or correct the account code. The last account code entered is the one that is used for the call.

- **Before dialing a call.** A user can press ***11** before dialing a call to enter an account code for that call. The user picks up the phone and dials ***11 <account code> <access code> <phone number>**. In the following example, spaces are shown for clarity:

  *11 8877 9 212 123 4567

  In this example, 8877 is the account code and 9 is the access code.

  In ViewPoint, users can enter an account code before placing a call by using the Place Call To dialog box (or the **Dial** field in any view). To do so, they type the phone number, then a vertical bar (|), then the account code.

- **After a call has finished.** In ViewPoint, a user can enter an account code for a completed call by selecting the call in the Call Log and choosing **Actions > Enter account code**. The user must have the permission **Access Call Log folder** set to "View and Edit" (see "Wave permissions" on page 11-49).

Indicating the end of an account code

When users use the phone to specify account codes, Wave detects the end of an account code when any of the following occurs:

- The account code reaches the maximum number of digits. To define the maximum number of digits, see “Setting general account code options” on page 21-7.
- The user presses #.
- Three seconds elapse after the user entered a digit. The system uses the digits already entered as the account code that the user intended to enter.

If a user does not enter an account code before 5 seconds have elapsed after the beep, the system beeps again to prompt the user to enter the account code.

Note: If you have a high maximum number of digits and your account codes can be of variable lengths, you should encourage users to press # when they reach the end of an account code.

Users can cancel an account code entry while they are entering it by pressing *.

Creating a valid account code list

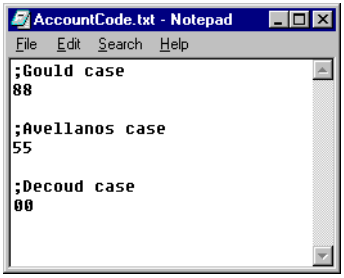
If you want to use verified account codes for some or all users, you must create a text file that lists your valid account codes. The text file must be called `Accountcode.txt` and reside in the `\Accountcode` directory on the Wave ISM computer. By default, the complete path is:

```
C:\Program Files\Wave Server\Accountcode\Accountcode.txt
```

When a user whose account code mode is set to “Verified” enters an account code, Wave checks the account code against the contents of the text file. If the account code is not listed in the text file, Wave prompts the user to enter it again.

Formatting the text file

Type each account code as a separate line in the text file. Blank lines are permitted and are ignored by the system. If you want to add a comment line that is ignored by the system, begin the line with a semicolon (;).



Account codes can contain numbers, letters, and other characters. However, users must use ViewPoint to enter characters other than numbers. If your users will be entering account codes via the phone, use numeric-only account codes.

You can also use the wild card characters ? and % (see the next section).

Note: Account codes in the text file must meet your account code length requirements or they will not be added to the list of valid account codes. For example, if your account codes must be between 2 and 4 digits, a 5-digit account code will be rejected even if it appears in the text file. See “Setting general account code options” on page 21-7 for instructions on setting account code length requirements.

Using wild card characters

You can use the wild card characters ? and % when you enter valid account codes in the text file:

- **Question mark (?).** Indicates any single digit. For example, an account code entry of 12? would make 123, 124, and 129 all valid account codes. In this case, however, neither 12 nor 1233 would be valid account codes.
- **Percent sign (%).** Indicates any number of digits, including none. For example, an account code entry of 12% would make 12, 123, 1233, and 12789213120 all valid account codes.

If you use either of these wild card characters in an account code, it must be the final character in an account code, and if you use both of these wild card characters in the same account code, the % character must be the final character.

Valid	Invalid
12?	1?2
12??	1%2
12%	?12
12?%	%12
12?????%	12%?

Note: Account codes that are identical except for wild card characters conflict with each other. For example, 1234 conflicts with 1234? and 1234%. In the case of conflicting entries, only the first entry is used to verify account codes.

Using a verbal account code prompt

By default, the account code prompt is a single beep. You should explain to your users that they must enter an account code when they hear the beep. Wave provides an alternate account code sound file, with a verbal prompt that says, "Please enter an account code."

To use the verbal account code prompt instead of the beep:

1. Find the file `AccountCodePrompt.vox` in the user directory. This file contains the beep. By default the path is `C:\Program Files\TeleVantage Server\Vfiles\User\AccountCodePrompt.vox`.
2. Rename the file, for example, to `AccountCodePrompt.vox.beep`.

Users now hear the verbal prompt instead of the beep when they are prompted to enter an account code.

Note: By renaming the beep file, Wave automatically uses another AccountCodePrompt.vox file, which is found in your language directory and which contains the verbal prompt. The default path for the English language verbal prompt file is the following. It (or any other language version of this file) can be rerecorded using the System Prompts view.

```
C:\Program Files\TeleVantage Server\Vfiles\EN00\AccountCodePrompt.vox
```

Viewing account codes in the Call Log or Call Monitor

The Call Log view contains an Account Code column that shows the account code associated with each call. If the Account Code column is blank, no account code was entered for the call. Click the Account Code column header to sort the Call Log by account code. For more information, see "Using the Call Log view" on page 23-5.

Note: In the Call Log you can you can change a call's account code or enter a new one. Select the call and choose **Call Log > Enter Account Code**. You must have the permission **Access Call Log folder** set to "View and Edit" (see "Wave permissions" on page 11-49).

ViewPoint's Call Monitor view also contains an Account Code column, but it is hidden by default. In the Call Monitor view, choose **View > Current View > Show Columns** to display it.

Generating account code reports

For information about generating reports that show account code usage, see the *Vertical Wave Contact Center Administrator's Guide*.

You can also export the Call Log, with its account code information, to a .CSV file that you can view in spreadsheet applications. See "Exporting the Call Log" on page 23-11.

Defining custom data variables

Wave lets you attach extra information to incoming calls, using *custom data variables*. The information is displayed to users in ViewPoint's Call Monitor, and can also be used to automate call handling. Examples of attaching extra information to calls using custom data variables include the following:

- Based on the caller's auto attendant choice, set a variable called Product to the name of the product that the caller is calling about. For example, callers who press 1 have Product="Widget," while callers who press 2 have Product="Advanced Widget." When users answer the calls they see the product name in the Call Monitor in a column labeled "Product."
- Based on contact recognition, set a variable called Priority to a higher number for VIP callers to a call center queue. For example, a normal caller has Priority=1, while a VIP caller has Priority=10. VIP callers are automatically bumped closer to the head of the queue.

Note: Custom data variables are case sensitive.

Using custom data variables is a two-step process, as follows:

1 Defining a custom data variable.

2 Setting the value for a custom data variable.

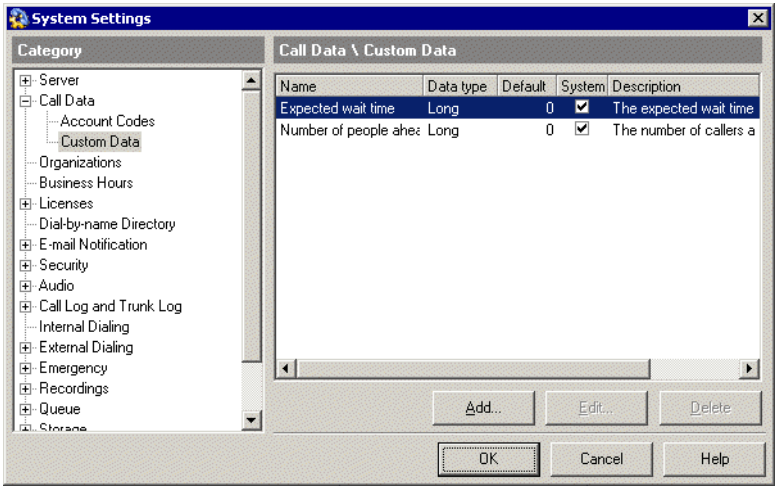
These steps are described in the following sections.

Defining a custom data variable

You can define as many custom data variables as you want.

1 Choose **Tools > System Settings**. The System Settings dialog box opens.

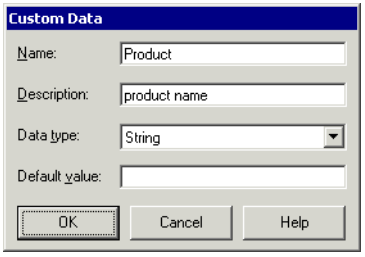
2 Choose the Call Data \ Custom Data tab, which lists the custom data variables created so far.



Each custom data variable is attached to every incoming call, though a given variable might not be used for every call.

Note: If you have purchased the Wave Call Center module, two system variables are present by default, Expected wait time and Number of people ahead. For instructions on using them, see the *Vertical Wave Contact Center Administrator's Guide*.

1 To create a new custom data variable, click **Add**. The Custom Data dialog box opens.



2 Enter the following information for the custom data variable:

- **Name.** Enter a name for the variable. Keep the name relatively short, as it will appear in a column header in ViewPoint's Call Monitor. Custom data variable names are case sensitive.
- **Description.** Enter a description of the variable if needed.
- **Data Type.** This determines the type of information that the variable holds. Select one of the following:
  - **Long.** An integer number.
  - **Double.** A number that have decimal places.
  - **Boolean.** The value must be either 0 or 1.
  - **String.** Text. Numbers can be part of the text string, but they are treated as text characters.
- **Default value.** Enter the value that the variable receives if no other action sets a value. For string variables you can leave the field blank, meaning the variable is empty by default. For numeric variables you must enter a number, usually 0.

3 Click **OK** to add the custom data variable to the list.

4 Click **OK** to close the System Settings dialog box.

The variable you created is now available to be attached to any incoming call (for example, by an auto attendant or call center queue). Users have a corresponding column in the Call Monitor where they can view the variable's value for each call.

Setting the value for a custom data variable

You can have Wave set the value of a custom data variable in the following ways:

- **Auto attendant choice.** When defining an auto attendant menu choice, you can have it set the value of one or more custom data variables. See "Defining menu choices" on page 13-4.
- **Call center queue.** If you purchased the Wave Call Center module, you can have a queue set the value of a custom data variable based on caller data entry. See the *Vertical Wave Contact Center Administrator's Guide*.
- **IVR Plug-in.** An IVR Plug-in can set the value of custom data variables based on a variety of methods, including when it was called and caller data entry. For more information see Appendix G of *Vertical Wave Installation Guide*.

- **Wave Call Classifier.** The Wave Call Classifier can set custom data variables based on database queries, Caller ID name or number, DID, account codes, or other custom variables.

Advanced Data Networking Configuration

CHAPTER CONTENTS

Configuring advanced connection protocol settings

Caution: *Do not modify these settings unless you are a Vertical Wave configuration expert.*

Configuring dial-up routing

When configuring dial-up routing, you will typically configure the parameters only once, when you install and configure Vertical Wave the first time. If you change ISP providers or access numbers, you may need to modify these settings.

Configuring dial-up routing requires you to configure demand-dial interfaces. To configure demand-dial interfaces, you must create an entry for *each* remote location (ISP, headquarters, another sales office) to which you want to dial out. The RRAS administrator stores the settings needed to connect to a particular remote router or network in a "phone book entry." Once an interface is configured in RRAS, it acts like any server.

Note: When configuring an internal modem for dial-out routing, you cannot configure the modem to dial digits following the connection of the call. For example, you cannot configure an internal modem to dial a number, delay, and then dial more digits.

After initial configuration, you will only need to modify these settings if you add remote locations or change phone access numbers.

Typically, you configure dial-up routing for both dial-in and dial-out capabilities. You can configure for only one or the other, and if you do, how you define dial-out properties depends on several things. Various possibilities are described in Table 22-1.

Table 22-1 Dial-out options

Modem Port Usage	Enables	Wave Variables
Dial out as RAS client	The Wave ISM behaving as a dial-up client, calling a server / router. A WAN device will be used for outbound dial-on-demand connections.	This is typically used only for debugging or testing Wave connections, because it creates a client-to-server connection, where Wave is the client—instead of a network-to-network connection.
Receive calls as RAS server	Outside clients (non-network-connected users) calling into Wave. WAN devices will be used for inbound dial-on-demand connections.	If you have a T-1 data line to the Internet, you could select this option for one WAN device to provide remote access for employees.
Dial out and receive calls as a demand-dial router	The Wave ISM calling an ISP (a network-to-network connection from one router to another). WAN devices will be used for inbound and outbound dial-on-demand connections.	If you have a T-1 data line to the Internet, you could select this option for any WAN device.

Caution: *When connecting two Wave ISMs together using ISDN, set the network side of the connection to the linear hunt type and the user side to the reverse linear hunt type. For more information about GLARE, see "Minimizing GLARE" on page 26-7.*

Configuring network services and routing protocols

The following sections describe how to configure network services and routing protocols on the Wave ISM.

Configuring network routing protocols

Note: By default, these routing protocols are installed but not configured, as they are not required for typical configurations. If you need to configure these, see "Configuring network routing protocols" on page 22-2.

- Configuring routing information protocol (RIP)

- Configuring the open shortest path first (OSPF) routing protocol
- Configuring and enabling IPX

Configuring routing information protocol (RIP)

Hint: If you are using RIP with multiple connection lines and want line speed taken into account during routing, modify routing protocol metrics accordingly when configuring an interface or when adding a static route.

Note: Unlike making network settings changes, when using RRAS, your changes will take effect immediately; the Wave ISM will not restart.

To configure RIP:

Click 

1 Open the Microsoft RRAS applet under Data Administration on the General Administration tab of the Management Console. Log on using your Wave username and password. The Routing and Remote Access dialog box opens.

For more information about logging in with a remote connection, see “Remote Access Application applets” on page 2-5.

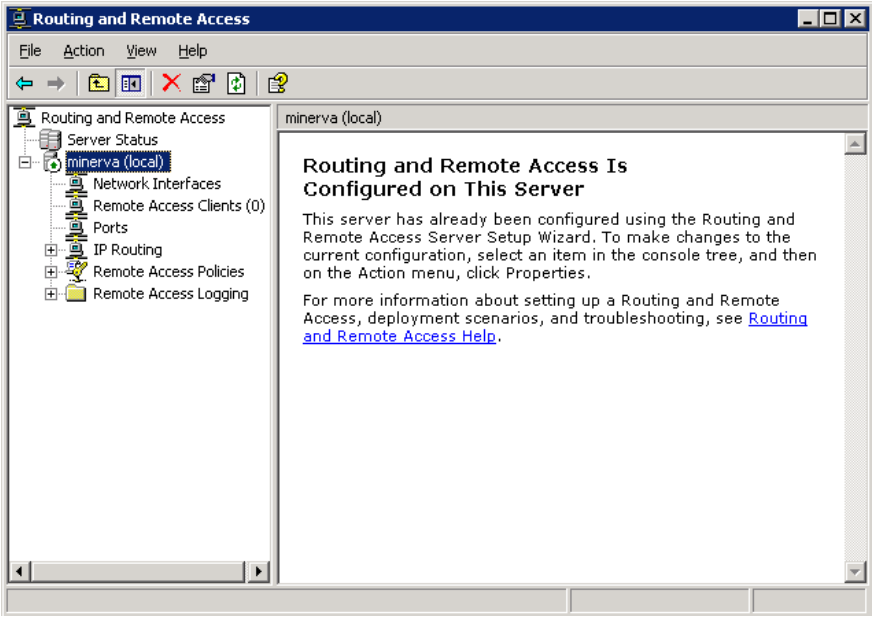


Figure 22-1 Microsoft RRAS administration tool

2 Add the RIP protocol.

Right-click the General folder under IP Routing, and choose **New Routing Protocol**. In the New Routing Protocol dialog box, click "RIP Version 2 for Internet Protocol" and click **OK**.

3 Select each interface on which you want to enable the routing protocol.

Right-click RIP in the IP Routing folder and select **New Interface**. Select the desired interface, then click **OK**. Configure the Internet properties for that interface on the dialog box that opens, then click **OK**.

4 Close the Routing and Remote Access dialog box to return to the Management Console.

Note: If you are routing across a WAN, be sure to configure the WAN interface on the Integrated Services Card with RIP. Auto-static, static, and default routing can be used with demand-dial interfaces. Auto-static makes static routing table entries, and is used only for demand-dial connections, and only with other Wave ISMs or with a remote Microsoft Windows server acting as a router. Periodic polling will keep a line up all the time, and should be used only with persistent connections.

Configuring the open shortest path first (OSPF) routing protocol

To configure OSPF:

Click 

1 Open the Microsoft RRAS applet under Data Administration on the General Administration tab of the Management Console. Log on using your Wave username and password. The Routing and Remote Access dialog box opens.

For more information about logging in with a remote connection, see “Remote Access Application applets” on page 2-5.

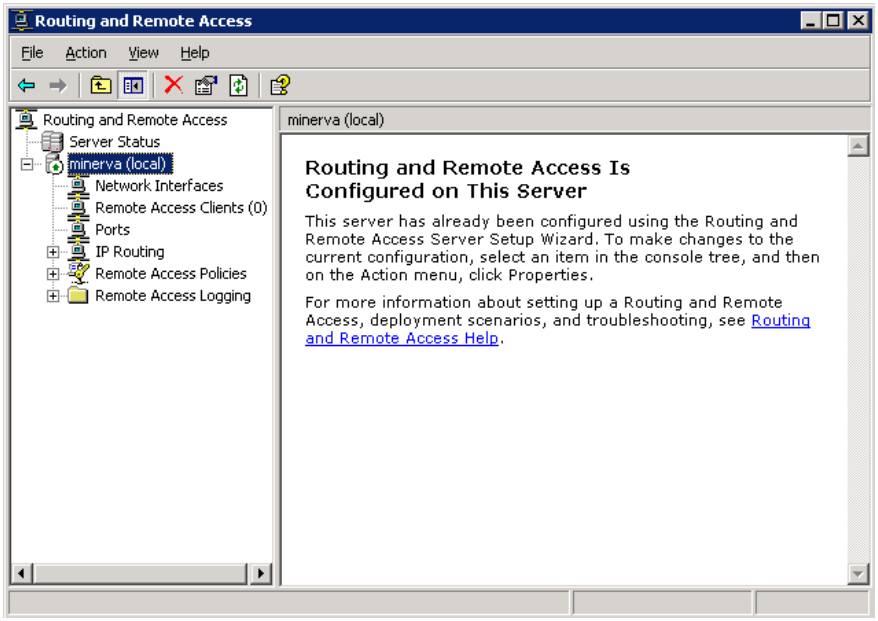


Figure 22-2 Routing and RRAS Admin administration tool

2 Add the OSPF protocol.

Right-click the General folder under IP Routing, and choose **New Routing Protocol**. In the New Routing Protocol dialog box, click “Open Shortest Path First (OSPF)” and click **OK**.

3 Select each interface on which you want to enable the routing protocol.

Right-click OSPF in the IP Routing folder and select **New Interface**. Select the desired interface, then click **OK**. Configure the Internet properties for that interface on the dialog box that opens, then click **OK**.

Note: If the interface you want to add is not show in the Select Interface dialog, add it to the Summary by choosing Add Routing Protocol from the Actions menu.

4 Close the Routing and Remote Access dialog box to return to the Management Console.

Configuring and enabling IPX

Note: When you configure IPX, RRAS automatically adds RIP and SAP. The Microsoft default of 0 for RIP and SAP timers will not work. You must update them to larger values, such as 30 for the update timer and 3 for the timeout multiple. Refer to Microsoft RRAS documentation for complete instructions.

After configuring IPX, enable it using RRAS to instruct Microsoft Windows to register bindings, automatically add RIP and SAP, and show adapters as Up in the IPX Summary.

To configure IPX:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Network Services & Adapters icon, located in the Data Administration section.

3 Log on using your Wave username and password. The Network Connections dialog box opens.

For more information about logging in with a remote connection, see “Remote Access Application applets” on page 2-5.

4 Right-click the desired interface and select **Properties**.

5 Select NWLink IPX/SPX Compatible Transport from the list.

If this IPX option is not on the list, you will need to click Install... and follow the onscreen instructions to install it first.

6 Click Properties.

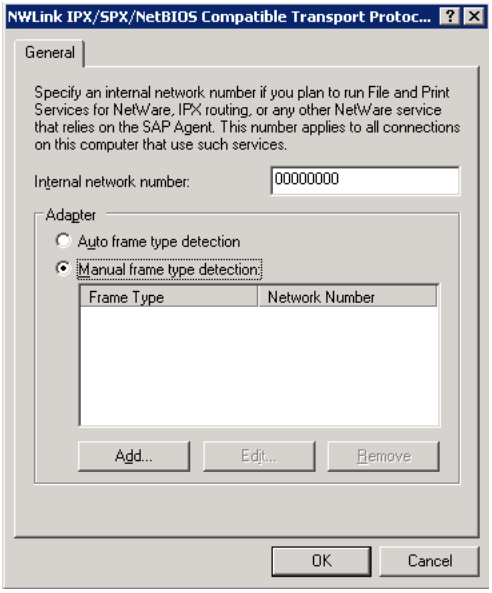


Figure 22-3 NWLink IPX/SPX Properties dialog

7 Specify a unique Internal Network Number for the Wave ISM.

8 Select Manual Frame Type Detection.

9 Click Add.

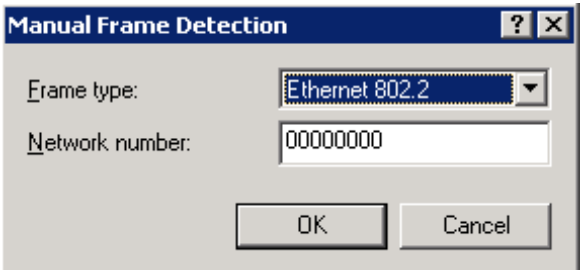


Figure 22-4 Manual Frame Detection dialog

10 Select a frame type from the Frame Type drop-down list. If IPX is only used across Ethernet, any of the frame types can be used.

11 Type a network number.

This number must be the same as the IPX server network number.

12 Click OK.

The frame type you have selected appears in the list.

13 Repeat steps 4 through 12 if you have additional interfaces on which IPX needs to be enabled.

14 Return to the Management Console.

Configuring the Wave ISM as a network services client

The Wave ISM cannot be a client to a DHCP server, as each Wave LAN network interface / routing port must use a static IP address.

- Configuring the Wave ISM as a DNS client
- Configuring the Wave ISM as a WINS client

Configuring the Wave ISM as a DNS client

To configure your Wave ISM as a DNS client:

1 Make sure the Wave ISM has a valid static IP address.

2 If necessary, click the Administration tab of the Management Console.

Click

3 Click the IP Network Settings icon, located in the Data Administration section.

4 Click the DNS tab.

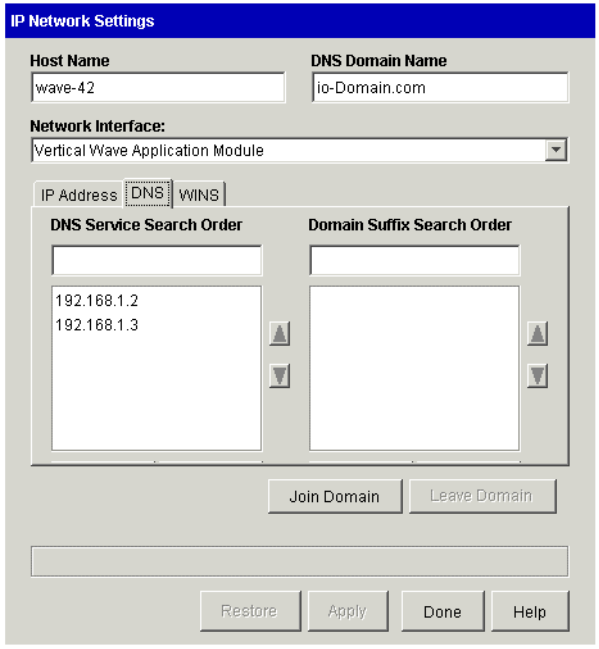


Figure 22-5 IP Networks applet, showing DNS tab

5 Enter the IP address of your DNS server (the server that resolves DNS name queries) in the DNS Service Search Order field, then click Add.

The order in the list is the order in which they will be queried. Put the IP address of the preferred DNS server first. Typically, the local company's DNS server should be first.

If the list contains addresses, you can use the arrows to move the IP addresses up and down to change the search order.

If you need to remove the DNS server, select the address in the list and click Remove.

You can add additional DNS servers to the list for redundant or additional name resolution services.

6 Enter the domain suffix in the Domain Suffix Search Order field, then click Join Domain.

If the list contains domain suffixes, you can use the arrows to move the them up and down to change the search order.

You can add additional domains to the list.

7 Click Apply to confirm your changes.

Changes take effect after you reboot your Wave ISM.

Configuring the Wave ISM as a WINS client

To configure your Wave ISM as a WINS client:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the IP Network Settings icon, located in the Data Administration section.

3 Select the WINS tab.

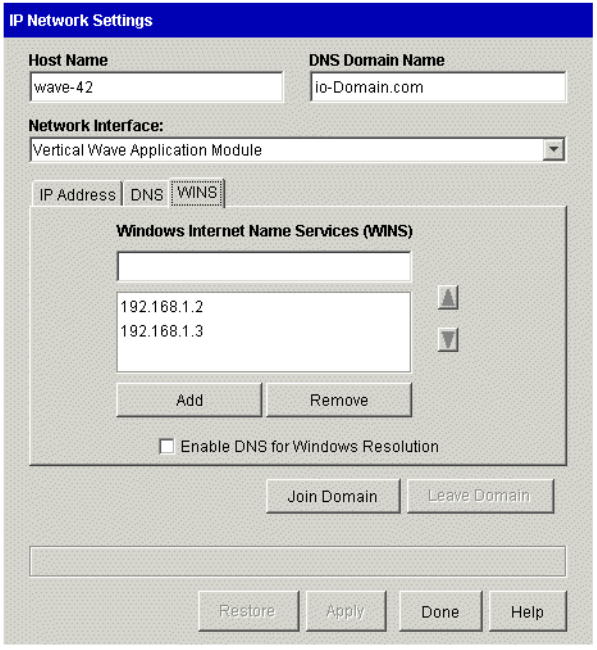


Figure 22-6 IP Network Settings applet, showing the WINS tab

4 Select a network interface from the Network Interface drop-down list.

Setting up each network interface as a WINS client is recommended.

5 Enter the appropriate server address in the WINS field, and click Add.

Wave registers its name and IP address with the primary WINS server.

6 Select the Enable DNS for Windows Resolution option, if the Wave ISM will also be a DNS client.

This option ensures that DNS servers are also used to resolve client requests.

Note: When DNS is enabled here, you also need to enter DNS server information on the DNS tab of the IP Network Settings applet.

7 Repeat steps 4 through 6 to configure each interface.

8 Click Apply to confirm your changes.

Changes take effect after your Wave ISM is rebooted.

Configuring DHCP relays

Note: Before starting this procedure, ensure you have the IP address of your DHCP server.

To enable and configure a DHCP relay agent:

Click 

1 Open the Microsoft RRAS administration tool, and log on using your Wave username and password.

For more information about logging in with a remote connection, see “Remote Access Application applets” on page 2-5.

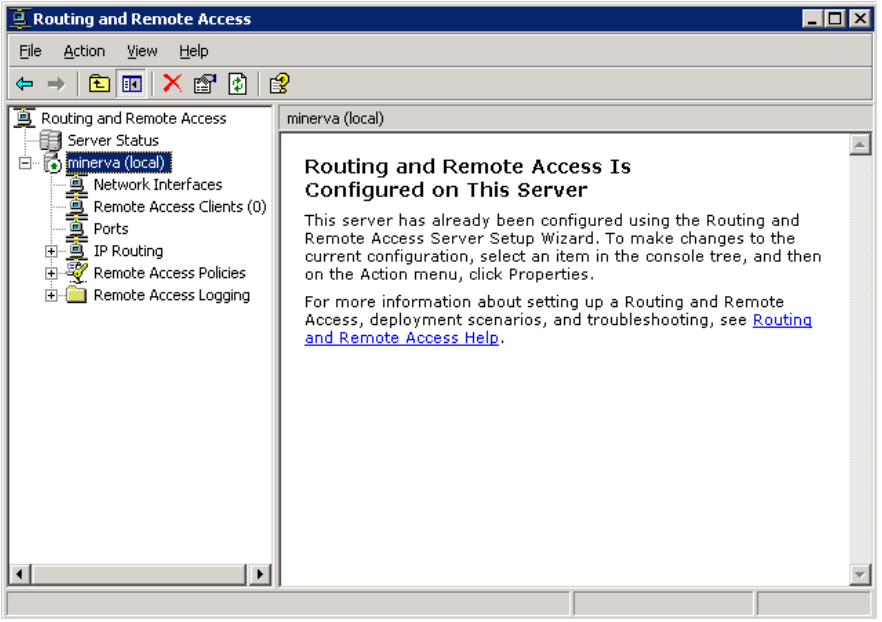


Figure 22-7 Microsoft RRAS administration tool

2 Right-click DHCP Relay Agent in the IP Routing folder and select **New Interface**.

3 Select the desired interface and click **OK**.

4 Return to the Management Console.

Setting up static routes

To set static routes:

Click

1 Open the Microsoft RRAS administration tool, and log on using your Wave username and password.

For more information about logging in with a remote connection, see “Remote Access Application applets” on page 2-5.

2 Right-click Static Routes in the IP Routing folder, and choose **New Static Route**. The Static Route dialog box opens.

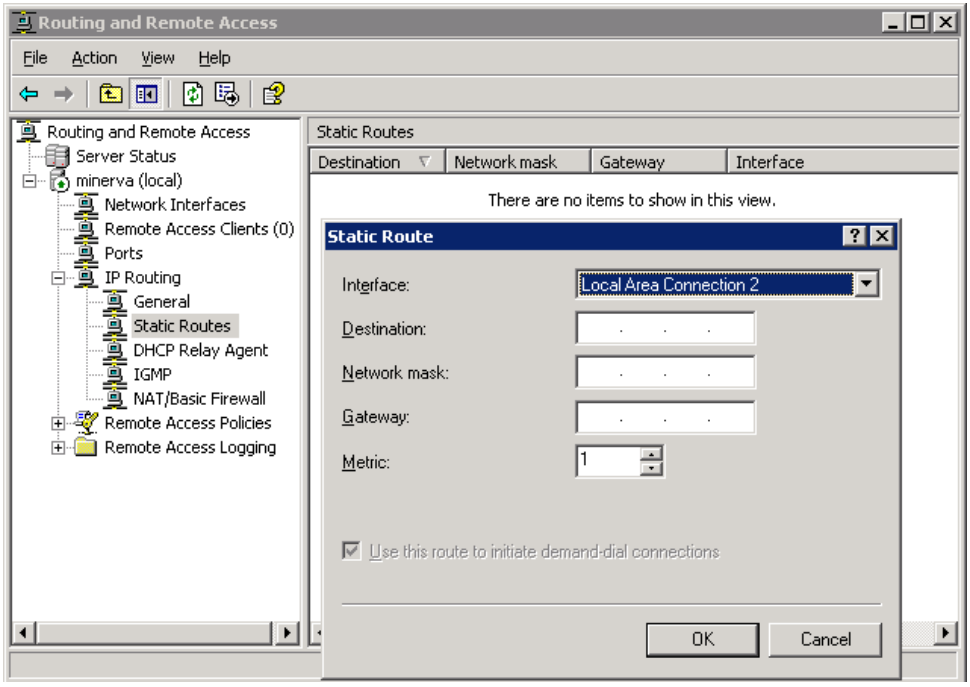


Figure 22-8 Static Route dialog

3 Select an interface from the list.

4 Type a destination IP address, subnet mask, gateway, and metric.

5 Click OK.

6 Close the Routing and Remote Access dialog to return to the Management Console.

Note: When you are configuring for a demand-dial modem connection, you must create a static route for each modem connection to the ISP / headquarters because it is not part of a larger network. If you know the IP address of a remote office, you can put it in the static routing table. You will typically create a default static route (IP address `0.0.0.0`, subnet `0.0.0.0`, and an appropriate gateway address) to be used as a last resort for packets that Wave does not know where to send. When you are configuring a static route for a digital connection, you must enter the gateway address, which is the

IP address for the router on the other side of the digital connection, sometimes called the *far end* or *next hop* router. If you configure a gateway address, you will set up a default static route to that gateway.

Monitoring and Maintenance

CHAPTER CONTENTS

About monitoring and maintaining your Wave system

This chapter describes several methods of monitoring and maintaining your Wave system from within the User / Workgroup Management applet.

To open the User / Workgroup Management applet, click the icon for **User/Workgroup Management**, located in the PBX Administration section of the Management Console.

The instructions in this chapter all assume that you are in the User / Workgroup Management applet.

Other monitoring options

You can also monitor your system using the Wave Call Center Reporter, which lets you run reports on a variety of system elements, including trunk use, call traffic, queues, agents, identified callers, account code use, and more. For more information on running the Call Center Reporter, see *Vertical Wave Contact Center Administrator's Guide*.

You can also automatically record any or all calls in the system for review later. See Chapter 20.

Database server memory usage

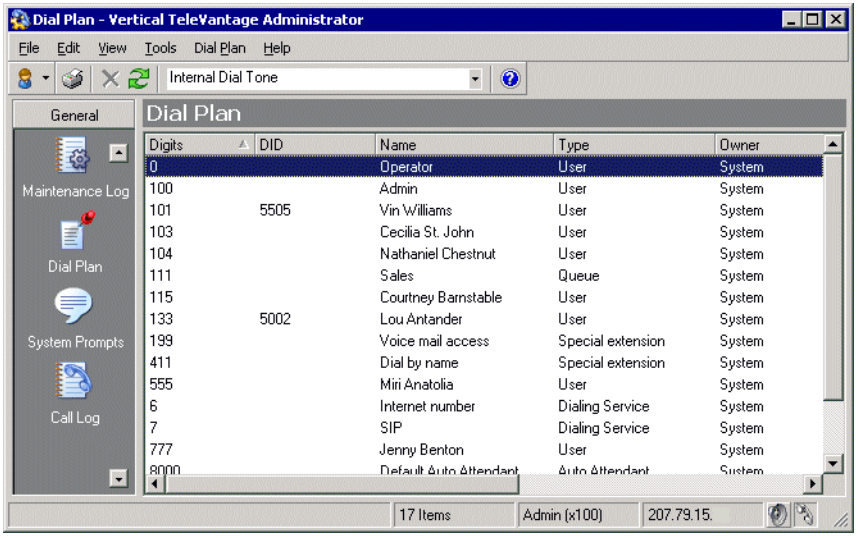
The Wave database is configured by default to use up to 50% of the available system memory, which Wave automatically allocates to itself at system startup. Memory size is set when the Wave ISM starts. If you add more memory to the system (for example, to support more extensions or trunks), memory size is reset the next time you start the Wave ISM.

Memory usage by the database server is dynamic. Some types of database activity (for example, nightly Call Log archiving on busy systems) may require more memory. If more memory is required to support database operations, the database server requests it from Windows. However, this memory is not released automatically when it is no longer needed. For this reason, memory usage by the Wave database typically ramps up to the maximum available, and then levels off. This is normal behavior—not a memory leak—and is not an indication that memory used by the database server is about to reach the maximum or that the system may fail.

If Windows needs the memory back at a later time for its own use or for another application, it will ask the database server to release some. Also, when you stop the Wave ISM, all the memory allocated for use by the database server is released.

Managing your dial plan with the Dial Plan view

You can view and manage your dial plan as a whole using the Dial Plan view.



The Dial Plan view shows each number in your system that can be dialed from an internal dial tone, identified by name and type. It lists only numbers beginning with the digits 0-9, and so does not include Wave telephone commands such as those beginning with Flash or *. It does include the following:

- All enabled extensions (users, auto attendants, call center queues, IVR Plug-ins, etc.)
- Users' contacts dialable by the user's extension + PIN
- User extensions plus * for direct-to-voice-mail dialing, if the feature is enabled (see "Setting general Wave options" on page 4-3)
- Dialing service access codes
- System extensions such as 411 for the dial-by-name directory

You can filter the Dial Plan view using the toolbar dropdown list to show only those numbers that are dialable from external phones (**PSTN**) or SIP servers.

You can use the Dial Plan view to check your dial plan for ambiguous numbers and correct them when they occur. For more information, see “Managing your dial plan with the Dial Plan view” on page 23-3.

You can edit a dial plan entry by selecting it and choosing **Dial Plan > Open**. The appropriate dialog box for editing that number opens. Editing an extension-plus-Contact-PIN opens Wave ViewPoint as if you had chosen **Users > Edit all ViewPoint Settings** from the Users view.

Note: If the **Dial Plan > Open** option is unavailable, you may not have permission to access or edit the selected item.

You can delete a dial plan entry using the Delete key or the toolbar Delete icon.

Using the Maintenance Log view

The Maintenance Log view displays tracked actions and presents details about each action. Information contained in the log is stored in the database. To open the Maintenance Log view, click its button in the view bar. The Maintenance Log tracks many administrative actions, including:

- Restarting a device
- Starting the Wave ISM
- Stopping the Wave ISM
- Scheduling a Wave ISM shutdown
- Changing a user’s password
- Changing a queue’s password
- Logging on to the User / Workgroup Management applet
- Logging out of the User / Workgroup Management applet
- Account lockout
- Trunk hangup after maximum login attempt
- Changing any editable item in any User / Workgroup Management applet view
- Deleting an item from a view
- Enabling or disabling a device

The following columns appear in the Maintenance Log view:

- Action taken
- Item that was acted upon (if applicable)
- Date and time of the action
- Name of the user who was logged on when the change was made
- Name of the computer from which the change was made
- Details about the action

Navigating the Maintenance Log view

The Maintenance Log view shows 50 entries at a time, in a default order starting with the most recent. You can show the next or previous 50 entries by choosing **Maintenance Log > Next 50 entries** or **Maintenance Log > Next 50 entries**.

You can also jump to a particular date by choosing **Maintenance Log > Jump to date**. Enter the date in the dialog box that opens and click **OK**.

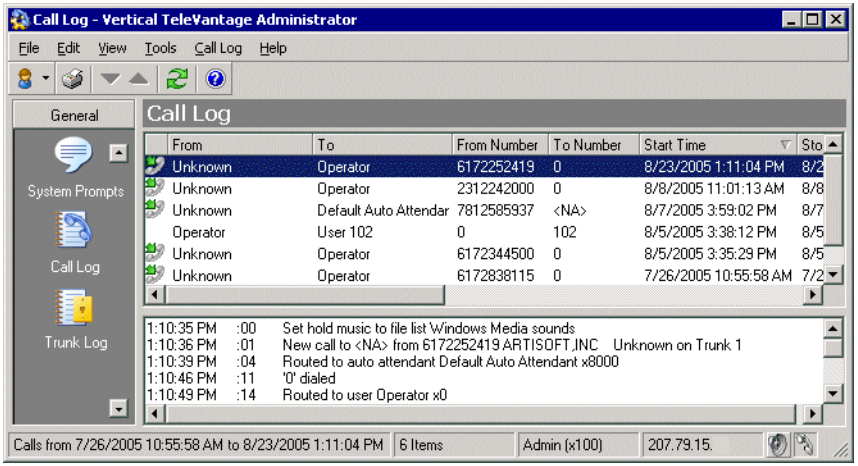
Clearing the Maintenance Log

To clear the Maintenance Log, click  in the toolbar.

Using the Call Log view

The Call Log view displays a record of the calls placed and received on the Wave system. Each call appears as a row in the view. You can use the Call Log view to analyze system usage patterns, and you can export Call Log records to generate traffic analysis reports.

To open the Call Log view, click its button in the view bar.



Call Log columns

The following table shows the information that is displayed for each call. Several columns are hidden by default. To show and hide columns, right-click the columns header and choose **Columns**.

Column	Description
From	Name of the person who placed the call. On incoming calls, “Unknown” appears unless the user identified the caller as a contact. On outgoing calls, this column contains the user’s name.
To	Name of the party who received the call. On incoming calls, the user’s name appears. On outgoing calls, “Unknown” appears unless the user identified the person as a contact.
Answered By	Name of the user who answered an incoming call or was last dialed. On unanswered calls, the name of the user who was dialed. On answered calls that were subsequently transferred, the name of the transfer recipient, whether or not they answered.

Column	Description
Number	On incoming calls, Caller ID name and number if available. On outgoing calls, the number the user dialed. On a call to or from another Wave user, this field contains <NA>.
From Number	On incoming calls, the caller's extension or external phone number. On outgoing calls, the user's extension.
To Number	On incoming calls, the user's extension or, if the user called into Wave externally, the external number. On outgoing calls, the external number or extension the user called.
Callback Number	If a caller enters a callback number, it appears with the prefix "Callback:"
Called Number	On incoming calls, your Direct Inward Dial (DID) number if the caller used it to call you. The field is blank for incoming calls without DID. On outgoing calls, the number you dialed.
Start Time	Date and time that the call started.
Wait Time	On incoming calls, the length of time between dialing the user's extension and the call being answered. On outgoing calls, Wait Time is always 00:00.
Duration	Length of time that the parties are connected.
Call ID	The Wave ID number of the call. The call ID number also appears in queue logs to identify the call (see Appendix A of the *Vertical Wave Contact Center Administrator's Guide*).

Column	Description
Result	How the caller's wait ended. The assigned values for the possible outcomes are: **Abandoned.** Caller hung up before call was answered. **Connected.** Caller was connected to a party. **To voice mail.** Caller went to voice mail, but did not necessarily leave a message. **Blind transfer.** A blind transfer sent the caller to another party. **Supervised transfer.** A supervised transfer sent the caller to another party. **Login.** Caller logged in to a valid Wave user account. **No Answer.** Outbound call that was not answered. **Login failed.** The caller attempted to log in to a Wave account, but failed to enter a valid password for the maximum number of retries (see "Enforcing strong password security" on page 4-11). **Unknown.** Wave was unable to identify the outcome of the call.
Account Code	The account code entered for the call, if any.
Message	If checked, the caller left a voice message.
Recorded by User	If checked, this call was recorded by a user who handled it.
Recorded by Queue	If checked, this call was automatically recorded by a call center queue.
From Device	On incoming calls, the trunk or extension from which the call originated. On outgoing calls, the user's station number.
To Device	On incoming calls, the user's station number. On outgoing calls, the trunk used for the call. If an incoming call was transferred, this column shows the last station that took the call.
Parties	Number of people who took part in the call, including the caller, the called party, anyone to whom the call was transferred, and any conference call participants.

Column	Description
Dial String	Digits that Wave actually dialed over the trunk, which may be different than the digits Wave displays in a contact's phone number. For example, a dial string may contain an international or long-distance access code, a dialing prefix, or a dialing suffix.
From Type	Type of incoming call: Phone or Internet.
From Code	Access code of the dialing service that will be used to return this call. Only applicable to calls coming in from remote Wave ISMs over an Internet trunk.
From Rules	If checked, Wave's routing rules will be applied when returning this call.
To Type	Type of outgoing call: Phone, Centrex, or Internet.
To Code	Access code used to dial an outbound call.
To Rules	If checked, routing rules were used to make an outbound call.
Organization	Organization associated with the call, if any. Organizations are associated with outbound calls only, and represent the Organization to which the calling party belongs. For more information see “Using Organizations” on page 21-2.
Custom Data	Custom data, if any, associated with the call.

Copying a Call Log entry

Choosing **Edit > Copy** with a Call Log entry selected copies that Call Log entry as text, including call history.

Viewing a call’s history

When you select a call in the Call Log, its history in the system appears in the History pane below. The History pane shows the complete “cradle-to-grave” record of the call from the moment it entered the Wave system until it was disconnected. You can see how a call was routed or transferred, and how it ended.

By default call history data is automatically purged from the system after 5 days to conserve disk space. To adjust the number of days, see “Setting Call Log options” on page 23-12.

Setting Call Log options

To choose whether or not to use the Call Log, and whether or not to log internal calls, see “Setting Call Log options” on page 23-12.

Displaying a specific number of Call Log entries

The Call Log can become very large over time and its size can cause a delay in its display. To reduce this delay, you can view fewer Call Log items at one time and not load the full database.

To set the number of calls displayed in the Call Log:

1. From the User / Workgroup Management applet, choose **Tools > Options**. The Options dialog box opens.
2. In **Display __ Call Log entries at a time**, enter the number of entries that you want to appear when you open the Call Log view, using the following as a guide:
   - A high setting will likely cause a delay while the specified number of entries are copied over the network, but you can navigate within the information easily using the scrolls bars after the entries have been retrieved.
   - A low setting minimizes the delay before information is displayed, but you must retrieve entries more often in order to view the entire Call Log.
3. Click **OK**.

Note: This option controls how many entries are transferred in one request, but does not limit the entries available for view. All Call Log entries are always available by choosing **Call Log > Next __ Calls** or **Previous __ Calls**, or using the buttons on the toolbar.

By default, only external calls are logged. For information about logging internal calls, see “Setting Call Log options” on page 23-12. For information about archiving the Call Log, see “Archiving the Call Logs” on page 23-48.

Entering an account code for a call

To enter an account code for a call or change the one already entered, select the call and choose **Call Log > Enter Account Code**.

Account codes are a means of marking calls for tracking or billing purposes. For more information, see "Using account codes" on page 21-6.

Exporting the Call Log

You can export the Call Log to a comma-separated value (.CSV) file that can be read by most spreadsheet and database applications. Exported Call Log entries are not deleted from the Wave database, and the size of the Wave database does not change after an export.

1. Choose **File > Import and Export**. The Import and Export Wizard opens.
2. Under **Select an import or export action**, select **Export Call Log** and click **Next**.
3. In **Save exported file as**, enter the path and file name for the exported file or click **Browse** to specify a destination.
4. Under **Options**, enter the **Start date** and **End date**.
5. Click **Finish** to export the file. Depending on the size of your Call Log, an export may take several minutes to complete.

Archiving the Call Log

See "Archiving the Call Logs" on page 23-48.

Result codes when exporting the Call Log

When the Call Log is exported, the Result field appears as a code. Use the following table to interpret the result codes:

Code	Result
0, 3	Abandoned
1, 2	Connected

Code	Result
4	Left message
5	Blind transfer
6	Supervised transfer
8	Login to telephone commands
12	Login failed max number of times

Setting Call Log options

You can choose whether to log calls, and which type of calls are logged in the Call Log. To do so:

1 Choose **Tools > System Settings**. The System Settings dialog box opens.

2 Choose the Call Log tab.

3 Use the following fields to set up your call logging choices:

- **Log calls.** If checked, Wave logs calls in the Call Log according to the selections you make on this tab. If unchecked, the Call Log is not used.
- **Log internal calls.** Check to have internal (station-to-station) calls logged in the Call Log. If unchecked, the Call Log keeps track of calls that involve a trunk only.
- **Log call history events.** Check to have call history events logged for recent calls displayed in the Call Log (note that call history events are purged after a number of days, as defined below).
- **Delete call history events older than __ days.** Enter the number of days that call history text remains in the system before being automatically deleted.

4 Click **OK**.

Viewing the Wave Event Log

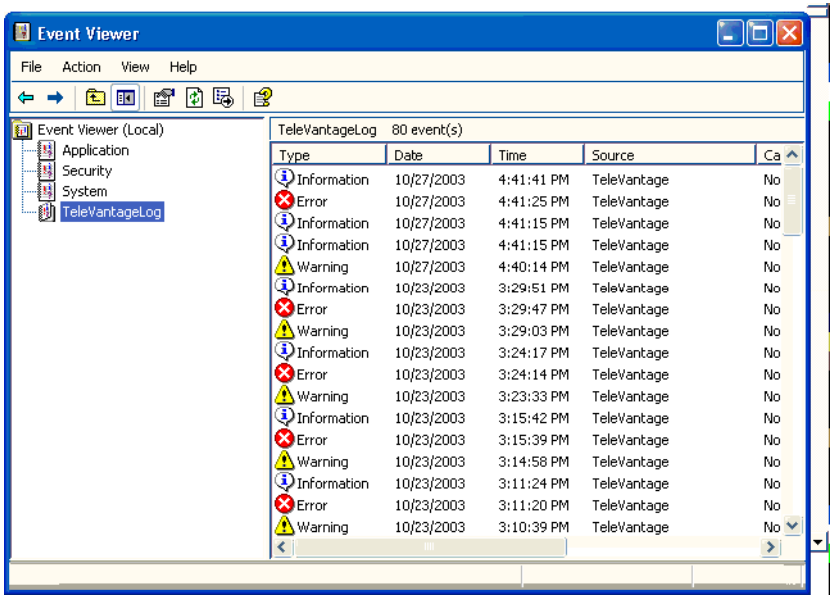
The Wave Event Log contains a record of all Wave-related system events, including start and stop times of the Wave ISM and other Wave applications, and error messages.

Errors indicate that a failure has occurred. Warnings indicate that a critical resource is getting low, though no failures have occurred yet.

Note: All calls to 911 are logged in the Windows Event Log as an entry.

You can set up Wave to send e-mail notifications when events are logged to the Wave Event Log. For more information, see “Setting up Wave Event Log notifications” on page 23-13.

To view the Wave Event Log, choose **Start > Programs > Administrative Tools > Event Viewer.** Click **WaveLog.**



Setting up Wave Event Log notifications

You can configure Wave to send e-mail notification of each event logged in the Server’s Wave Event Log. By setting up notifications, you can stay informed of critical problems, like low disk space, no matter where you are.

To receive e-mail notification of Wave Event Log events:

1 Choose **Tools > System Settings**. The System Settings dialog box opens.

2 Choose the E-mail Notification \ Event Log tab.

3 Under **E-mail phone system events for**, select one of the following from the drop-down list:

- **No events.** This is the default. No notifications are sent.
- **Errors and warnings.**
- **Errors only.**
- **All events.**

4 Under **E-mail to**, identify to whom the e-mail notifications are sent:

- **All phone system administrators.** Notifications go to all Wave users with Global Administrator permissions who have e-mail notification turned on. The users you identify here must also have e-mail notification set to receive Windows Event Log notifications (see "Setting e-mail notification" on page 11-22).This is the default setting.
- **E-mail address(es).** Enter the e-mail addresses of users whom you want to receive notifications, separated by semicolons.

5 Click **OK**.

Wave Event Log messages

Messages are identified in the Wave Event Log by application and message number. Double-click a message to see its text.

The following messages are posted to the Wave Event Log:

This SQL Server has been optimized for 8 concurrent queries. This limit has been exceeded by # queries and performance may be adversely affected.

This event means that occasionally the Wave ISM and ViewPoint are concurrently accessing the Wave database in excess of the 8 simultaneous database transactions allowed by Microsoft's MSDE database. You can ignore this message if you only receive 100 or so of these events per day. If you're getting this event hundred of times per day, you should upgrade to the full version of Microsoft SQL Server which doesn't have a limit on the number of simultaneous queries. See Chapter 3 of *Vertical Wave Installation Guide* for more information.

100 - Informational
Server Started -- Version ##

An informational message indicating when the Wave ISM started.

101 - Informational
Server Stopped

An informational message indicating when the Wave ISM was shut down. This message indicates an orderly shutdown, not a shutdown caused by a problem.

102 - Informational
Connecting to SQLServer

103 - Informational
Disconnecting from SQL Server

Information messages indicating when the Wave ISM connected to and disconnected from SQL Server.

104 - Error
DSSQL Error

105 - Error
No Voice Resource Available

This message indicates that Server was unable to provide a voice resource for a requested operation. This error should not be encountered in normal operation and may indicate that you need additional voice resources for your current load. For more information on how to add voice resources, see *Installing Intel Telephony Components*.

106 - Informational
Device ## Restarted

This message indicates a trunk or station was restarted to recover from an error condition. The restart may have been initiated automatically by the Wave ISM or manually by the administrator. If this message appears only infrequently, it can be ignored. If it is seen often, contact your Wave provider.

107 - Informational
Inbound call detected on outbound trunk ##

This message indicates a call was received on a trunk allocated for outbound calling only. The Wave ISM played a wrong number message and disconnected the call. If this message is seen frequently, it may indicate that the number for the line in question has been distributed to potential callers or that the line is included in an inbound hunt group.

108 - Informational
Inbound H.323 Gateway authentication failed. Trunk ##, Gateway extension: ##, Source: nnn.nnn.nnn.nnn

This message indicates that an inbound H.323 Gateway call failed to provide the correct password.

110 - Error
Error occurred trying to perform least-cost routing.

111 - Error
Unable to start Mail Server. Voice Mail notifications via Email will be disabled.

On startup, the Wave ISM was unable to start the e-mail notification process. For example, it could not establish a MAPI connection with your mail post office. Mail notification will be disabled until the problem is resolved. Contact your Wave provider.

112 - Informational
Started Mail Server.

An informational message indicating that the Wave Mail Server started successfully when the Server started.

113 - Warning
No loop current detected on outbound trunk N

114 - Error
Thread performing least-cost routing is not responding.

115 - Error
Server Restarted

The Wave ISM had to be restarted by the Wave Watchdog process.

116 - Error
Server cannot record any more voice messages or calls. Disk space is low.

Wave cannot perform call recording on voice messages or calls, because the disk space on the voice files disk is low.

117 - Informational
Server can now record voice messages and calls. Disk space is available.

Call recording can resume, after having been disabled due to low disk space. Sufficient disk space on the voice files computer is now available.

118 - Error
Stopped using trunk ##: the trunk may have been disconnected.

Wave ISM has stopped using a trunk.

119 - Error
Failed to Restart Server: Total Restarts Exceeded.

Wave ISM failed to restart after trying several times.

120 - Error
Failed to Stop Device Handle ##.

121 - Error
Unable to start Exchange Server synchronization. Exchange Server synchronization will be disabled.

Unable to start Wave Exchange Server synchronization.

122 - Informational
Started Exchange Server synchronization.

Wave ISM started Microsoft Exchange Server synchronization.

123 - Error
Unable to open device: ##

Wave ISM was unable to open the device.

124 - Error
Unable to delete temporary message file for device ##.

This is recorded when there is a problem deleting a temporary message file for a device. The temporary message file for station 2 is `S2-m.vox`. For example, if this file cannot be deleted, an invalid message will be left for the recipient.

125 - Error
T1 Alarm: <Alarm Information>

A T1 alarm occurred on the trunk.

T1 alarms

The following two T1 alarms are written to the Windows Event Log:

- **Red Alarm.** Signals that the Robbed Bit T1 line has lost synchronization with the switch to which it is connected. Wave disables all channels on the affected digital span so that spurious signals are not processed as incoming calls.

- **Red OK.** Signals that synchronization has been restored. All channels on the affected digital span are re-enabled.

All T1 alarms are written to the Wave ISM logs.

126 - Error
Unable to start IVR Plugin '<ProgID>': License count exceeded.

Unable to start the IVR Plug-in because the number of your Station licenses is less than the total number of stations assigned to users plus the total number of IVR Plug-ins currently running (every running IVR Plug-in uses 1 Station license).

127 - Error
Insufficient licenses: <message>

Wave ISM detects an insufficient number of Trunk, IP Port, ViewPoint, or Server licenses, and the ISM was unable to start. Make sure that you have Wave licenses for every user, trunk, and IP trunk you have added in the Global Administrator.

128 - Error
Notification via pager failed; Unable to allocate trunk; user '<username>', number '##', access code ##

An attempt to send a pager notification of a new voice message failed. The error message shows the user's name and the full dial string of the pager number that was dialed unsuccessfully. Alert the user that the pager number might be incorrect or that pause characters should be added to the dial string.

130 - Error
Disabling Exchange Server synchronization. Unable to connect to database.

Wave could no longer access the SQL Server database and disabled Exchange Server synchronization.

131 - Error
Failed to reset station N. Please restart the server.

132 - Error
Ring failed on station ## with error 14. Please restart the station.

133 - Error
Device ## is not responding, restarting...

Wave was unable to open the device and is automatically restarting it.

134 - Error
Unable to offer call to IVR Plug in '<ProgID>'. Reason: '<reason>'.

Started the IVR Plug-in but OfferCall failed.

135 - Error
CallPlaced Event failed IVR Plug in '<ProgID>'. Reason: '<reason>'.

Failed to hand off and outbound call to an IVR Plug-in.

136 - Error
Unable to start IVR Plug in '<ProgID>'. Reason: '<reason>'.

137 - Error
Device ## is not responding.

The trunk or station has stopped responding to events. Try restarting it.

138 - Error
Email notification thread is not responding.

E-mail notifications will be disabled until the problem is resolved.

139 - Error
Device ## Disabled.

This station or trunk was disabled by a user through the Global Administrator.

140 - Informational
Device ## Enabled.

This station or trunk was re-enabled by a user through the Global Administrator.

142 - Informational
Emergency: <Username> at extension x## dialed <emergency number> from <station ##>

The specified user dialed Wave's emergency number (usually 911) from the specified station.

143 - Informational
Timed Out Waiting For Response from IVR Plugin '<AppID>'. Reclaiming voice device.

The specified IVR Plug-in did not respond to the Wave ISM. The ISM assumed that the Plug-in was hung, and has terminated it and reclaimed its associated voice resource.

144 - Informational
Maintenance log cleared.

The Maintenance Log has been cleared using the User/Workgroup Management applet. See "Using the Maintenance Log view" on page 23-4.

145 - Warning
Account <name> has been locked out due to password failures.

The named user account has been locked out due to repeated attempts to access the account with bad passwords. .

146 - Warning
No Low Priority Voice Resource Available

There are no low-priority voice resources in the pool available to generate FSK signals for CLASS or ADSI phone features such as message waiting light, Caller ID display, intercom, paging, or voice-first answering. Voice resources will continue to be allocated for other tasks such as playing and recording voice files. For more information on managing voice resources, *Vertical Wave Installation Guide*.

147 - Error
No Voice Resource Available For System Call Recording

148 - Error
Removing Failed Sink: <name>

149 - Warning
Database size is nearing critical limit. Archive call log or upgrade to full version of SQL Server.

Your Wave database is nearing the 2GB limit of MSDE. Archive the Call Log to make more room (see "Archiving the Call Logs" on page 23-48), or upgrade to the full version of SQL Server if you have not done so already. See the database server requirements in *Vertical Wave Installation Guide*

150 - Error
Database size has passed the critical limit and call logging has been stopped. Archive call log or upgrade to full version of SQL Server.

New calls are not being written to the Call Log because the Wave database has passed the critical MSDE size limit (about 2 GB). Archive the Call Log to make more room (see "Archiving the Call Logs" on page 23-48), or upgrade to the full version of SQL Server if you have not done so already. See the database server requirements in *Vertical Wave Installation Guide*.

151 - Informational
Hook State mismatch occurred on station N.

155 - Error
Infinite Loop:

Wave detected a call center which may be sending callers back and forth to an extension in an infinite loop. This can happen if the queue redirects callers to an extension whose routing list automatically sends calls to the queue.

157 - Error
Failed to resolve the following email addresses:

An email notification was sent where at least one of the email addresses could not be resolved from a name to an address, for example, an address of "John Smith" could not

be resolved as an e-mail address. Possible causes include a mistyped name (for example, “Jhon Smith”), an ambiguous name (for example, “John S”), or a problem with the address book associated with the default MAPI profile on the Wave ISM PC.

158 - Error
Failed to send email. subject:

Wave failed to send the specified email notification. This can happen for numerous reasons, such as a network failure. The specific error is included if available.

159 - Error
Exchange server synchronization failed for Wave <username> with Exchange mailbox <name> on Exchange Server <servername>

Wave failed to synchronize voice messages with email notifications in the Exchange mailbox for the specified user. This can happen for numerous reasons, such as a network failure. The specific error is included if available.

160 - Error
Error archiving voice mail: <name>

161 - Error
No Voice Resource Available For Beep during Call Recording

162 - Error
Server Started After Unexpected Shutdown

163 - Warning
No conference resource available

The ISM has run out of conference resources. These messages will be logged every 15 minutes while conference resources are out.

164 - Warning
Server cannot communicate with Workstation applications because you have Internet Connection Firewall (ICF) enabled.

For the ISM to operate properly with a firewall, you must upgrade your PC to Windows XP SP2 or higher. Alternatively you can disable ICF.

165 - Warning
Server cannot communicate with Workstation applications because Windows Firewall exceptions are not allowed.

Please enable Windows Firewall exceptions by selecting "Start" > "Control Panel" > "Windows Firewall" and uncheck "Don't allow exceptions".

166 - Warning
ISM cannot communicate with Workstation applications due to a problem creating a Windows Firewall exception.

Please disable the Windows Firewall by selecting "Start" > "Control Panel" > "Windows Firewall" and uncheck "On".

167 - Warning
Server cannot communicate with Workstation applications due to a problem with system DCOM settings.

168 - Warning
Cannot communicate with your <name> Server because you have Internet Connection Firewall (ICF) enabled.

To use this application with a firewall, you must upgrade your PC to Windows XP SP2 or higher. Alternatively you can disable ICF.

169 - Warning
Cannot communicate with your <name> Server because Windows Firewall exceptions are not enabled.

170 - Warning
Cannot communicate with your <name> Server due to a problem creating a Windows Firewall exception.

To use this application please disable the Windows Firewall by selecting "Start" > "Control Panel" > "Windows Firewall" and uncheck "On".

171 - Warning
Cannot communicate with your <name> Server due to a problem with system DCOM settings.

172 - Warning
Windows networking settings have been updated so the <named> workstation applications can operate properly. You must restart your computer before the new settings will take effect.

173 - Informational
Server is configured to ignore all telephony devices.

To detect telephony devices, choose **Tools > System Settings**, click the Server tab, and uncheck **Server should not detect devices during startup.**

174 - Warning
Device N State Changed. Reason: <name>.

175 - Error
Exchange server synchronization failed for user "<name>"

The listed user has an Exchange mailbox that matches more than one entry on the Exchange server. Edit the user and specify a unique mailbox name.

176 - Error
Wave is unable process email because it cannot connect to the database.

Wave could not connect to the database after 10 attempts. Possible reasons include email notification and/or Exchange synchronization may not be working properly.

177 - Error
Missing language file: <name>.

178 - Error
No voice resource available for hold audio source N. No hold audio will be played.

179 - Error
No files for hold audio source N. No hold audio will be played.

180 - Error
Unable to open file <name> for hold audio source N. File will be skipped.

186 - Error
The N Driver Updates version N was not installed on this PC. Please install these N Driver updates for proper operation.

188 - Error
No IP Media Resource Available

189 - Error
No Low-bit Rate Codec Resource Available

190 - Warning
The custom N network capture filter is invalid and the default capture filter will be used instead. Ensure that the custom N capture filter was entered properly or contact your N Provider to obtain a valid capture filter.

For more information, see the capture filter syntax in the documentation section of http://www.winpcap.org.

191 - Error
The Server did not start because the IP address specified when you installed HMP is no longer valid.

You must change it by editing the HKEY_LOCAL_MACHINE\SOFTWARE\SBLabs\dm3ssp registry key. You should use a static IP address, not one that is dynamically assigned.

192 - Error
MP3 Conversion Error: <name> in function N.

193 - Error
Unable to start SIP span N. Reason: <name>.

194 - Error
SIP trunks are out of service: no available IPM resources found in the system.

195 - Warning
'Off hook' event received from station N, which is currently out of service and not registered with the Server.

Please check the SIP device's configuration and its registration with the Wave ISM's SIP span.

196 - Error
Attempted to call station n, which is currently out of service.

Please check the station configuration and its registration with the Wave ISM.

198 - Warning
Server cannot capture network traffic due to low disk space.

Please make sure N MB of disk space is free for network traffic to be captured.

199 - Informational
Server is now capturing network traffic. Disk space is available.

200 - Error
Username <name> has been locked out from SIP authentication for N seconds due to N repeated authentication failures.

201 - Error
New voice mail call notification failed for user <name>; Unable to reach <name>.

202 - Warning
Network capture was unable to start because it was unable to discover a valid NIC.

203 - Warning
Network capture was unable to start because no valid WinPCap library.

204 - Error
This beta version of the Server ## has expired.

The ISM will be able to process calls from stations or logged-in trunks until it is upgraded to a newer version. Please contact your Wave provider for a newer version.

205 - Warning
This beta version of the Server ## will expire on <date>.

On this date the ISM will not be able to process calls from stations or logged-in trunks until it is upgraded to a newer version. Please contact your Wave provider for a newer version as soon as possible.

206 - Error
Server logging has been disabled due to a disk operation error. Failed to open log file ##.

Please check the drive for errors.

207 - Warning
A hard drive partitioned as FAT32 has been detected on the Server.

Please convert the drive to NTFS to ensure mission critical reliability for the ISM.

7000 - Error
The dlgcmpd service failed to start due to the following error: The system cannot find the device specified.

7001 - Error
The dlgcmcd service depends on the dlgcmpd service which failed to start because of the following error: The system cannot find the device specified.

Viewing Wave performance counters

When the Wave ISM is installed, the Setup program registers with Windows a set of Wave-specific performance counters for tracking run-time ISM statistics. A Wave performance counter template is also installed that you can enable to aid in the tracking down of any performance issues on the Wave ISM PC, including third-party applications.

Note: If you have created or deleted Wave devices, performance counter data may not be accurate until you restart the device.

Enabling the Wave performance counter template

1. On the Wave ISM PC, choose **Start > Programs > Administrative Tools > Performance**. The Performance dialog box opens.
2. Expand the Performance Logs and Alerts tree view and select **Counter Logs**.
3. Do one of the following, depending on your system:
   - **Windows XP / Windows 2003 Server.** Select **TvPerformance** in the list.
   - **Windows 2000.** Choose **Action > New Log Settings From**, and browse to \Program Files\Wave Server \TVPerformance.htm. Click **OK** twice. When **TvPerformance** is added to the list, select it.
4. Choose **Action > Start** to enable logging.

Once enabled, performance log data is written to the \Program Files\Wave Server\Logs directory.

Limiting performance data logging

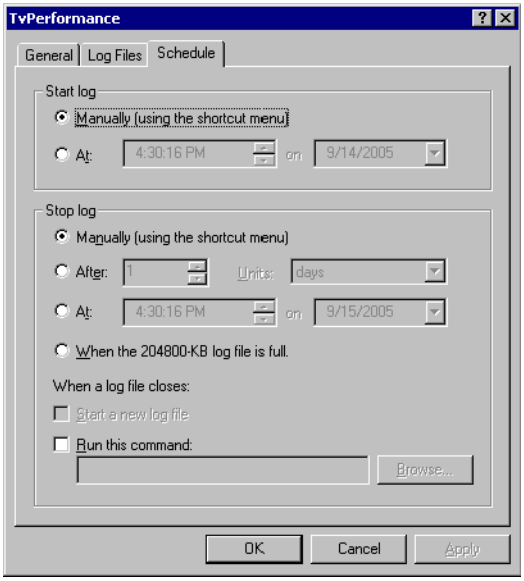
By default, data is continuously written to multiple 200 MB files as long as there is available disk space on the drive, or until you turn performance logging off (by selecting **TvPerformance** as described in the previous procedure, then and choosing **Action > Stop**.)

To avoid having to monitor available disk space on the drive and manually turn off performance logging when disk space gets low, you can limit the size of the logs or the logging time period. To do so:

1 Open the Performance dialog box as described in step 1 above.

2 Right-click **TvPerformance**, and then choose **Properties**.

3 Click the Schedule tab.



4 Use the fields in the **Stop log** section to specify when logging will end automatically.

5 Click **OK** to save your change.

How Wave counters are organized

The counters are organized into two groups: Phone System Calls and Phone System Devices. The counters can be monitored by system administration tools such as the performance monitoring utilities provided with Windows.

The Phone System Calls group has the following counters:

- **Existing calls.** Total number of active calls currently being handled by Wave.
- **Total calls.** Total number of calls handled by the ISM since it was last started.

The Phone System Devices group has the following counters:

- **Stations.** Total number of internal and external stations configured and in service in the system.
- **Station in use.** Number of stations off-hook.
- **% stations in use.** Percentage of stations off-hook.
- **Trunks.** Total number of configured trunks in the system.
- **Trunks in use.** Number of trunks allocated to calls.
- **% trunks in use.** Percentage of trunks allocated to calls.
- **Voice Resources.** The total number of shared voice devices, plus any disconnected voice devices. A disconnected voice device is an LSI port without a physical trunk plugged in, that displays as “No Loop Current” in the Device Monitor. For example, if a system had one D/160SC-8LS trunk board with physical trunks plugged into four of the eight slots, the Performance Counters voice resource figure would be 12—eight shared plus four disconnected.
- **Voice Resource in use.** Number of voice resources currently being used.
- **% voice resources in use.** Percentage of voice resources currently being used.
- **IP Media Resources.** The total number of shared IP Media resources (also known as Intel RTP resources) in the system available for SIP. This number does not include IPM resources attached to trunks disabled using the "DisableDevices" registry setting.
- **IP Media Resources in use.** The total number of shared IP Media resources being used.
- **% IP Media Resources in use.** The percentage of shared IP Media resources being used.

- **RTP Relays in use.** The total number of RTP Relays being used. This number indicates how many SIP trunks are currently using RTP Relays.
- **LBR Codec Resources.** The number of low-bit rate (LBR) codec resources (g723 and g729) on a system running HMP. The number of concurrent SIP calls using low-bit rate codecs is limited to the number of LBR codec resources. All calls in excess of this limit will use the g711 codec if it is configured in the span or dialing service, or fail if g711 is not configured. The **LBR Codec Resources in use** and **% LBR Codec Resources in use** counters show how many LBR counters are currently being used by the system. Note that on a non-HMP system, these counters will always show as 0.

Viewing performance counters in Windows

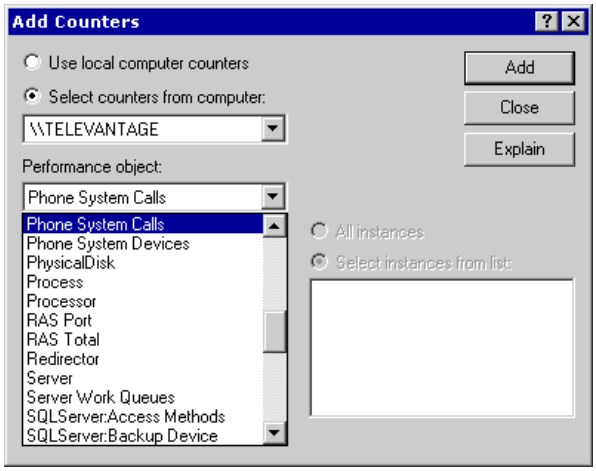
The performance monitoring utility that comes with Windows is the application most commonly used to view performance counter information. You can add Wave counters to a performance monitor's display just as you can with the pre-installed Windows counters.

Note: This section does not describe the performance monitoring utility in depth. See the utility's Help if you need more detailed information.

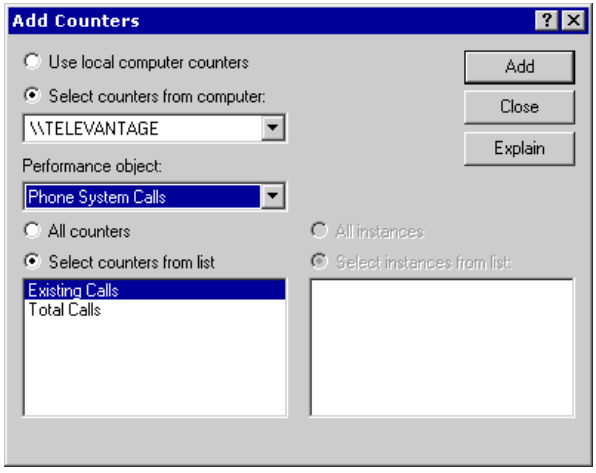
To start the Windows Performance Monitor, choose **Start > Administrative Tools > Performance Monitor.**

In Windows 2000, the utility is part of the Microsoft Management Console and is called the System Monitor. To start the Management Console, choose **Start > Administrative Tools > Performance**. The following examples use the System Monitor from Windows 2000.

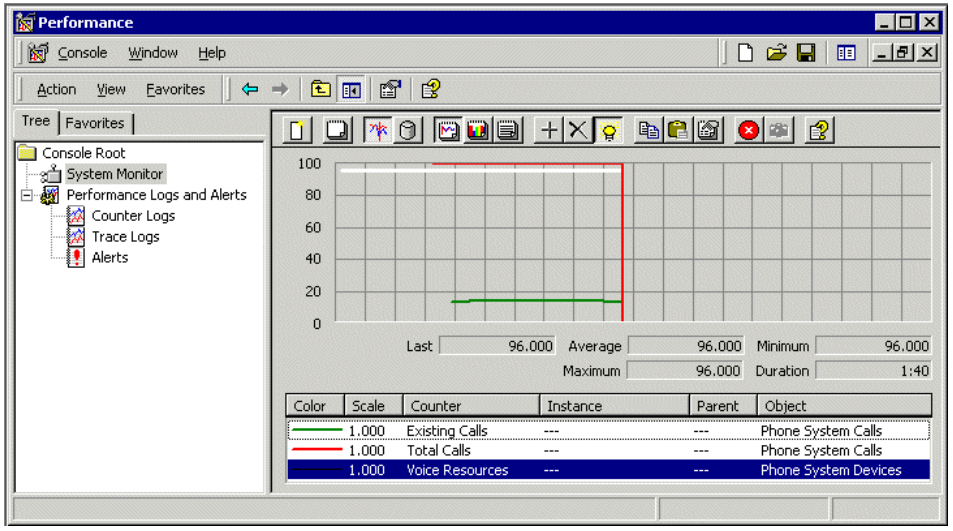
To add the Wave counters to the System Monitor display, right-click on the display and choose **Add Counters** from the shortcut menu. In the Add Counters dialog box, choose one of the Wave groups from the **Performance object** drop-down list.



As shown in the next figure, Wave performance counters for the group you have chosen are listed under **Select counters from list**. To add a counter, select it from the list and click **Add.** Repeat this process for each counter that you want to display. When you have selected all of the counters that you want to view, click **Close**.



The counters you have selected are listed below the performance graph in the main System Monitor window.



Archiving call recordings and voice mail

If you record all calls or even a significant portion of calls, or if you have users with thousands of saved voice messages and large maximum mailbox sizes, disk space on the Wave ISM can quickly fill up with voice messages and call recordings. In addition, ViewPoint performance will suffer when managing thousands of recordings, or when recordings are being delivered to the user in quick succession.

To handle thousands or even millions of recordings effectively, Wave lets you archive mailbox recordings (voice mail and call recordings) to a network directory of your choice, called the archive folder. Archiving moves the mailbox recording as well as all information about the recording from the Wave ISM to the archive folder, so archived voice messages and call recordings no longer appears in ViewPoint.

Users can then search for and manage archived recordings using the Wave Archived Recording Browser without burdening the Wave ISM, Wave database, or ViewPoint.

You can restore archived recordings to the mailbox of origin or export them to another location. (When an archived recording is restored or exported, it remains in the archive

folder until purged.) For more about managing and listening to archived recordings using the Wave Archived Recordings Browser, see Appendix E in *Vertical Wave User's Guide*.

This section describes how to do the following:

- Configure the Recording Archive Service. See page 23-37. (For installation steps, see Chapter 15 in *Vertical Wave Installation Guide*.)
- Start and stop the Recording Archive Service. See page 23-39.
- Archive mailbox recordings automatically and manually. See page 23-40.

About the Wave Recording Archive Service

The Wave Recording Archive Service, which manages the archive process, runs on the archive server, a separate PC from the Wave ISM. By off-loading archive processing, the Recording Archive Service can handle the resource-intensive archiving process without impacting Wave performance, and can also archive mailbox recordings from multiple Wave ISMs.

About mailbox recording file formats

You can archive mailbox recordings in any of the following formats. You can specify which format to use on a user-by-user basis (see "Archiving mailbox recordings" on page 23-40.)

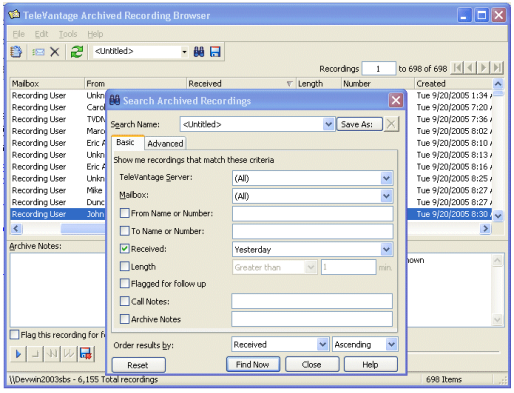
- .VOX is Wave's native format. (.VOX size = 64 Kbps, 469 Kb / minute.)
- .WAV format is commonly used by Windows applications such as Windows Media Player, which cannot play .VOX files. (.WAV size = 64 Kbps, 469 Kb / minute.)
- .MP3 is a popular format that consumes less disk space than .VOX files because of its very high compression rate. The compression rate makes it consume a significant amount of CPU and time when converting files into it. (.MP3 size = 20 Kbps, 146 Kb / minute.)

Note: When you archive using .VOX format, mailbox recordings are simply copied to the archive location. When you archive in .WAV or .MP3 format, each recording is converted from .VOX to the other format as it is copied to the archive folder, so using .WAV or .MP3 format may make archiving slightly slower. Archiving a mailbox

recording in .MP3 format results in the smallest file size, about one-third the size than if you archived the same recording in .VOX or .WAV format (.VOX and .WAV formats result in files of the same size.)

Searching and acting on archived recordings

You use the Wave Archived Recording Browser to search and manage archived recordings.



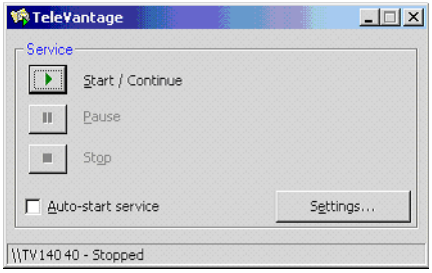
To use the Archived Recording Browser, you log on using an archive browser user name and password. Archive browser users do not necessarily correspond to Wave users, and you do not have to create an archive user browser for each Wave user who needs to search for and act on mailbox recordings. Multiple Wave users can log on to the Archived Recording Browser simultaneously using the same archive browser user name and password.

Typically, you create archive browser users with different levels of access rights, and then provide the appropriate archive browser user name and password to those Wave users who need to use the Archived Recording Browser.

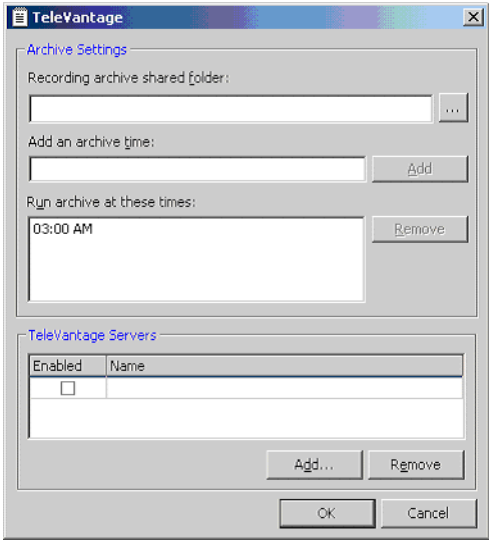
For details on how to use the Archived Recording Browser to search for and act on mailbox recordings, or to import a recording archive from Wave ISM 1.0, see Appendix E in *Vertical Wave User's Guide*.

Configuring the Recording Archive Service

1 To configure the Wave Recording Archive Service, choose **Start > Programs > Vertical Wave > Wave Recording Archive Service Manager.** The Wave Recording Archive Manager opens:



2 Click **Settings**. The Wave Recording Archive Service Manager Settings dialog box opens:



3 To specify the **Recording archive shared folder**, Click ... and browse to the archive folder you created (see Chapter 15 of *Vertical Wave Installation Guide*). The archive folder is a network folder where mailbox recordings are archived, that must be shared with full read / write permissions to any user who wants to access the recordings. If you are archiving mailbox recordings from multiple Wave ISMs, all ISMs archive to individual subfolders within the archive folder.

4 Specify the time when mailbox recordings will be archived automatically. (The default archive time is 3:00 AM.) You can specify additional archive times if you need to archive more frequently.

Under **Add an archive time**, enter the time using the format `hh:mm AM` or `PM` and then click **Add** to add it to the **Run archive at these times** list.

To remove an archive time from the list, select it, and then click **Remove**.

5 To add a Wave ISM to the list of ISMs from which mailbox recordings will be archived, click **Add**, and then browse to the ISM that you want to add.

When you specify multiple Wave ISMs for archiving, archiving occurs on one ISM at a time, in the order that the ISMs are specified here. Once archiving completes on one ISM, it starts on the next ISM in the list. Mailbox recordings from all of the ISMs are archived to the same archive folder.

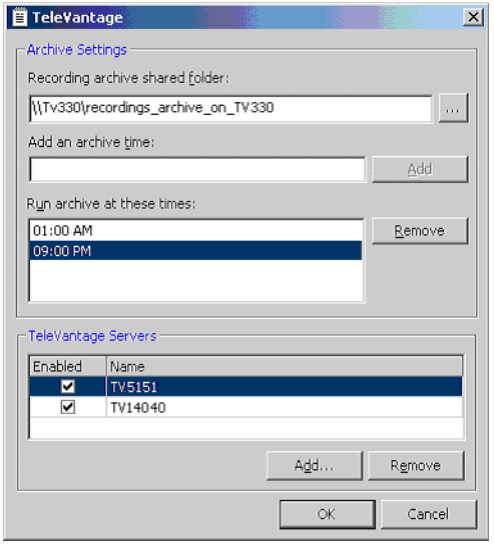
Note: Each Wave ISM name that you specify here is used to populate the **Archiving server** field on that Server's Recording \ Archive tab (**Tools > System Settings** in the User / Workgroup Management applet.) For details, see Section "Message 'Wave Recording Archive Service has not been configured to archive this server' when starting the Global Administrator on the Wave Server" in Appendix B in *Vertical Wave Installation Guide*.

To permanently remove a Wave ISM from the list, select it and then click **Remove**. Once removed from the list, you cannot automatically or manually archive mailbox recordings from that ISM. To temporarily prevent mailbox recordings on a specific ISM from being archived, see the next step.

6 Select the **Enabled** checkbox for each ISM that you want to archive automatically.

Note: If **Enabled** is not checked, mailbox recordings will not be archived automatically on the ISM, but you can still perform manual archives according to the instructions in "Archiving mailbox recordings manually" on page 23-42.

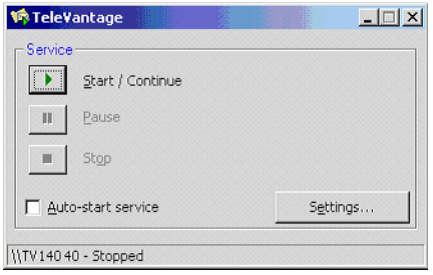
7 Click **OK** to save your changes.



Starting and stopping the Wave Recording Archive Service

Caution: *The Recording Archive Service must be running on the archive server in order for an automatic or manual archive to occur. It is recommended that you set the Recording Archive Service to auto-start according to the following instructions.*

1 On the archive server, choose **Start > Programs > Vertical Wave > Wave Recording Archive Service Manager.** The Wave Recording Archive Manager opens:



2 Use the buttons to **Start/Continue**, **Pause**, or **Stop** the Recording Archive Service manually.

Note: If you pause the Archive Recording Service, scheduled or manual archives will not start until you click **Start/Continue** and the Service is running again. If you click **Pause** while a scheduled or manual archive is in process, the Service will show a status of **Pause Pending** until the archive has completed. The status of the Service will then automatically be set to **Paused**.

3 Select the **Auto-start service** checkbox to start the Recording Archive Service automatically whenever the Wave ISM starts.

Archiving mailbox recordings

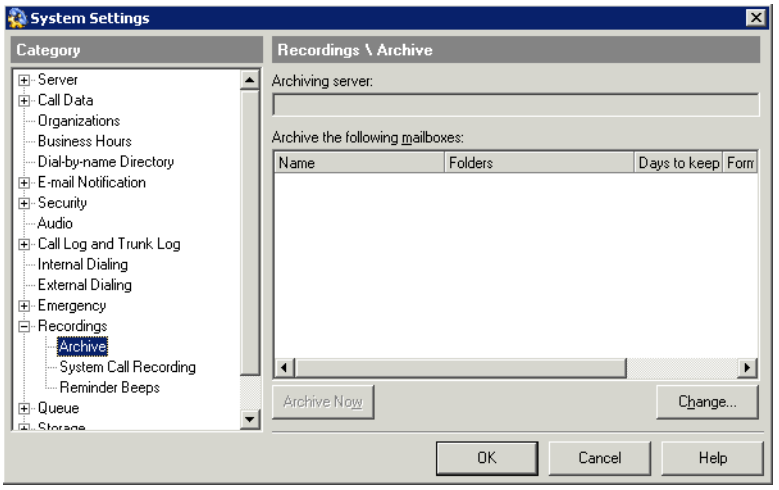
You can archive mailbox recordings automatically according to the settings in the Recording Archive Service Manager, or archive manually at any time. You can modify the mailbox archive settings for an individual user when you set up the archiving event.

Archiving mailbox recordings automatically

Use the User / Workgroup Management applet to configure automatic archiving for various mailboxes according to the following steps.

To archive mailbox recordings automatically:

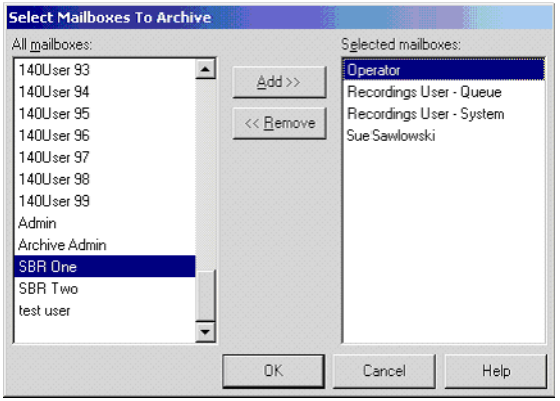
1 Choose **Tools > System Settings**. When the System Settings dialog box opens, choose the Recordings \ Archive tab.



The **Archiving server** field is blank until you configure the Recording Archive Service to include the list of Servers from which mailbox recordings will be archived, according to the instructions in “Configuring the Recording Archive Service” on page 23-37.

Note: If you set up automatic archiving according to the following steps, archiving will not occur if **Archiving server** is blank, and a message will be displayed to that effect each time you start the User / Workgroup Management applet.

2 The **Archive the following mailboxes** list shows the users whose voice mailboxes will be automatically archived. To add users to the list or change the users listed, click **Change**. The Select Mailboxes To Archive dialog box opens.



3 Users in the **Selected mailboxes** list will have their mailbox recordings automatically archived. Use the **Add** and **Remove** buttons to modify the list. Click **OK** to return to the Recordings \ Archive tab.

4 To modify the mailbox archive settings for an individual user, click the following columns for the user in the **Archive the following mailboxes** list:

- **Folders.** Select which of a user's folders to archive from the drop-down list:
  - **Inbox only.** Only mailbox recordings in the user's Inbox are archived.
  - **All folders except Deleted.** All the user's mailbox recordings are archived, including those in custom folders. Mailbox recordings in the user's Deleted folder are not archived.
- **Days to keep.** Enter the number of days that the user's recordings remain in the database before being archived.
- **Format.** Select whether to archive the user's audio files as MP3, VOX, or WAV files.

5 Click **OK**.

Archiving mailbox recordings manually

At any time, you can manually archive all mailbox recordings selected for automatic archiving, or a single user's or queue's mailbox recordings. (You can archive a single user's recordings even if the user is not already included in the selected mailbox list used for automatic archiving.)

Use the User / Workgroup Management applet to archive mailbox recordings manually according to the following steps.

To manually archive all selected mailbox recordings:

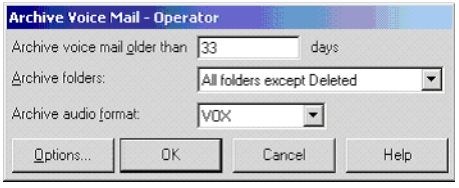
1 Choose **Tools > System Settings**. The System Settings dialog box opens.

2 Choose the Recordings \ Archive tab.

3 Click **Archive Now**. Wave archives all selected mailbox recordings already specified on the System Settings dialog box, Recordings \ Archive tab (see page 23-40.)

To manually archive a single user's or queue's mailbox recordings:

1 In the Users view, select the user and choose **Users > Archive Mailbox Recordings**. For a queue, select it in the Queues view and choose **Queues > Archive Mailbox Recordings**. The Archive Voice Mail dialog box opens.



2 Modify any of the following settings:

- **Archive voice mail older than ___ days.** Enter in days which mailbox recordings you want to archive now.
- **Archive folders.** Select which of a user's folders to archive from the drop-down list:
  - **Inbox only.** Only mailbox recordings in the user's Inbox are archived.
  - **All folders except Deleted.** All the user's mailbox recordings are archived, including those in custom folders. Mailbox recordings in the user's Deleted folder are not archived.
- **Archive audio format.** Select whether to archive the user's audio files as MP3, VOX, or WAV files.

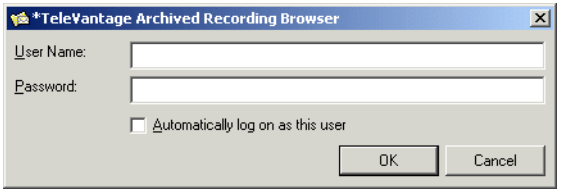
3 Click **OK** to start archiving the user's mailbox recordings.

Configuring who can manage archived recordings

You can configure one or more Archive Recording Browser user accounts. You might create multiple accounts, each with different privileges to manage recordings. Each account can be shared by multiple users. For instructions on installing the Archive Recording Browser, see *Vertical Wave Installation Guide*.

To add new archive browser users:

1 Start the Archived Recording Browser by choosing **Start > Programs > Vertical Wave > Wave Archived Recording Browser**. The Wave Archived Recording Browser dialog box opens:

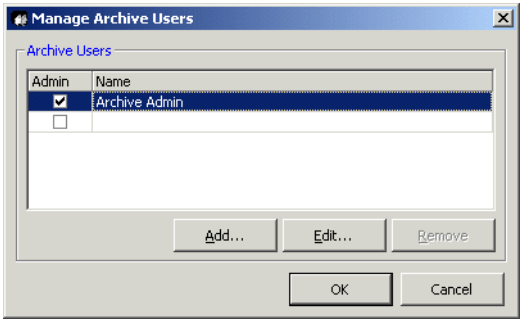


2 If you are running the Archived Recording Browser for the first time, enter a **User Name** of `Archive Admin`, leave the **Password** field blank, and then click **OK**. Otherwise, log in as any archive browser user with Archive Admin privileges.

Close the Search Archived Recordings dialog box when it opens.

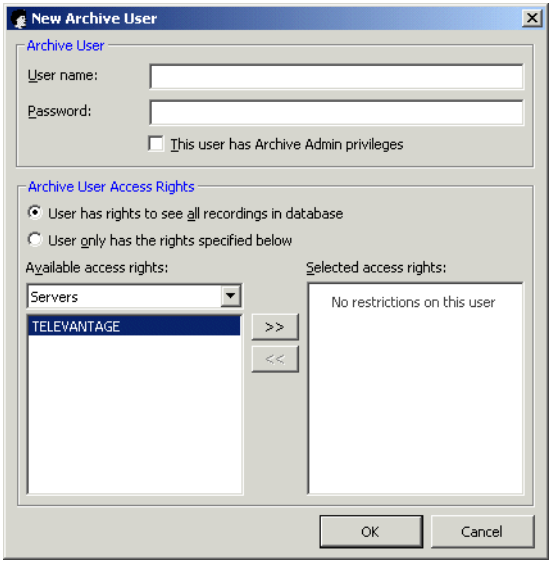
Note: Be sure to change the default password for the Archive Admin user for improved security.

3 In the Archived Recording Browser, choose **Tools > Manage Archive Users**. The Manage Archive User dialog box opens:



4 Password-protect the default Archive Admin user. To do so, select the Archive Admin user, and then click **Edit**. In the Edit Archive User dialog box, enter a **Password** and then click **OK** twice to save the new password.

5 To add another archive browser user, in the Archived Recording Browser, choose **Tools > Manage Archive Users**, and then click **Add**. The New Archive User dialog box opens:



6 Enter the **User Name** and **Password** for the archive browser user. These do not have to be the user's Wave user name and password (see "Searching and acting on archived recordings" on page 23-36 for more about archive browser users.)

7 Optionally, check **This user has Archive Admin privileges** if you want the user to be able to add, edit, or delete archive users, or create other Archive Admin users.

8 Click one of the following to specify the user's access rights.

- **User has rights to see all recordings in database.** Select this option if you want the new user to be able to view and act on all archived mailbox recordings. Click **OK** and then go to step 10.
- **User only has the rights specified below.** Select this option to limit the new user's access rights to only the options you specify in the next step.

9 Select one of the following from the drop-down list:

- **Servers.** If given access to a Wave ISM, the user can search and manage only the mailbox recordings that were archived from the specified ISM.

- **Archived Mailboxes.** If given access to an Archived Mailbox, the user can search and manage only the mailbox recordings that were archived from the specified Mailbox.
- **Users and Contacts.** If given access to a user or contact, the user can search and manage all archived voice messages and call recordings involving the specified user or contact.

To give the user an access right, select it in the **Available access rights** list, and then click >> to add it to the **Selected access rights** list. Repeat this step to give the user all of the access rights required. To remove an access right, select it in the **Selected access rights** list and then click << .

10 When you are done setting the user's access rights, click **OK**.

11 Add any additional archive browser users by repeating steps 5-10.

Using the Wave Archive Recording Browser

For instructions, see Appendix D of *Vertical Wave User's Guide*.

Monitoring database and disk usage

Wave's database stores your system configuration settings (information about trunks, users, auto attendants, and so forth), the Call Log, and an index to voice prompts, greetings, voice titles, and voice message files in a database. The voice files themselves are stored separately on disk.

Tasks associated with monitoring database and disk space include:

- Allocating database space
- Allocating disk space

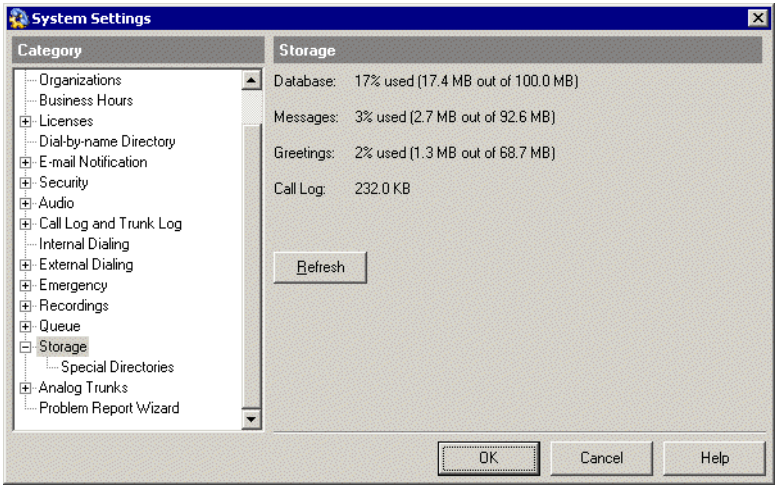
See *Vertical Wave Installation Guide* for information on the limits of MSDE and SQL Server databases.

Viewing storage statistics

To view how much of the available space your system is currently consuming, do the following:

1 Choose **Tools > System Settings**. The System Settings dialog box opens.

2 Choose the Storage tab.



The tab provides the following storage information:

- **Database.** Percentage of disk space allocated for the Wave database that is currently used, also shown in kilobytes used out of the total number of kilobytes allocated. The size of the Wave database is set and the required disk space allocated when the Wave ISM is installed. The default database size is 100 MB. It will grow automatically up to a maximum of 2 GB if you are using the MSDE database, or to the size of your hard drive if you are using SQL Server Standard or Enterprise editions. See *Vertical Wave Installation Guide* for supported databases and requirements.

  When you start the User / Workgroup Management applet, Wave displays a warning message if the Wave database is 80% or more full. You should check the database usage periodically to make sure that you are not running out of space. You will also automatically receive e-mail notifications of low space if you have set up Windows Event Log notifications (see “Setting up Wave Event Log notifications” on page 23-13).

- **Messages.** Percentage of disk space allocated for all users’ voice mail messages, as well as any call recordings users have made, that is currently used.

- **Greetings.** Percentage of disk space allocated for all users’ greetings and voice titles that is currently used.

- **Call Log.** Amount of space currently used in the Wave database for Call Log records, in kilobytes. Some or all of this space can be recovered by archiving Call Log information if total database usage is high (see "Archiving the Call Logs" on page 23-48).

Click **Refresh** to refresh the tab with current data.

Archiving the Call Logs

Over time, Call Log information will begin to fill up your Wave database. To recover database space, you can archive old Call Log information that is no longer needed to a location outside the database.

Caution: *Archived information is permanently removed from the Wave database. You cannot run Call Center reports on the time period that has been archived.*

Call Log information is written to a comma-separated value (.CSV) text file that can be read by most spreadsheet and database applications. The default path is `C:\Program Files\Wave Server\Archive\Calllog.csv`..

You can archive Call Log data in the following ways:

- Set up automatic archiving, which takes place at 1:00 a.m. every day.
- Automatically overwrite the Call Log after a number of days that you specify.
- Perform a manual archive on an as-needed basis, in addition to daily automatic archiving. You can do a manual archive whether or not automatic archiving is turned on.

You do not need to stop the Wave ISM or any other Wave components to perform an archive. However, because archiving is database-intensive, you may want to perform it during off-peak hours so that it does not affect normal system operation.

To archive Call Log information:

1. Choose **Tools > System Settings**. The System Settings dialog box opens.
2. Choose the Call Log > Archive tab.
3. Use the following fields to specify how you want to perform archiving:

- **Archive Call Log daily.** If checked, the Call Log is archived automatically at 1:00 a.m. every day. If unchecked, the log will continue to grow unless you manually archive it.
- **Archive calls older than ___ days.** Number of days a call remains in the Call Log until it is archived.
- **Archive file name.** Locations of the Call Log archive file on the Wave ISM. The file is in .CSV format and can be viewed with most spreadsheet or database applications.
- **Overwrite archive every ___ days.** Number of days that archived information will be appended to the Call Log archive file. After that number of days, archived information in the file will be deleted and the file will be reused.
- **Archive will be overwritten on.** Date and time that the Call Log archive file will next be overwritten and the data in it deleted. To preserve the archived data, back up the file just before it will be overwritten.

4 Click **Archive Now** to manually archive the Call Log according to the settings specified above. The archive begins immediately and may take several minutes to complete. You cannot perform any other Global Administrator functions until the archive completes. You can perform a manual archive at any time whether or not automatic archiving is turned on.

5 Click **OK** to save your archiving settings.

Note: Use the Import and Export Wizard (see "Exporting the Call Log" on page 23-11) to create a file containing Call Log information without removing the information from the database.

Changing special Wave directories

You can change the location where Wave stores the following important components on disk:

- The database.
- The database transaction log.
- The database backup.
- Voice files.

Note: You must shut down the Wave ISM before changing the location of special directories.

To change special Wave directories:

1. Choose **Tools > System Settings**. The System Settings dialog box opens.
2. Choose The Storage \ Special Directories tab.
3. Click **Move** next to a component to specify a new location for that component.
4. When you are done changing special directory locations, click **OK**.

Identifying security risks

You can analyze your system for potential security risks by choosing **Tools > Analyze Security**. For more information on system security, see Appendix A.

Capturing network troubleshooting logs

By default, Wave continually captures network traffic information and writes it to logs that can help simplify the troubleshooting of client / server or voice-over-IP communications issues.

Network capture logs capture the following protocols:

- Session Initiation Protocol (SIP).
- Realtime Transport Protocol (RTP), turned off by default.
- Trivial File Transfer Protocol (TFTP)
- Address Resolution Protocol (ARP)
- Internet Control Message Protocol (ICMP)
- Transmission Control Protocol (TCP) (H.225, H.245)
- Microsoft Distributed Component Object Module (DCOM)
- Dynamic Host Configuration Protocol (DHCP)
- Bootstrap Protocol (BootP)
- Domain Naming System (DNS)

When network capture is enabled, a separate series of log files is written for each network interface card (NIC) in the Wave ISM PC. By default, each series consists of 20 files of 32 mb each, that are continually overwritten starting with the oldest. The logs are written to the ISM's log directory, typically C:\Program Files\Wave Server\Logs. The filenames of the captured traces are in the format `Tv_cap_nnnnnnnnnnnn_00xx.cap`, where `nnnnnnnnnnnn` represents the last 12 digits of the WinpCap NIC ID, and `00xx` represents the capture number (for example, 0001, 0002 ...0020). For example: `Tv_cap_1E2F3B4A5C85_0010.cap`.

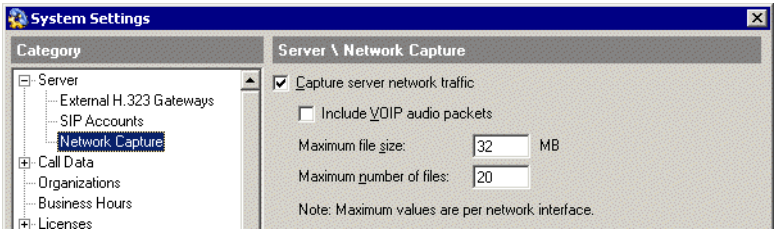
Note: Network capture logs are not included in the problem report package created by the Problem Report Wizard (described on page 23-52.) You must manually gather and submit network capture logs as directed by your Wave provider.

Adjusting or turning off network capture

In the User / Workgroup Management applet, you can adjust the number and size of the log files or files or turn off network capture completely.

To adjust or turn off network capture:

1. Choose **Tools > System Settings**.
2. Click the Server \ Network Capture tab.



3. To disable network capture, uncheck **Capture server network traffic**.
4. If **Capture server network traffic** is checked, adjust any of the following options:
   - **Include VOIP audio packets.** Check to have the logs capture the audio portion of Voice-over-IP calls (RTP protocol.) This option is turned off by default because it can cause network capture files to fill up quickly. Select this option only if you are experiencing problems with voice quality issues on VoIP calls.
   - **Maximum file size.** Specify the maximum size of each log file before Wave increments the file number and begins creating a new log file.

- **Maximum number of files.** Specify the total number of log files that can be on the system at any one time. When that number is reached, Wave begins overwriting the existing log files starting with the oldest.

5 Click **OK**.

Reporting problems to your Wave provider

Use the Problem Report Wizard to report any problems you experience with Wave ViewPoint system to your provider for technical support.

Note: The Problem Report Wizard is used for ViewPoint-related problems only. To collect logs for troubleshooting the Wave ISM, see "Downloading Wave files" on page 24-13.

The Problem Report Wizard asks you to describe the frequency, patterns, and circumstances of the problem you are reporting. Based on the information you supply, the Problem Report Wizard isolates exactly when and where the problem occurred and automatically collects the appropriate Wave log files and other information from your computer. By assembling all the relevant information, the Wizard helps your provider quickly identify the problem and begin to solve it.

Note: For information about known issues and workarounds for currently reported problems, see the Known Issues topic in the online Help for the Wave Global Administrator.

Setting Problem Report Wizard defaults

You can set values for the Problem Report Wizard that will be automatically supplied as defaults whenever it is run. The user running it can always change the defaults.

To set Problem Report Wizard defaults:

1 Choose **Tools > System Settings**. The System Settings dialog box opens.

2 Choose the Problem Report Wizard tab.

3 Fill in any **Default information for the person reporting the problem**.

4 To set up a default status of e-mailing the Problem Report Package, check **Send package via e-mail by default** and specify the default **E-mail address**.

5 Click **OK**.

Reporting ViewPoint-only problems

For problems with ViewPoint, run the Wizard on the computer that is experiencing the problem.

Examples of ViewPoint problems include:

- ViewPoint behaves unexpectedly.
- User cannot connect to the network.
- User cannot connect to the Wave database.
- ViewPoint does not start.
- ViewPoint closes unexpectedly.
- Data or commands executed in ViewPoint don't look or behave properly.

To report a workstatio:n application problem

1 On the computer that is experiencing the problem, choose **Start > Run**. Enter the following path and then click **OK**. The path on your system may be different.

```
C:\Program Files\Common Files\Vertical\Wave\TVPRwizard.exe
```

Alternately, to report a problem with a specific call or voice message, select the problem call (or the call that left the problem message) in the Call Log view and choose **Actions > Report a Problem**. The Problem Report Wizard starts with information about the call already entered.

2 Answer the questions presented in each Wizard window.

Reporting ViewPoint-Server problems

For problems that occur with both ViewPoint running on a user's computer and the Wave ISM (such problems usually involve the ViewPoint Call Monitor view), run the Wizard on the user's computer. Then collect ISM logs as described in "Downloading Wave files" on page 24-13.

Examples of distributed problems include:

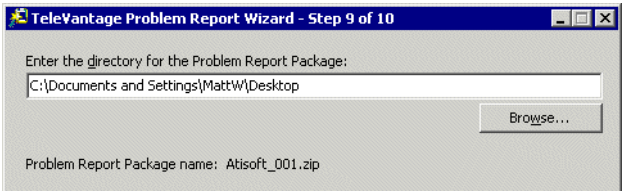
- Problems with specific calls in ViewPoint.
- Problems with specific voice messages in a ViewPoint Voice Messages folder.
- Call-handling problems that involve ViewPoint or the ISM (calls cannot be conferenced, for example).
- User cannot make outbound calls from ViewPoint.

The problem report package

The problem report package is a single .ZIP file. It contains all the information gathered about the problem by the Problem Report Wizard. The Wizard saves the problem report package to the location you specify.

The Wizard summarizes the information reported, including the date and time the report was created, in a `ProblemInfo.txt` file within the .ZIP file. You can open a .ZIP file with any zip utility (for example, WinZip).

To prevent problem report packages from being overwritten, the Wizard gives each one a unique name based on your company name and a sequence number.



E-mailing the Problem Report Package

Optionally, you check **Send Problem Report Package via e-mail** in the final window to e-mail the problem report package to a destination of your choice. Because a problem report package can be large, after you send you should delete it from your system to regain disk space.

Running the Problem Report Wizard from the command line

You can run the Problem Report Wizard without having a Wave application open by running it from the command line. This can be useful for automatically creating

scheduled Problem Report Wizard captures using the Windows scheduling service. Run the file `TVPRWizard.exe`, located in C:\Program Files\Common Files\Vertical\Wave. You can run the file in the following ways:

- To run the PRWizard normally, specify `\createcab:Yes`. The PRWizard runs with whatever parameters you specify.
- To run the PRWizard automatically, do not include the `\createcab` parameter. The PRWizard runs in the background, with a progress bar showing.

When running the Problem Report Wizard from the command line, you can use any of the following parameters. All are optional.

Parameter	Description
/calllogentry:	Specified Call Log entry from the Global Administrator or ViewPoint
/stations:	List of stations involved
/clientpackage:	Full path and filename of a client package to include
/includedatabase:	If Yes, includes a database backup
/estimateddate:	Estimated date of occurrence
/estimatedtime:	Estimated time of occurrence
/exactdate:	Exact date of occurrence
/exacttime:	Exact time of occurrence
/rangestartdate:	Start date of log range
/rangestarttime:	Start time of log range
/rangeenddate:	End date of log range
/rangeendtime:	End time of log range
/summary:	Text summary of the problem
/reproducible:	Whether the problem is reproducible. Enter Yes, No, or Unknown.
/details:	Text describing details of the problem
/contactname:	Name of contact at your company

Parameter	Description
/contactcompany:	Your company
/contactphone:	Your contact phone number
/contactemail:	Your contact email address
/supportname:	Name of your support contact
/supportissue:	Support issue number
/packagepath:	Directory in which to place the .ZIP file
/packagefile:	Filename of the .ZIP file
/mailpackage:	Whether the package should be e-mailed (not applicable if /createcab is set to Yes)
/createcab:	If Yes then the .ZIP file creation will begin automatically
/maxevents:	Maximum number of Event Log events per Event Log type
/cabpriority:	Process priority for cabarc. Enter Normal, Idle, High, Realtime, Below_normal, or Above_normal.

Continuing System Administration

CHAPTER CONTENTS

This chapter provides background and step-by-step procedural information for performing general administrative tasks and monitoring system performance.

Restoring your system configuration

Use System Backup / Restore to restore Wave to the configuration it had when you last did a backup if a power loss has corrupted the database. The restore operation restores from the last backup cabinet (CAB) file located in C:\inetpub\ftproot\private\iocabfiles.

Note: You can only restore a system of the same version number as your current system.

To restore Wave:

1 Manually restore the following items:

- Network Adapters and Settings (including host name / machine name, setting the TCP / IP domain, and IP Address / Subnet Mask / Gateway per adapter. Adapters include: Integrated Services Card, 10 / 100Base-T Ethernet)
- Wave account user names and passwords in the Password Administration applet.
- The system date, time, and time zone in the Date and Time applet.
- RAID-1 Configuration (disk mirroring).
- Windows Workgroup or Network Domain

2 If you are restoring from a backup CAB file that was saved in a place external to the Wave ISM, make sure that the backup CAB file (Iobackup.cab) appears in the C:\inetpub\ftproot\private\iocabfiles directory on your Wave ISM.

If this directory does not exist, create it and copy or FTP the CAB file into the directory.

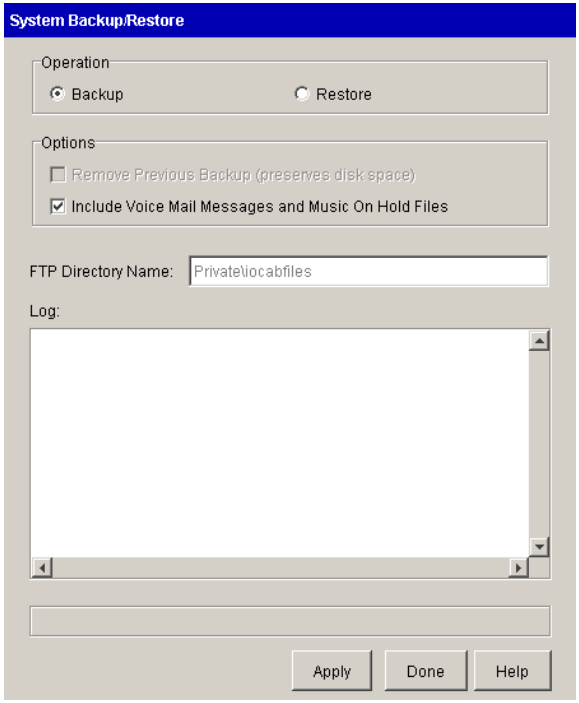


Figure 24-1 System Backup / Restore applet

3 Select Restore.

4 Check Include Voice Mail Messages and Music on Hold Files to restore the Voice Mail messages and Music on Hold WAV files from the backup file.

5 Check Include Call Navigator Prompts to restore Call Navigator prompt files from the backup file.

6 If necessary, click the Administration tab of the Management Console.

Click

7 Click the System Backup / Restore icon, located in the General Administration section.

8 Click Apply.

9 Click Yes to confirm the Restore operation.

Detailed results of the operation will appear in the Log.

10 Click OK at the end of the restore process to reboot the Wave ISM.

Restoring network settings after using the Vertical Wave Deployment Disk

In the event that you need to use the Vertical Wave Deployment Disk that came with your system, you will need to restore your customized settings using the System Backup / Restore applet with a previously created backup file. In some cases, you may need to manually reconfigure your network settings and adapter information.

After you have restored your settings using the System Backup / Restore applet (see "Restoring your system configuration" on page 24-1), a log displays in the applet that provides information about the Restore action. If Wave could not restore your network adapter information successfully, the log will include the following error message:

```
Error: Cannot Restore Network Adapters
```

If the error message does not appear in the log, then Wave successfully completed the restore operation and you do not need to manually reconfigure your network settings.

To restore your network settings:

1 Print or write down the network settings information in the log file.

The information in the log that you will need looks like this, but has values specific to your Wave ISM.

```
Hostname=EastCoastIO
Domain=domain.com
NameServer=192.168.1.2 192.168.1.3
SearchList=domain.com
[(Slot 6 + 5) 10/100 Base-T Ethernet Integrated Services Card
   3]
IPAddress=192.168.75.4
DefaultGateway=192.168.75.1
SubnetMask=255.255.255.0
Primary WINS=192.168.1.2
Secondary WINS=192.168.1.3
[[Unknown, DLCI 16] Untitled]
IPAddress=192.168.74.1
DefaultGateway=
SubnetMask=255.255.255.0
Primary WINS=
Secondary WINS=
```

2 Follow the instructions in “Identifying your Wave ISM on the LAN” on page 3-2, to reconfigure your system name and IP addresses for each of your network adapters with the information in the log.

Upgrading the Wave software

This section addresses upgrading Wave software with major releases. For information about applying HotFixes and Service Packs refer to the documentation accompanying your HotFix or Service Pack. For information about downgrading software and deleting backups refer to the Management Console Help system.

A compressed archive of all the upgrade-install files is contained in a cabinet (CAB) file. Obtain an upgrade CAB file in the following ways:

- Receive an upgrade on CD or DVD
- Download an upgrade from the Vertical Communications Web site (www.vertical.com)

The upgrade procedure has two parts:

- Uploading files
- Upgrading

You can choose to do both at once, or you can upload at one time (for example, your lunch hour), and upgrade at another (for example, after 6 P.M.).

Uploading files

Uploading does not interrupt Wave services, including the telephone or data systems. Since upload time is based on file size, uploading files using your browser over the LAN can take up to an hour. Upgrading from the Vertical Communications Web site generally takes about three times as long as upgrading from a CD-ROM or DVD.

When you upload the file using a Web browser, a spinning icon is your only status indicator. Unless your Web browser reports an error, the file upload is probably working fine. Do not interrupt the upload.

If you are planning to upgrade over a modem, be sure to check the size of the upgrade CAB file. Uploads will take the longest over a modem. For example, if the upgrade

CAB file is 20 MB, expect a two-hour upload. For this reason, only small HotFixes should be uploaded using a modem.

Upgrading

The automated upgrade procedure unpacks files, starts the SNMP Alarms applet (which runs throughout the process so you can see the upgrade status), restarts the Wave ISM, copies files, restarts again, and verifies the upgrade. In addition, Wave may exercise an option to automatically break and restore the disk mirror with the redundant hard drive for subsequent upgrades, so that if the upgrade fails you can boot with your previous software version from the second drive.

Note: When you start an upgrade, the SNMP Alarm panel pops up and you can monitor the progress of your upgrade. If you have a browser pop-up blocker on your system, the SNMP Alarm panel is blocked and doesn't come up. You can usually configure these blockers to allow popups from specific domains and IP addresses.

The upgrade checks the Wave software versions only. It does not check individual file versions. The registry, Call Detail Report database, and files are backed up as they are replaced. If the upgrade is successful and Wave is fully functional, the setup files are removed.

If you have mirrored disks, use the Disk Management to verify the health of your disks before proceeding with an upgrade. For information about checking your disks using Disk Management, refer to “Identifying RAID disk health” on page 24-29.

Caution: *You cannot see any SNMP alarms during an upgrade unless trap destinations are configured in the SNMP Configuration applet. For instructions, see “Configuring SNMP agents” on page 24-16. In addition, be sure to run the Software Upgrade applet over the LAN or modem, as described in Figure 24-2, if you want to view SNMP status.*

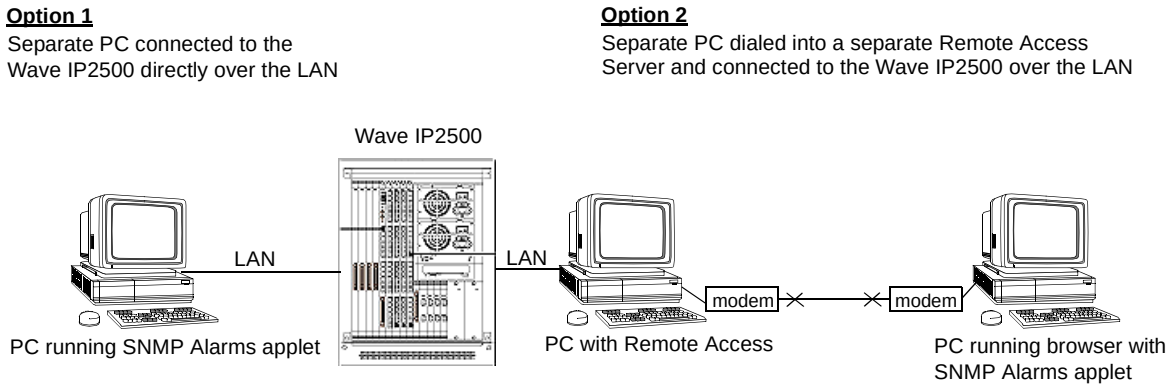


Figure 24-2 Options for viewing SNMP status

To upgrade from a CD or DVD:

1. Obtain a CD or DVD with the latest version of the upgrade CAB from Vertical Communications or an authorized distributor.
2. Insert the CD or DVD in the Wave ISM CD-ROM drive.
3. Log on to the Management Console.

   To upgrade Wave software, your user account must have permissions to the Software Upgrade applet.
4. If necessary, click the Administration tab of the Management Console.
5. Click the Software Upgrade icon, located in the General Administration section.

Click

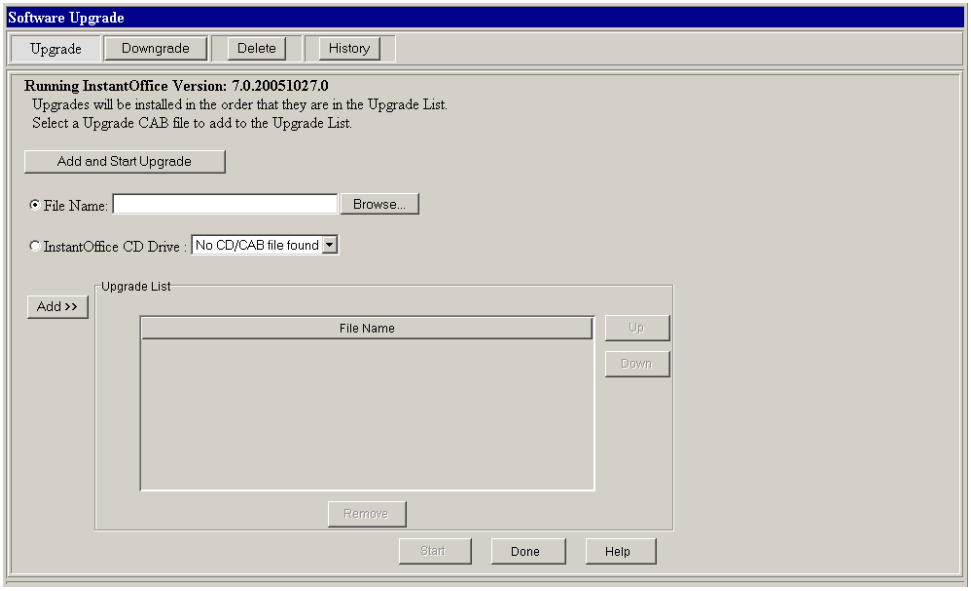


Figure 24-3 Software Upgrade applet

6 Click Upgrade.

7 Select the Wave ISM CD Drive option, and click Start.

The upgrade begins immediately. It takes approximately 45 minutes to unpack files, start the SNMP Alarms applet, restart, copy files, restart again, and verify the upgrade.

8 After the upgrade is complete, open a new instance of the browser to access the Management Console.

Note: If you have any problems accessing the Management Console after upgrading or restoring files, check the event log to make sure the Wave ISM is available on the network.

To upload files and upgrade:

1 Log on to the Management Console.

Click

2 If necessary, click the Administration tab of the Management Console.

3 Click the Software Upgrade icon, located in the General Administration section.

4 Select the File Name option.

5 Enter the path to the upgrade CAB file in the File Name field, or click Browse to find it.

6 Click Start.

The upgrade begins immediately. Depending on the size of the CAB file, it takes approximately 45 minutes to unpack files, start the SNMP Alarms applet, restart, copy files, restart again, and verify the upgrade.

To upload files and upgrade a later time

1 Log on to the Management Console.

2 If necessary, click the Administration tab of the Management Console.

Click

3 Click the Software Upgrade icon, located in the General Administration section.

4 Select the File Name option.

5 Enter the path to the upgrade CAB file in the File Name field, or click Browse to find it.

6 Click Add. This will upload the file and add the file to the Upgrade List. You can exit the Software Upgrade applet at this time and re-enter it later to start the upgrade.

7 Once you re-enter the upgrade applet, click **Start**. The upgrade begins immediately. Depending on the size of the .CAB file, it takes approximately 45 minutes to unpack files, start the SNMP alarms applet, restart, copy files, restart again, and verify the upgrade.

Downgrading

Downgrading your Wave software is not recommended. All backups are removed during an upgrade to prevent you from attempting a subsequent downgrade which could render Wave inoperable.

During the downgrade process, the SNMP Alarms applet provides status. As in the upgrade process, the Wave ISM is restarted twice while a downgrade is performed.

Caution: *When you downgrade to the software version that was originally shipped with your Wave ISM, you also replace your registry with the registry that was shipped with your Wave ISM. You will lose your configuration.*

To downgrade software:

1 Log on to the Management Console.

2 If necessary, click the Administration tab of the Management Console.

Click

3 Click the Software Upgrade icon, located in the General Administration section.

To downgrade your Wave software, you must log on with an Wave user account that has permissions to the Software Upgrade applet.

The Software Upgrade applet appears (see Figure 24-3).

4 Click Downgrade.

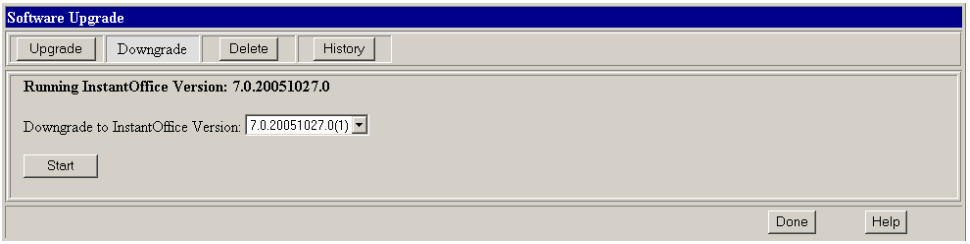


Figure 24-4 Software Upgrade applet, showing Downgrade options

5 Select the Wave version from the drop-down list.

If it is not possible to downgrade, no release will be listed.

6 Click Start.

A Downgrade Status message appears, and immediately afterwards, the SNMP applet appears so you can monitor the process of the downgrade.

Note: The downgrade procedure reboots the Wave ISM twice.

7 After your Wave ISM is back on-line, click Done in the Software Upgrade dialog box.

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Software Upgrade icon, located in the General Administration section.

Accessing the Fault Monitor error log

The fault monitor module stores copies of a subset of the system traces that are stored by the system trace manager, specifically those that are flagged as severe or fatal errors. The Fault Monitor main buffer is implemented as a circular buffer so that it always contains the most current traces. The buffer is 28 K bytes, and can contain around 250 traces, depending on the size of each trace. On each reboot, the entire contents of this buffer is saved to the file fmlog.*.txt, where the * represents the date and time the traces were saved. You can find the fmlog.*.txt files on the Wave ISM hard drive in the C:/Program Files/Wave/Logs directory.

If a bluescreen event occurs, the operating system bluescreen data generated by the bluescreen event is saved to the Fault Monitor bluescreen buffer. This data can be useful when troubleshooting the bluescreen event. This buffer is 4 K bytes, and will either be empty or contain the most recent bluescreen event. On each reboot, the entire contents of this buffer is saved to the file fmblu.*.txt, where the * represents the date and time the traces were saved. You can find the fmblu.*.txt files on the Wave ISM hard drive in the C:/Program Files/Wave/Logs directory.

The contents of these buffers are lost if the Wave ISM is powered off. In any situation where the Wave is non-responsive and you wish to preserve the contents of these buffers for later access, you should use the black reset button located on the Integrated Services Card. The Wave ISM should not be powered off so as to preserve the traces in the fault monitor buffers.

The fault monitor module must be connected to a dedicated analog trunk for dial-in access and pager notification to work. For information on connecting the fault monitor module to a trunk, refer to the *Vertical Wave Installation Guide*. For a full discussion of using the fault monitor once it is configured, refer to the *Vertical Wave IP 2500 Hardware Reference Guide*.

To view the Fault Monitor Error Log

1. If necessary, click the Administration tab of the Management Console.
2. Click the General Settings icon, located in the General Administration section.
3. Select the Fault Monitor tab.
4. Click the View Fault Monitor Error Logs button.

Click

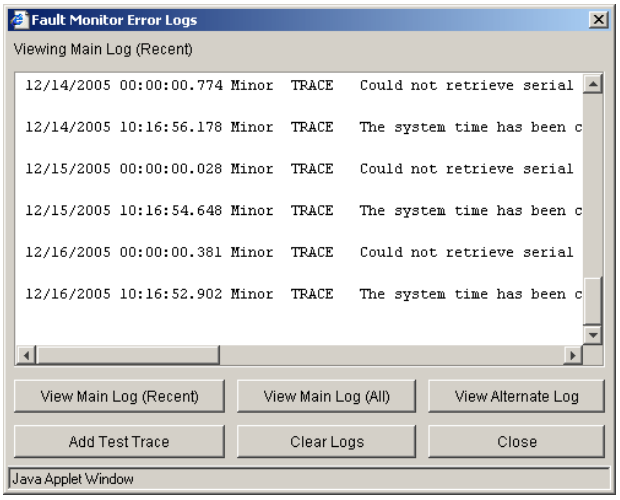


Figure 24-5 Fault Monitor Error Logs dialog

5 Click one of the following buttons to display the view you want:

- View Main Log (Recent)—displays the contents of the last 4K of the Main Log (default view)
- View Main Log (All)—displays the entire contents of the 32K Main Log
- View Alternate Log—displays the contents of the Alternate Log
- Add Test Trace—adds a test trace with an appropriate time stamp and the text `Management Console ==> Test trace` to the end of the Main Log. To view the test trace, click either View Main Log (Recent) or View Main Log (All)
- Clear Logs—clears the contents of the Main Log and Alternate Log. To verify that the logs have been cleared, click View Main Log (Recent), View Main Log (All), or View Alternate Log

6 Click Close to close the dialog and return to the General Settings applet.

7 Click Apply to save your changes.

8 Click Done to return to the Management Console.

Downloading Wave files

The Download applet is a diagnostic tool that allows you to download files from the Wave ISM to your workstation for inspection. Files are downloaded by sending them through FTP to the web browser on your workstation. The browser will prompt you to choose a location to save the files.

You can download files from one of the following categories:

- CMS Reports—reports and log files for Vertical Wave Fax Manager and Vertical Wave Service Response products
- Call Navigator Reports—reports and log files for Call Navigator
- Client Components—executables for distribution to client workstations
- Global Administrator History—log file for Management Console access
- System Backups—configuration backup CAB files and backup logs
- System Logs - Auxiliary—Wave ISM logs
- System Reports—daily archives from Call Detail Report and Trunk Statistics Report
- ViewPoint Data Provider Logs—Activity history for all ViewPoint database requests
- ViewPoint Data Provider Configuration and Components—Configuration settings for the ViewPoint Data Provider

To download Wave files:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Download icon, located in the General Administration section.

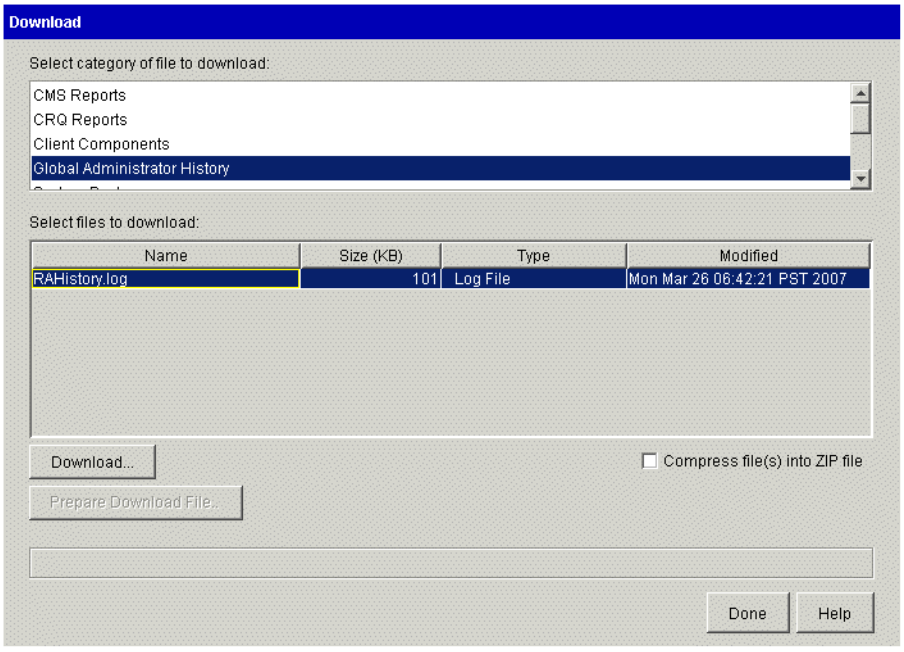


Figure 24-6 Download applet

3 Select a category from the top list.

4 Select a file or group of files from the file list.

5 Check the Compress file(s) into ZIP file check box to compress files using ZIP.

Note: If you select more than one file, the compression option is automatically selected.

6 Click Download.

7 Save the file to your local hard drive.

8 Click Done to return to the Management Console.

Setting the minimum free hard drive space notification limit

This option allows you to set a notification to warn you when there is between 50-400 megabytes of primary hard drive space left on your Wave ISM.

Note: You must be monitoring your Wave ISM with SNMP to benefit from this feature.

To set a minimum free hard drive space notification limit:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 Select the System tab.

4 Select a number from the Notify when less than ***n*** megabytes free drop-down list.

When your hard drive reaches the limit you set, an SNMP trap will be sent with the following message:

`Min Free Space=`*n*`. Current Avail Free Space=`*y*.

where *n* is the amount of minimum memory in megabytes you set, and *y* is the actual current available free space.

5 Click Apply to save your changes.

6 Click Done to return to the Management Console.

Configuring and using SNMP

Simple Network Management Protocol (SNMP) can be used to monitor and diagnose a Wave ISM, notifying you about any alarms and traps.

Using the SNMP Configuration applet, you can configure traps to notify specified clients about any unsolicited events and you can set up several levels of security. Using the SNMP Alarms applet, you can monitor current and review previous alarms. Wave supports the SNMP agents listed in Chapter 31, SNMP Agents.

All Management Information Bases (MIBs) reside on the Wave ISM in the C:\Program Files\SNMP\MIBs directory.

SNMP terminology

SNMP terminology used in the configuration applet is explained in Table 24-1.

Table 24-1 SNMP terminology

Term	Meaning
Community Name	Both the SNMP management system and SNMP agent must be members of a group so that SNMP messages can be passed between them. The logical name assigned to such a group can be any combination of alphanumeric characters, and is referred to as a *community name*. SNMP operations require a valid community name; up to seven community names can be specified. Community names, known only to registered users or administrators, provide the security required by SNMP SET operations. The globally known "public" can be used as a community name, but does not provide security. If no community is specified, all SNMP requests will be honored. The SNMP agent residing on the managed node accepts or rejects an SNMP request based on the community name contained in the request. For example, an agent configured with the community name "vertical" rejects all requests containing any other community name.
Host	The management system requesting SNMP information from this Wave ISM.
Trap	An unsolicited asynchronous message sent from an SNMP agent to a management system. Traps are typically sent by the agent when a predefined condition or event occurs. For details on such conditions and events, see Chapter 31, SNMP Agents.
Trap Community	The string encoded in a trap message (packet) by the agent; placeholder for trap destinations. Like community name, the trap community name can be any combination of alphanumeric characters; unlike community name, trap community names have nothing to do with security. "Public" is fine to use as a default.
Trap Destination	A specific network address (IP or DNS host name) to which a trap message is sent. Up to five trap destinations can be added for each trap community.

Configuring SNMP agents

You will typically access the SNMP Configuration applet (see Figure 24-7) to configure community names, trap destinations, and specific management (host) destinations. Once SNMP agents are configured:

- Users can view SNMP traps from the Wave ISM through the SNMP Alarms applet.
- Specified clients will be notified when SNMP traps occur.

To configure SNMP traps:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the SNMP Configuration icon, located in the General Administration section.

3 Enter information about a contact person for this Wave ISM.

You can enter a string of up to 255 characters in this field.

4 Enter information about the physical location of this Wave ISM.

You can enter a string of up to 255 characters in this field.

5 Select the Traps tab.

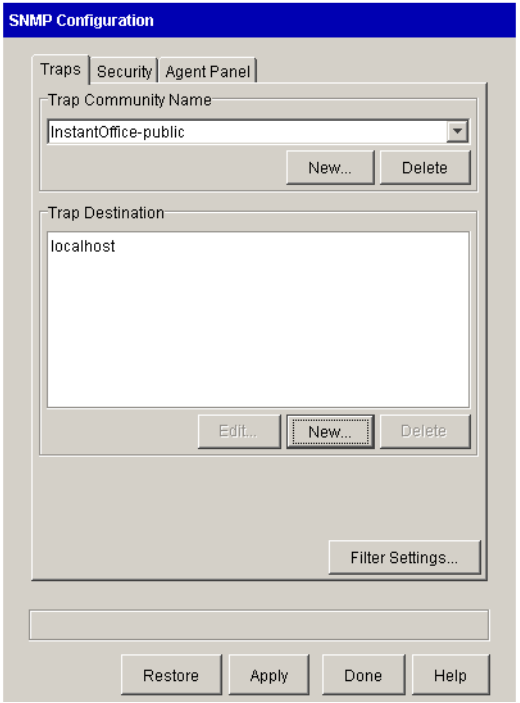


Figure 24-7 SNMP Configuration applet, showing Traps tab

6 Click New to add a trap community name.

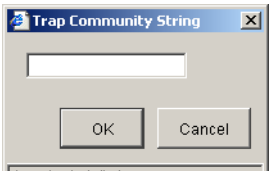


Figure 24-8 Trap Community String dialog

7 Type `InstantOffice-public`, and click OK.

You must have a valid trap community name in order to see SNMP alarms. Public is the default community string, but it can be changed.

8 Repeat steps 6 and 7 to add more trap community names.

To add a trap destination:

1 Choose a trap community name from the list.

2 Click New under Trap Destination.

The Trap Destination dialog appears (see Figure 24-9).

3 Type the DNS host name of the Wave ISM, and IP address of the trap destination, then click OK.

By default, the trap destination list includes localhost, which means that SNMP alarms will be returned to the Wave ISM you are configuring, and can be monitored via the SNMP Alarms applet in the Management Console.

4 Repeat to add more trap destinations.

Client machines listed as trap destinations receive SNMP traps, which can be viewed from the SNMP Alarms applet. All client destinations listed as trap destinations receive SNMP traps from this Wave ISM. The community name encoded in the trap message depends on which community the trap destination belongs.

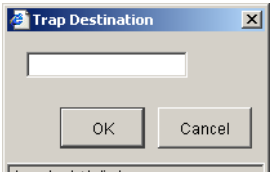


Figure 24-9 Trap Destination dialog

Configuring an SNMP trap filter

Using SNMP Filters, you can enable and disable specific groups (trap groups) of SNMP traps to filter the traps for network monitoring tools.

To filter SNMP traps:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the SNMP Configuration icon, located in the General Administration section.

3 Click the Filter Settings button on the Traps tab.

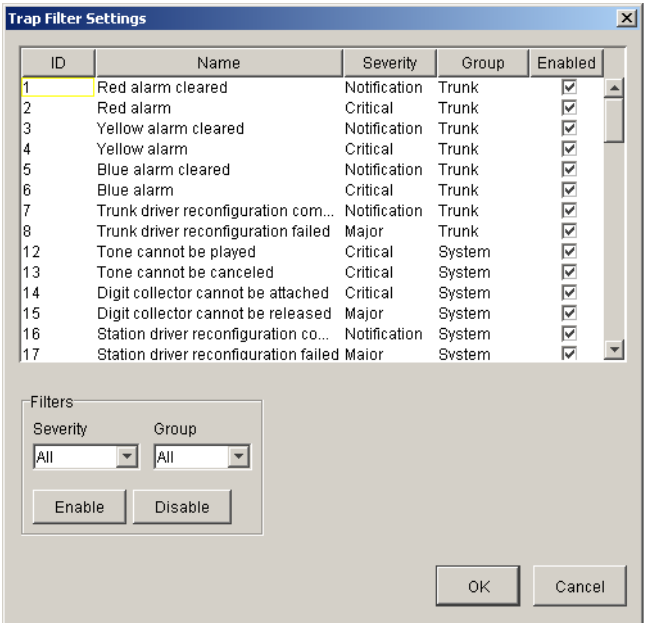


Figure 24-10 Filter Settings dialog

1 You can enable or disable traps by severity or by group using the Severity and Group drop-down lists and clicking Enable or Disable.

You can select All, Critical, Major, or Notification traps in the Severity drop-down list.

You can select All, System, Trunk, Upgrade, Hardware, OS, Data, and MSM from the Group drop-down list.

For those traps that are selected for filtering, the Enabled check box is checked.

2 Click OK.

3 Click Done to save your changes return to the Management Console.

Configuring SNMP security

To configure SNMP security:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the SNMP Configuration icon, located in the General Administration section.

3 Click the Security tab.

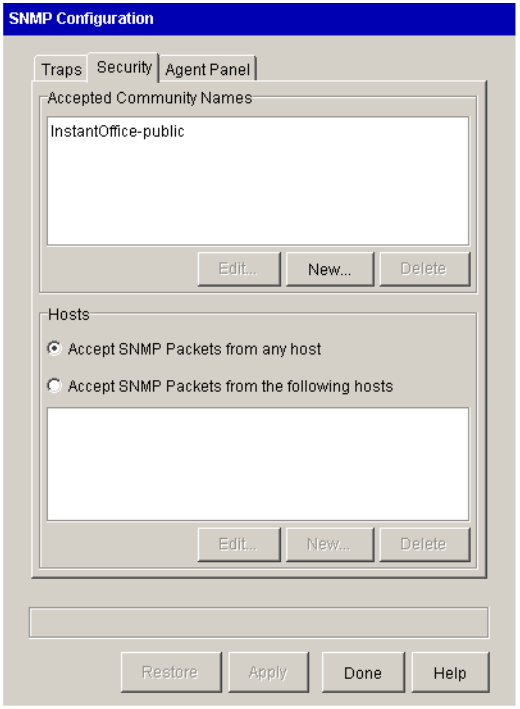


Figure 24-11 SNMP Configuration applet, showing Security tab

4 Click New to add an SNMP community name.

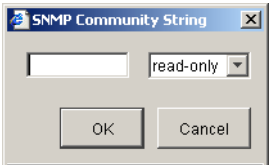


Figure 24-12 SNMP Community String dialog

5 Type a valid SNMP community name.

If no community name is specified, SNMP requests containing any community name are accepted. A certain level of security can be effected by setting the agent to allow another private community string. Up to seven such community names can be specified on the agent. SNMP requests will only be accepted if they contain one of the configured community names.

6 Specify if the community string is read-only or read-write using the drop-down list.

7 Click OK.

8 Repeat steps 4 through 7 to add more community names.

9 If you wish to specify that SNMP messages be accepted only from particular hosts:

- **a** Click the Accept SNMP packets only from the followings hosts option.
- **b** Click New.

  The SNMP Hosts dialog appears (see Figure 24-13).
- **c** Type the host name or IP address, and click OK.
- **d** Repeat to add more hosts.

  Naming particular hosts adds another level of security to SNMP monitoring. By default, SNMP packets are accepted from any host.

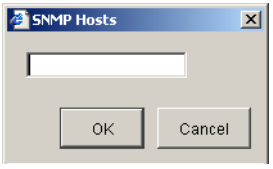


Figure 24-13 SNMP Hosts dialog

10 Click Apply to save your changes.

11 Click Done to return to the Management Console.

Configuring a contact

If you want to specify a person or organization to contact in the case of an SNMP alarm that requires immediate attention, you can enter that information in the Agent Panel tab in the SNMP Configuration applet.

To configure a contact:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the SNMP Configuration icon, located in the General Administration section.

3 Click the Agent Panel tab.

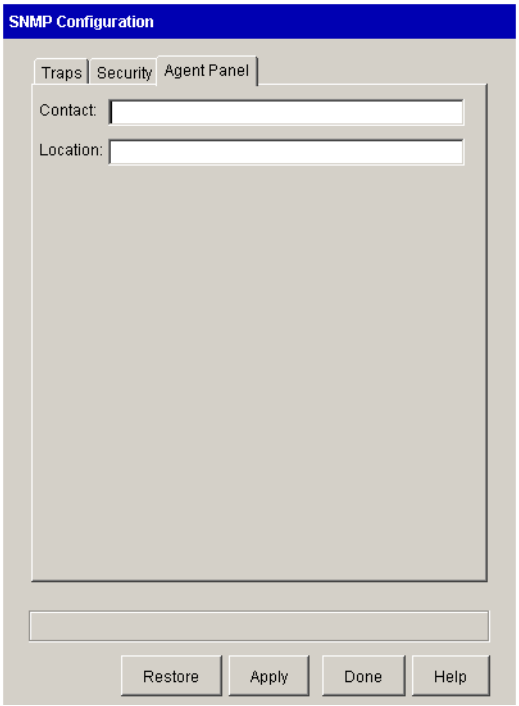


Figure 24-14 SNMP Configuration applet, showing Security tab

4 Type the name of the person or organization to contact in the Contact field.

5 Type the location, or a telephone number, of the person or organization to contact in the Location field.

6 Click Done to save your changes and return to the Management Console.

Using SNMP Alarms

You will access the SNMP Alarms applet frequently as you monitor the Wave ISM. Once the SNMP Configuration applet has been configured, the SNMP Alarms applet reports all SNMP traps sent by SNMP agents residing on the Wave ISM. You can view alarms to help determine why, for example, your T-1 link or the Wave ISM is down.

Caution: *You cannot see any SNMP alarms unless trap destinations are configured in the SNMP Configuration applet. You must configure a valid trap community name, and the host name or IP address of the Wave ISM as the trap destination.*

The SNMP Alarms applet provides two views:

- Current alarms, the real-time traps occurring in the Wave ISM. Once you have noted the trap, you can remove it from this view.
- Previous alarms, those that have occurred when the client was not monitoring alarms in real time. All alarms are retained in a permanent record which you can view at any time by using the Previous Alarms button.

Types and severity of alarms are detailed in Using SNMP Alarms.

Note: The alarms, **Connection to the system is lost** and **Connection to the system is restored** are not SNMP alarms and the time stamps associated with them are approximate.

To use the SNMP Alarms applet:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the SNMP Alarms icon, located in the General Administration section.

The most recent alarms are displayed in the upper list box.

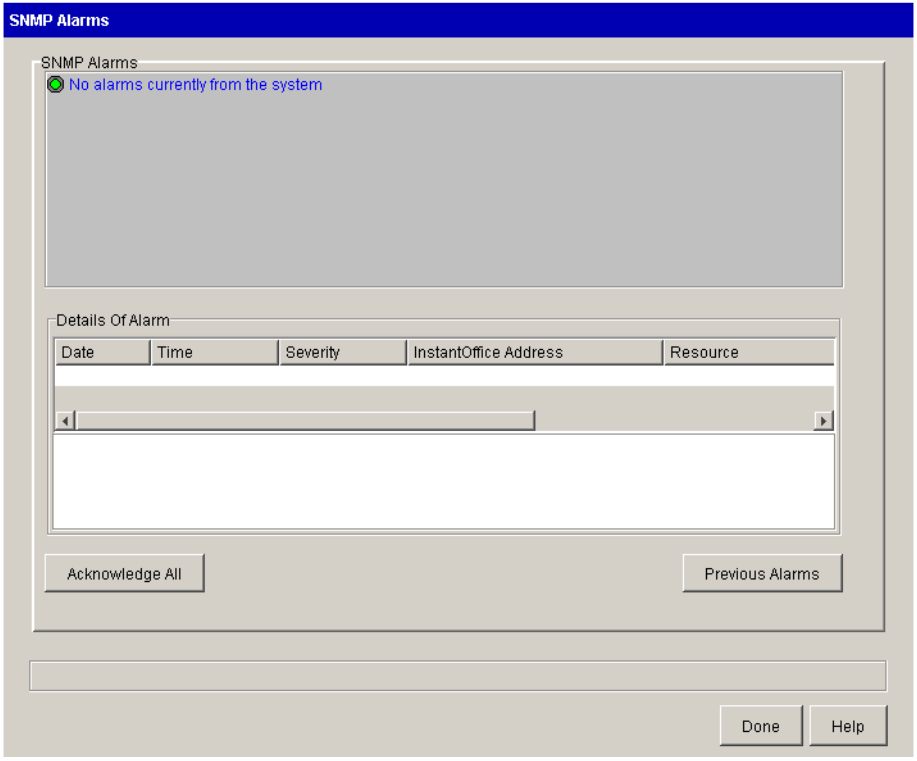


Figure 24-15 SNMP Alarms applet

To monitor alarms in real time, leave the applet open. Alarms are reported continuously, since a permanent connection with the Wave ISM is maintained.

The SNMP Alarms applet displays the most recent alarm at the top of the list.

3 Select an alarm to view details in the lower text area.

4 Click Acknowledge All to remove the list of current alarms and place them in the Previous Alarms log.

5 To see a list of all previous alarms, click Previous Alarms.

The SNMP Alarms applet displays all the previous Wave alarm messages.

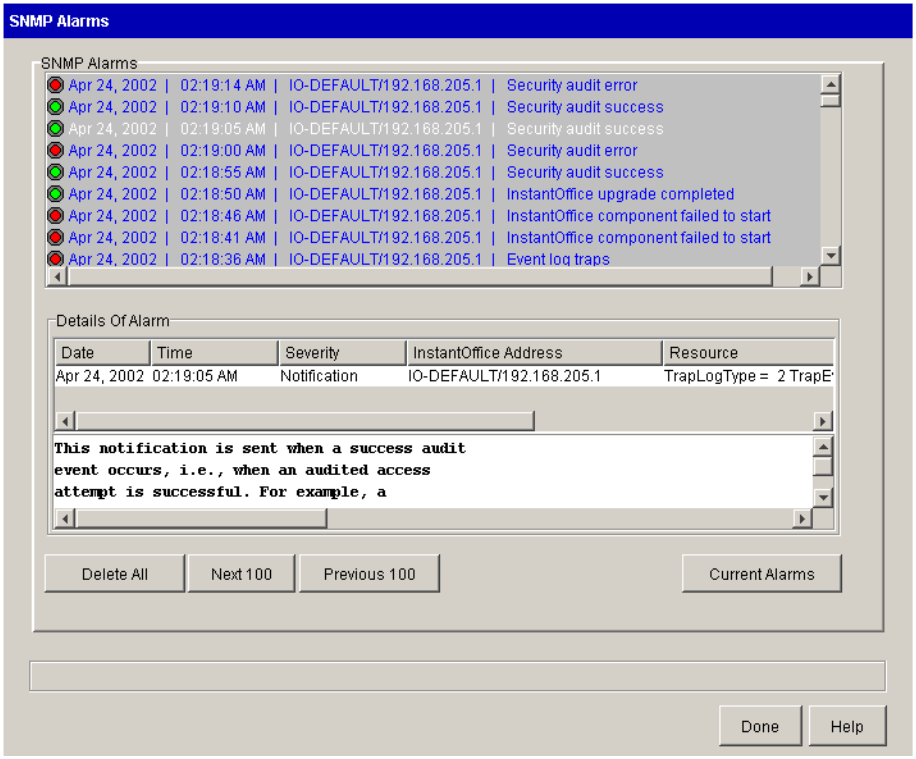


Figure 24-16 SNMP Alarms applet, showing previous alarms

6 Click Next 100 or Previous 100 to traverse through the previous alarms.

7 Double-click an alarm to display the details for that alarm.

8 Click Delete All to remove all the alarms from the Previous Alarms log. This also deletes the history file from the file system.

9 Click Current Alarms to return to the applet that lists only the current SNMP alarms.

10 Click Apply to save your changes.

11 Click Done to return to the Management Console.

Critical Alarms

Most critical (red) alarms are initiated by the Wave ISM, although in some cases a service provider's equipment signal will be displayed as a red alarm. Critical alarms indicate a significant problem with the T-1 link or the Wave ISM. Some of the causes for a critical alarm follow.

- Cable is not connected
- Not receiving a T-1 stream because of a short in the RCV wires
- Receiving an incompatible DS1 frame structure
- Receiving signal (voltage) is too weak because the trunk cable is too long

Major Alarms

Most major (yellow) alarms are initiated by your service provider because their equipment is not able to process the T-1 stream. Some of the causes for a major alarm follow:

- Service provider is receiving incompatible DS1 frame structure
- Transmitting signal is too weak because the trunk cable is too long

Notification Alarms

Notification (green) alarms indicate a system modification. For example, a T-1 module or analog station card has been reconfigured.

Using Disk Management and configuring RAID-1

You will typically access the Disk Management application using the RAID-1 Configuration icon to determine the status of your Wave ISM hard drives, mirror a new hard drive, or use a mirrored hard drive to recover Wave after a failure. You can also mirror a hard drive as a method of backing up your Wave configuration.

Clearing an old hard drive

To clear an old hard drive:

1 Shut down the Wave ISM.

2 Insert the old hard drive in slot B.

3 Restart the Wave ISM.

4 If necessary, click the Administration tab of the Management Console.

Click

5 Click the RAID-1 Configuration icon, located in the General Administration section.

For information about logging on using a remote connection, refer to “Initial logon” on page 2-1.

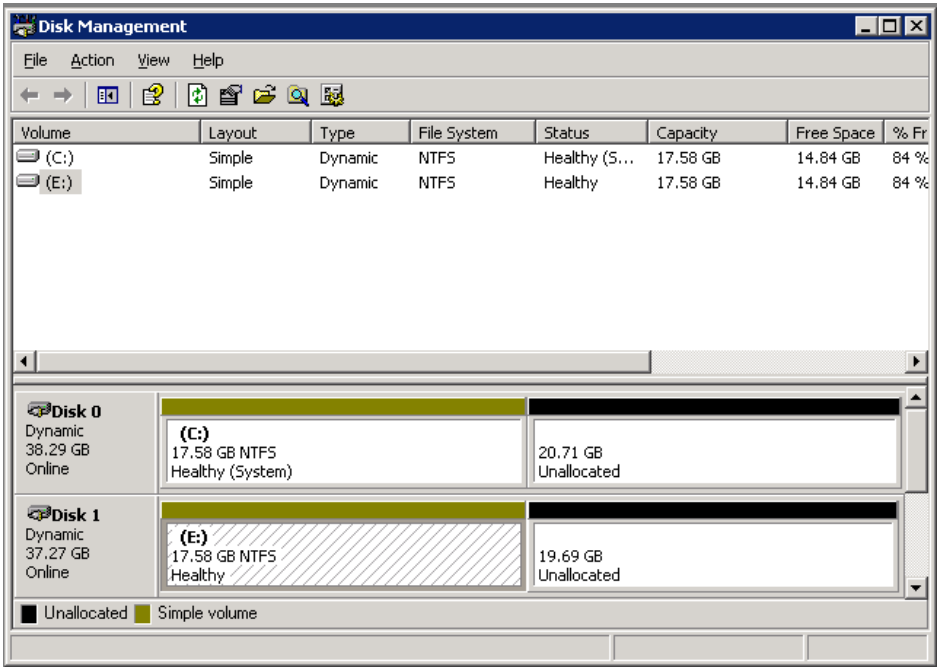


Figure 24-17 Disk Management application

6 Select a partition on Disk 1.

7 Choose **Action > All Tasks > Delete Volume**.

8 Click Yes.

The drive letter will be removed, the partition will be cleared, and a new color will indicate free space (the default is striped).

9 Repeat steps 6 to 8 for each partition.

A hard drive should be free and clear of partitions before it is used for mirroring.

Cloning a hard drive using RAID

Cloning a hard drive, using RAID, is an effective way to create a duplicate of Wave.

To clone a hard drive:

1 Create a mirror of the hard drive using the instructions in “Mirroring your hard drive” on page 15-6.

2 Shut down the Wave ISM.

3 Remove the hard drive from Slot B.

4 Restart the Wave ISM.

5 If necessary, click the Administration tab of the Management Console.

Click

6 Click the RAID-1 Configuration icon, located in the General Administration section.

For information about logging on using a remote connection, refer to “Initial logon” on page 2-1.

7 Select Action > All Tasks > Remove Mirror.

8 Select Disk 1, then click **Remove Mirror**.

9 Shut down the Wave ISM.

10 Insert a new hard drive and restart the Wave ISM.

11 Establish the mirror between the two hard drives, using the instructions in “Mirroring your hard drive” on page 15-6.

12 Install the hard drive you removed in another Wave ISM.

You will need to assign new IP addresses and a new host name to the Wave ISM housing the cloned hard drive you removed from the original Wave ISM.

For information about how to change the host name, refer to “Assigning a new host name” on page 3-2.

For information about how to assign a new IP address, refer to “Changing network interface static IP addresses” on page 3-3.

Identifying RAID disk health

To determine the condition of a mirror set, periodically check the status bar in the Disk Management application. Disk Management displays information about the mirror in the Status column in the Volume List. Table 24-2 describes each status type that could be displayed in the Disk Management Status column. If a partition in the set is damaged or loses synchronization with the other partition, FAILED or FAILED REDUNDANCY is displayed.

Table 24-2 RAID status

Status	Description
FAILED	Displayed when a volume cannot be started automatically or the disk is damaged.
FAILED REDUNDANCY	Displayed when one of the mirrored disks is not online.
HEALTHY	Status if the mirror set is healthy.
REGENERATING	Displayed while Wave is generating the mirror set.
RESYNCHING	Displayed while Wave is establishing the mirror.

To check the status of a RAID disk:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the RAID-1 Configuration icon, located in the General Administration section.

For information about logging on using a remote connection, refer to “Initial logon” on page 2-1.

3 If your disks are mirrored and HEALTHY, the Disk Management will appear as shown in Figure 24-18.

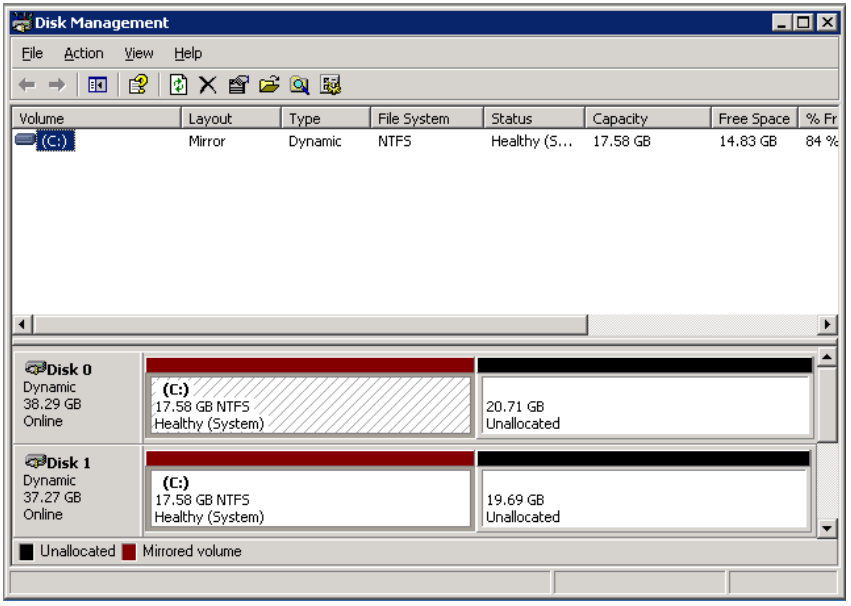


Figure 24-18 Disk Management with mirrored HEALTHY drives

Recovering with RAID-1 Configuration

If the disk in the Wave ISM's slot A is damaged, use the disk in slot B to restart the Wave ISM.

Hint: The Windows Event Viewer may help you determine hardware status and what happened to cause the damage.

To recover Wave from a mirrored disk:

1. Shut down the Wave ISM.
2. Remove the hard drive from slot A.
3. Move the mirrored hard drive from slot B to slot A.
4. Restart the Wave ISM.
5. If necessary, click the Administration tab of the Management Console.

Click

6 Click the RAID-1 Configuration icon, located in the General Administration section.

For information about logging on using a remote connection, refer to “Initial logon” on page 2-1.

7 Select **Action > All Tasks > Remove Mirror**.

8 Select Disk 1, then click **Remove Mirror**.

Note: No fault tolerance is available until a new mirror is established.

9 Re-establish fault tolerance (RAID-1).

- **a** Shut down the Wave ISM.
- **b** Insert a new hard drive in slot B.
- **c** Follow the instructions in “Mirroring your hard drive” on page 15-6.

Entering and Activating Wave Licenses

If you purchase additional Wave licenses or Wave add-on licenses, see Chapter 5 in the *Vertical Wave Installation Guide* for more information on how to enter and activate them

To enable software license keys:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Software Licenses icon, located in the General Administration section.

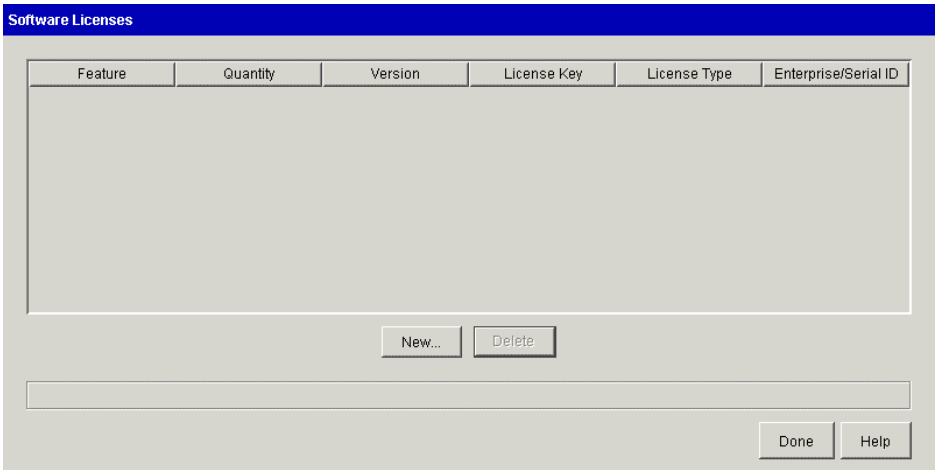


Figure 24-19 Software Licenses applet

3 Click New.

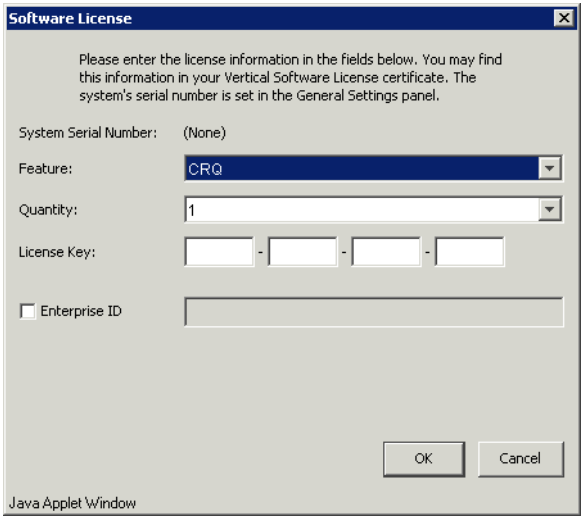


Figure 24-20 Software License dialog

4 Select the appropriate values from the Feature and Quantity drop-down lists.

Refer to your software license certificate for the information you will need to select the correct values.

5 Enter the full 16-character license key in the License Key field.

6 Click OK to close the dialog box.

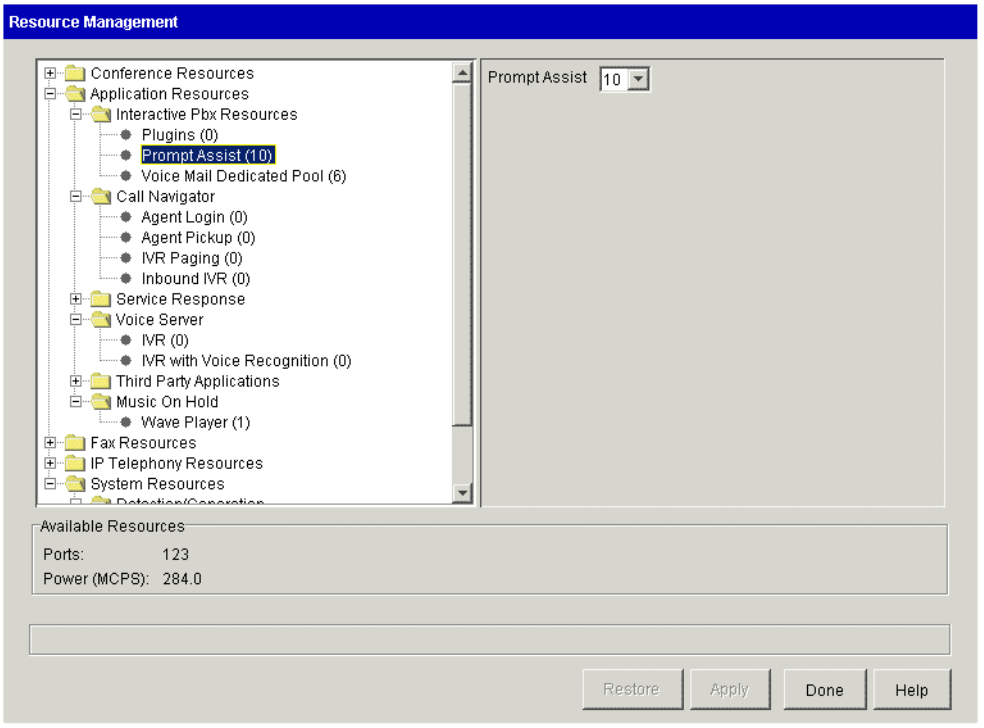
Once you enter your license information and click OK, you cannot edit the license; you can only delete it and re-enter it.

7 The software license information appears in the Software Licenses applet table.

Managing Wave system resources

Many Wave and third-party applications require system port DSP resources such as TAPI/WAVE ports, Fax ports, and IP telephony ports. The type and number of system ports available on your system may vary depending on which cards and modules are installed on it. For information about the resources included on your Wave ISM cards and modules, refer to the *Vertical Wave IP 2500 Hardware Reference Guide.*

Caution: *You must allocate an appropriate number of resources to cover your system demand. If you under-allocate resources, calls may be lost.*



Click an item in the left pane to adjust the number of resources allocated to it in the right pane. The **Available Resources** section at the bottom of the dialog shows the number of ports and MCPS (DSP cycles) available. Some resources consume more MCPS than others, so watch both numbers as you change resource allocations.

See the appropriate sections in this book, or other documentation referenced, for information about allocating resources for the following applications:

The following table describes the various resources listed in the Rescource Management applet:

Resource	Description
Conference Resources	

Resource	Description
Meet Me Conferencing	Not used in this version of Wave.
Ad Hoc Conferencing	Used for conference participants and for conference features invoked from a phone or ViewPoint. The most common use is initiating a conference call and adding parties. Call recording also uses these resources.
Application Resources	
Interactive PBX Resources	**Plugins** - Used for sessions of IVR and other Plug-in applications. **Prompt Assist** - Used for all telephone command prompts in a call, including call announcing. **Voice mail dedicated pool** - Used for voice mail access, either a caller leaving voicemail or a user playing it.
Call Navigator	Used for sessions of the separate Call Navigator application. The IVR resources cover only IVR used by that application, for example automatic call answering.
Service Response	Used for sessions of the separate Service Response application.
Voice Server	Used for Wave IVR, for example touchtone button pushes. If your system uses voice recognition, choose those IVR resources. Otherwise choose the standard IVR resources. There is normally no need to use both.
Third Party Applications	Not used in this version of Wave.
Music on Hold	Used for music-on-hold sessions that derive from sound files. Not used for hold music derived from an external device. See “Music On Hold” on page 18-14.
Fax Resources	
Fax Group	Not used in this version of Wave.
IP Telephony Resources	
Voice Over IP Group	See “Allocating IP telephony resources” on page 6-1. Note that Low Bit Rate codecs use more resources. You must have MRM resources available to use QOS codecs.
System Resources	

Resource	Description
Detection / Generation	These resources should only be adjusted by advanced users. chkbox: set up & scales automatically. Counts phones / trunks, sets optimal. **Caller ID** - Used for Caller ID detection and generation. By default **Use Automatic Port Allocation** is checked, meaning Wave automatically allocates resources for optimal performance based on your system's trunks and phones.

System resource assignment limits

The Resource Management applet enforces limits on the number of resources that can be assigned to each application.

- **Voice Over IP Group**—Purchased software licenses allow you to use the DSPs available on the Wave Integrated Services Card for IP telephony. No IP telephony licenses are required to enable IP telephony ports on DSP resource PCI Telephony Mezzanine Card (PTMC) devices. See the *Vertical Wave IP Telephony Administrator's Guide* for more information.
- **Voice Mail Group**—Limited by sub-group. See "Allocating TAPI resources to Voice Mail and AutoAttendant" on page 14-245 for more information.
- **Call Navigator**—For system resource assignment limits for this application, please see the *Vertical Wave Call Navigator Administrator's Guide* for more information.
- **Third Party Applications**—Limited to 100 ports.
- **Music On Hold**—1 port maximum.
- **Service Response**—For system resource assignment limits for this application, please see its accompanying documentation for more information.
- **Voice Server**—For system resource assignment limits for this application, please see its accompanying documentation for more information.

The Resource Management applet is arranged so that you can identify at a glance how many resources each application is using (indicated by a number next to each sub-group label) and how many resources are unused (indicated in the Available Resources group box at the bottom of the applet).

Some resources are restricted by licenses. If a category requires a license, such as Call Navigator, you will not be able to assign any resources to it until you have entered a valid license key in the Software Licenses applet. See “Entering and Activating Wave Licenses” on page 24-31 for more information.

Accessing Remote Diagnostic Tools

Open the Vertical Wave Remote Diagnostic Tools console when you need to troubleshoot Wave problems. The Remote Diagnostic Tools console provides access to Wave PBX, Voice Mail, networking, and Microsoft Windows troubleshooting tools through a Web browser interface.

To access Wave diagnostics select the Diagnostics icon from the Management Console.

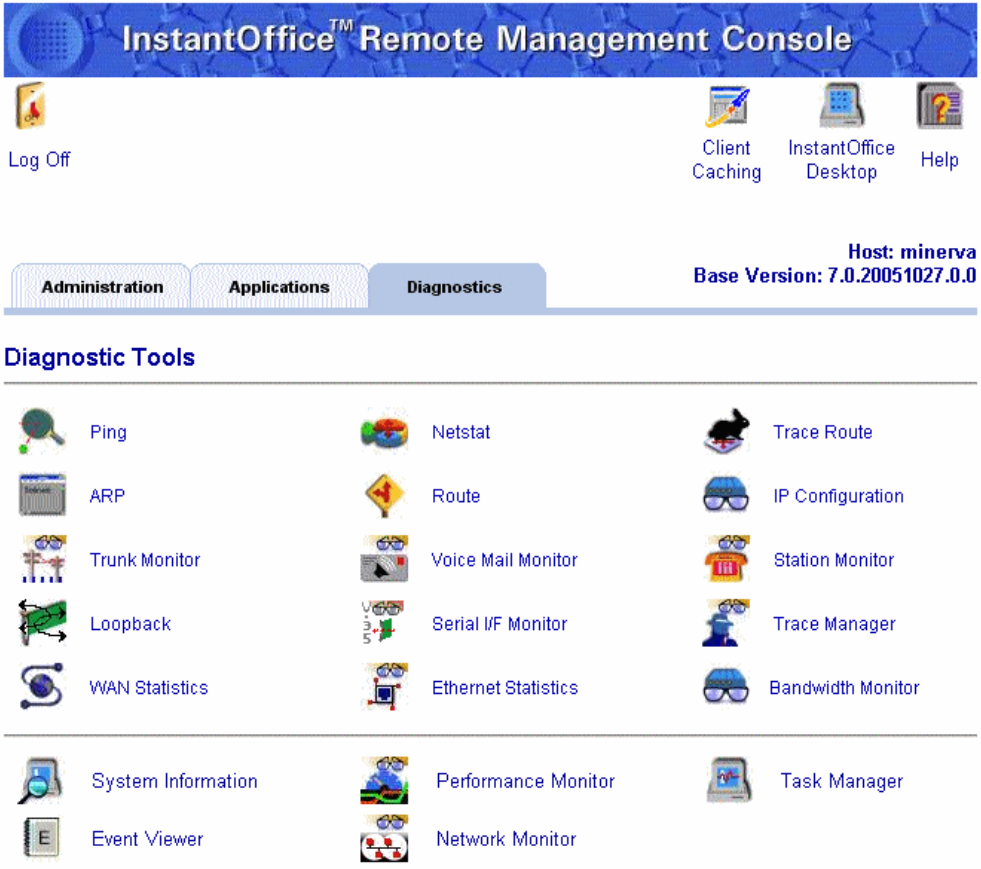


Figure 24-21 Vertical Wave Remote Diagnostic Tools console

For information on using the diagnostic tools, click the Help button on each Remote Diagnostic applet, or click the Help icon on the Diagnostic Tools console.

Client-Side Applications

CHAPTER CONTENTS

Client-side applications

Vertical Wave includes applications that you can install and run on your client machine.

This chapter provides installation and operating instructions for the following client-side applications:

- **Configuring local TAPI for OfficeAttendant**

  Local TAPI (Telephony Application Programmer's Interface) configuration options are used by Wave to provide the Vertical Wave OfficeAttendant application with local dialing properties.

- **Configuring the Network Telephony Service Provider (NTSP)**

  Vertical Communications' Vertical Wave Network TSP provides a method to initiate telephone calls directly from a third-party application such as Act! or Microsoft Outlook.

- **Configuring the Vertical Wave Remote Service for third-party Voice Mail**

  The Vertical Wave Remote Service provides an easy way to run TAPI applications (for example, third-party Voice Mail) on a client machine, utilizing the TAPI resources of Wave.

- **Enabling email access to Vertical Wave Voice Mail**

  Using an IMAP4-compliant Internet email client, you can access voice messages from Wave.

- OrganizationsConfiguring Organizations for OfficeAttendant

Configuring local TAPI for OfficeAttendant

Local TAPI (Telephony Application Programmer's Interface) configuration options are used by Wave to provide the Vertical Wave OfficeAttendant application with local dialing properties. This allows the OfficeAttendant application to prepend the correct external digit when a user leaves it off and to prepend other preemptive digit error correction for external calling.

Typically, you will only be required to set the local TAPI options once. The only time you will be required to change the local TAPI options is if you change the area code or the external digit setting in the First Digit Table.

To access Local TAPI Configuration:

Click

1 Click the Local TAPI Configuration icon, then log on using your Wave username and password. The Phone and Modem Options dialog box opens.

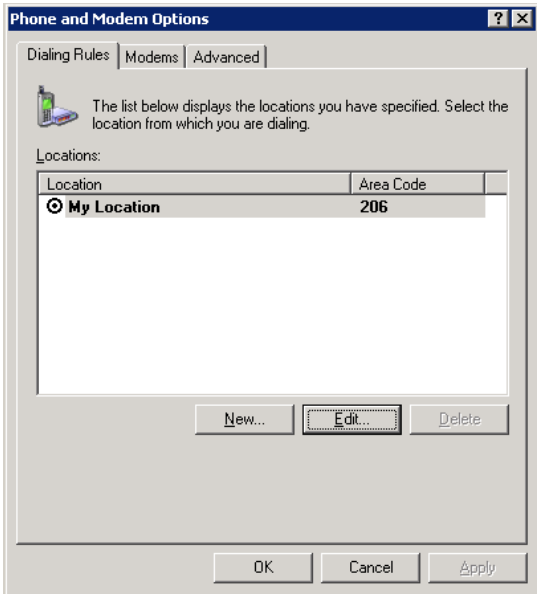


Figure 25-1 Phone and Modem Options dialog, showing the Dialing Rules tab

To configure local TAPI:

1 Double-click your Wave ISM host name in the Locations list in the Dialing Rules tab.

The default might be “My Location” as shown in Figure 25-1. The name in this field is not critical; however, entering the name of your Wave ISM host name will make long-term management easier.

2 Select the country / region for the location of your Wave ISM in the Country / region drop-down list.

3 Enter the area code for the location of your Wave ISM in the Area Code field.

The area code you enter is used by Wave to strip the area code from numbers dialed using the same area code.

4 Enter the first digit number for getting an external line in the **To access an outside line for local calls...** field.

This number is inserted by OfficeAttendant if a user should forget to enter the external digit when calling an outside number.

5 Enter the same number in the To access an outside line for long-distance calls... field.

6 Click OK.

7 Close the Phone and Modem Options dialog box to return to the Management Console.

Configuring the Network Telephony Service Provider (NTSP)

The Network TSP is a small telephony driver that is installed on a client system. The TSP allows third-party TAPI-based call-control applications to use Wave extensions over a TCP/IP network. Microsoft Outlook and Act! are certified to use this feature.

Supported features include:

- Answering calls
- Outbound dialing
- Transferring
- Conferencing
- Hold
- Park
- Pickup

With this application, you can run multiple TAPI-based applications concurrently. For example, and you can use OfficeAttendant to process incoming calls and Microsoft Outlook to make outgoing calls.

Note: TAPI 2.0 or above and the Microsoft networking components must be installed in order to run the Vertical Wave Network TSP. You have TAPI 2.0 or above if you have the tapi32.dll file in your C:\Windows\System32 folder. If you do not have TAPI 2.0 or above, you can download a copy of it from the Microsoft Web site.

Installing the Network TSP

To install the Vertical Wave Network TSP:

1 Using the following instructions, FTP or copy the VNINetworkTSP.exe file from the Wave Integrated Services Manager (ISM) to a temporary file on the target machine.

VNINetworkTSP.exe is a self-extracting file and resides in the Vertical Communications public ftp directory: ftp://*hostname*/public. You can either copy or FTP the file to the target machine.

To FTP using your browser:

- Type the following address in the Address field of your browser where *hostname* is either the name or the IP address of your Wave ISM:

  ftp://*hostname*
- Double-click the public directory.
- Double-click the VNINetworkTSP.exe file to download it to the local system.
- Select the Save this program to disk option, then click OK.
- Specify a destination for the file, then click Save.
- After the file is finished downloading, close the browser and navigate to the directory where you saved the file.

2 Double click the setup program, and follow the prompts to install Network TSP.

You will see the Configure Network TSP dialog box.

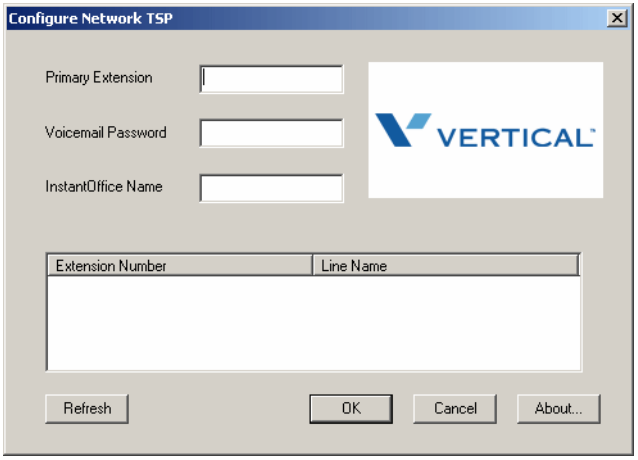


Figure 25-2 Configure Network TSP dialog

3 Configure Network TSP by entering your primary telephone extension, your Voice Mail password, and the host name of your Wave ISM.

4 Click Refresh to ensure that Network TSP can find your extension and Wave system.

5 Reboot your PC, when prompted.

6 Ensure that Network TSP was properly installed by checking that the TSP file exists in the Phone and Modem Options (Windows 2000, Windows XP, and Windows Server 2003) dialog in the Control Panel.

- Open the Control Panel.
- Double-click the Phone and Modem Options icon.
- Click the Advanced tab.

If the driver was installed properly, Vertical Wave Network TSP will be in the list.

Using the Network TSP

After you have installed the Network TSP on your system, you can initiate telephone calls directly from a contact application such as Microsoft Outlook, Act!, or the Microsoft Phone Dialer. Simply open the application, select the contact that you want to call, select the appropriate telephone number from the list, and click the icon or button that initiates a telephone call.

There must be a telephone number associated with the contact for the Vertical Wave Network TSP to initiate the call. Refer to the contact application documentation for more information about how to associate a telephone number with a contact.

Configuring the Vertical Wave Remote Service for third-party Voice Mail

The Vertical Wave Remote Service provides an easy way to run TAPI/Wave applications (for example, third-party Voice Mail) on a client machine, using the TAPI resources of your Wave ISM.

The server-side of the Vertical Wave Remote Service is already installed on your Wave ISM.

Note: To run the Vertical Wave Remote Service, you must have an applications-enabled Wave system.

The following sections provide detailed instructions about how to install and configure the Vertical Wave Remote Service:

- Configuring the server for remote TAPI/Wave applications
- Installing the Vertical Wave Remote Service and the Network TSP

Configuring the server for remote TAPI/Wave applications

Configuring the server for remote TAPI/Wave applications requires that you log in to the Management Console and set options in several of the remote administration applets.

To configure the server side of the Vertical Wave Remote Service:

1 Enable the Use Client Groups mapping option in the Remote TAPI Options of the General Settings applet.
   - Click the General Settings icon in the Management Console.
   - Check the Use Client Groups mapping option on the System tab.

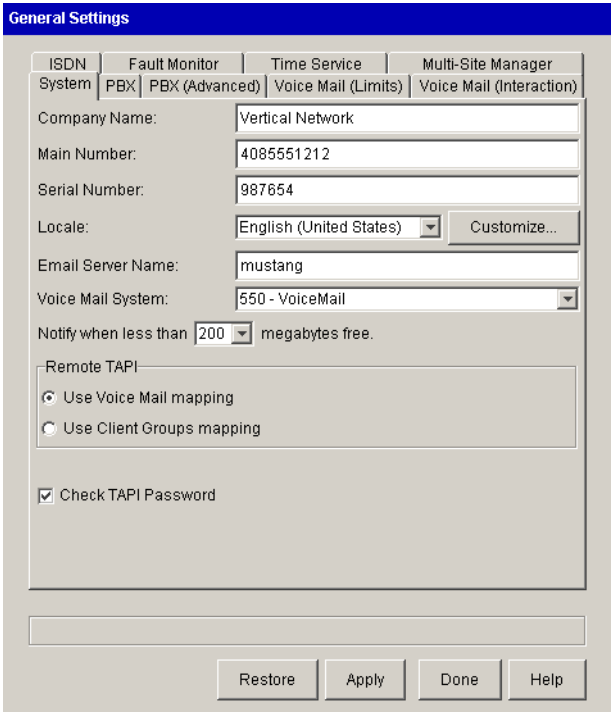


Figure 25-3 General Settings, showing the System tab

- Click Done to save your changes and return to the console.

2 Configure a Subscriber mailbox in the AutoAttendant and Voice Mail Configuration applet.

- Click the AutoAttendant and Voice Mail Configuration icon in the Management Console.
- Click Add on the Subscribers tab.
- Enter the following values (see Figure 25-4):
  - Mailbox ID: `100`
  - Extension: `100`
  - Password: `100`

Note: This example uses the Mailbox ID, Extension, and Password of 100 for simplicity. You can use other values.

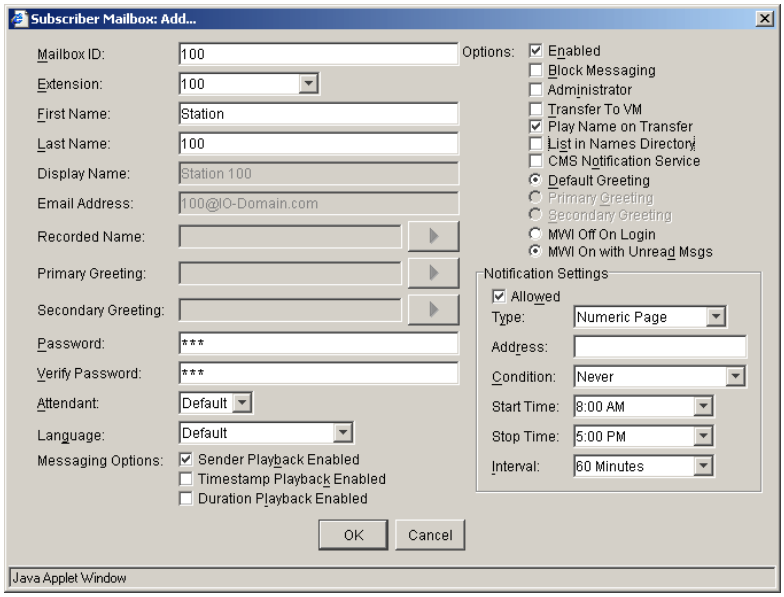


Figure 25-4 Subscribers Mailbox Settings dialog

- Uncheck the List in Names Directory check box.
- Click OK.
- Click Done in the Mailbox Configuration applet to save your changes and return to the console.

3 Allocate resources for your application in the Resource Management applet.

- Click the Resource Management icon in the Management Console.
- Expand the Application Resources folder and the Third Party Applications folder.
- Allocate TAPI ports to the Third-Party Common Pool by increasing the number shown in the Third Party Common Pool drop-down list in the Third Party Common Pool pane.

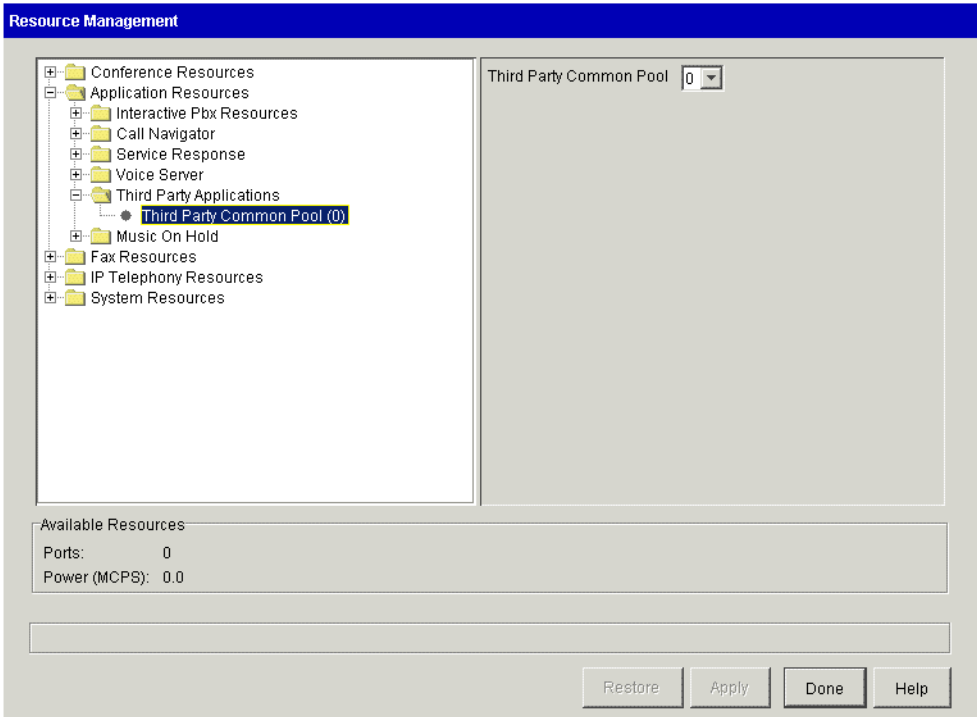


Figure 25-5 Resource Management applet

- Click Done to save your changes and return to the console.

4 Add a hunt group and allocate system ports in the Hunt Groups applet.

- Click the Hunt Groups icon in the Management Console.
- Click New in the Applications tab.
- Enter a pilot number (extension) for the new hunt group and choose Third Party from the Application Type drop-down list.
- Click Add in the Members group box and add all the available system ports.

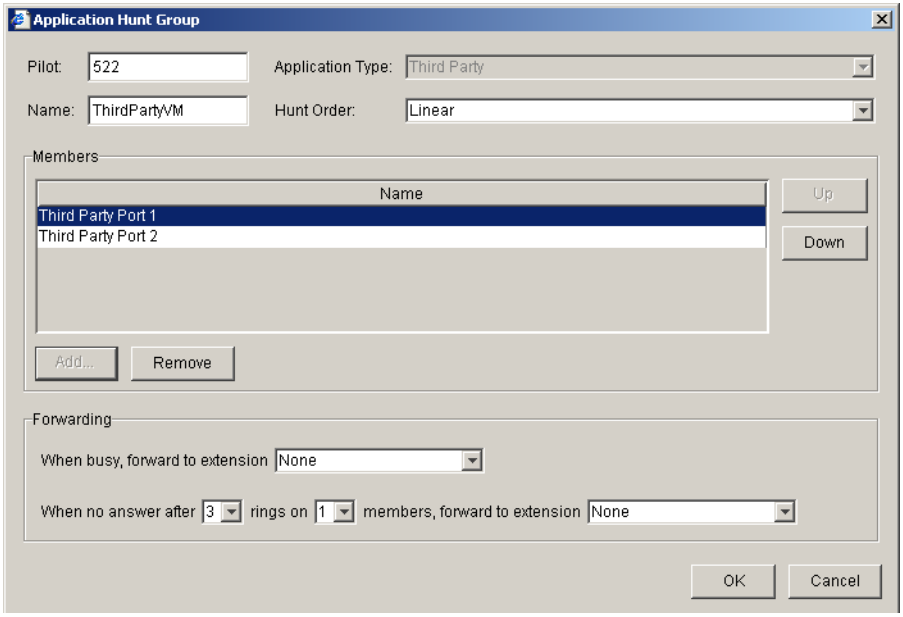


Figure 25-6 Application Hunt Group dialog

- Click OK.
- Click Done in the Hunt Groups applet to save your changes and return to the console.

Configuration of the server-side of the Vertical Wave Remote Service is complete. You do not need to reboot the Wave ISM.

Installing the Vertical Wave Remote Service and the Network TSP

To install Vertical Wave Remote Service and the Network TSP on a client machine:

1 FTP or copy the VNRemoteWave.exe file from the Wave ISM to a temporary file on the target machine.

VNRemoteWave.exe is a self-extracting file and resides in the Vertical Communications public ftp directory: ftp://*hostname*/public. You can either copy or FTP the file to the target machine.

To FTP using your browser:

- Type the following address in the Address field of your browser where *hostname* is either the name or the IP address of your Wave ISM:

  ftp://*hostname*
- Double-click the public directory.
- Double-click the VNIRemoteWave.exe file to download it to the local system.
- Select the Save this program to disk option, then click OK.
- Specify a destination for the file, then click Save.
- After the file is finished downloading, close the browser and navigate to the directory where you saved the file.

2 Double-click VNIRemoteWave.exe to extract the files.

VNIRemoteWave.exe extracts the files.

3 Double-click Setup.exe.

You will see the Configure Network TSP dialog box.

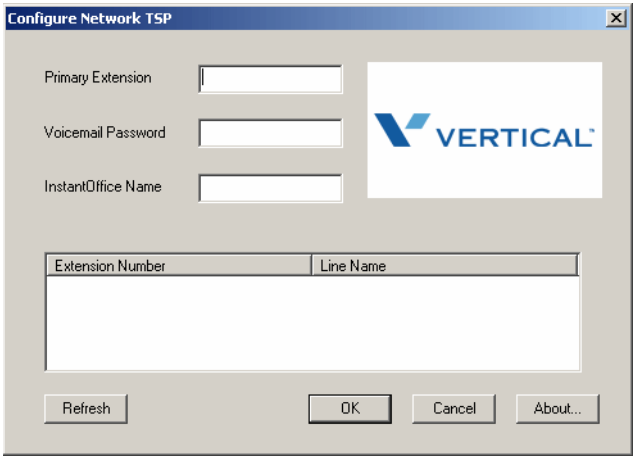


Figure 25-7 Configure Network TSP dialog

4 Configure Network TSP by entering your primary telephone extension, your Voice Mail password, and the host name of your Wave ISM.

5 Click Refresh to ensure that Network TSP can find your extension and Wave system.

6 Reboot your PC, when prompted.

7 Ensure that Network TSP was properly installed by checking that the TSP file exists in the Phone and Modem Options (Windows 2000, Windows XP, and Windows Server 2003) dialog in the Control Panel.

- Open the Control Panel.
- Double-click the Phone and Modem Options icon.
- Click the Advanced tab.

If the driver was installed properly, Vertical Wave Network TSP will be in the list.

Enabling email access to Vertical Wave Voice Mail

Using an IMAP4-compliant Internet email client, you can access voice messages from your Wave system. It does not matter what type of operating system you are running, as long as your email client supports IMAP4. Popular IMAP4 email clients are Eudora Pro, Microsoft Outlook Express and Microsoft Outlook 2002 and beyond.

The following topics provide further information on email access to your Wave Voice Mail:

- Configuring Microsoft Outlook Express for Voice Mail
- Listening to Voice Mail messages using Microsoft Outlook Express

Configuring Microsoft Outlook Express for Voice Mail

Outlook Express is Microsoft's fully-compliant Internet email client. You can set up multiple email accounts and have access to them from one interface. You can set up Outlook Express to access your corporate exchange email and Vertical Wave Voice Mail.

Using Outlook Express to access your corporate exchange email will interfere with using Exchange features like the calendar, scheduling or being scheduled in a meeting, tasks, journals, and notes. If you don't have or need access to an Exchange corporate email service then you should have no problems using Outlook Express to access both email and Voice Mail.

You can use Outlook Express to access your Vertical Wave Voice Mail and Microsoft Outlook to access your corporate exchange email. However, only one application will be able to alert you when you have new messages. For instance the new mail indicator for Outlook Express will not work when you are using it alongside Outlook. Outlook

disables this feature in Outlook Express. Therefore, the only indication of getting a new voice message would have to be from the telephone, either through a message waiting indicator or stutter dial tone.

To configure Microsoft Outlook Express to access Vertical Wave Voice Mail:

1 Launch Microsoft Outlook Express.

The Outlook Express application appears.

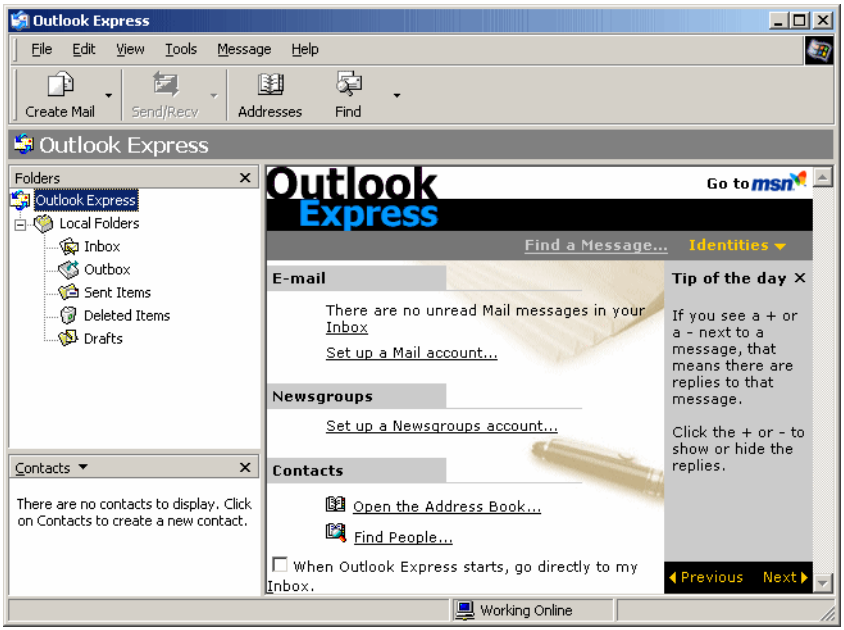


Figure 25-8 Outlook Express application

2 From the Tools menu, select Accounts.

The Internet Account window appears.

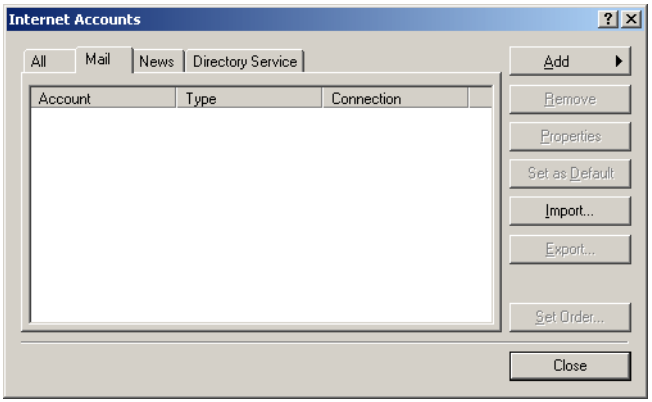


Figure 25-9 Internet Accounts dialog

3 In the Internet Accounts dialog, select the Mail tab.

4 From the Add button, select Mail.

Figure 25-10 Add>Mail

The Internet Connection Wizard appears.

5 Type the following information into the Internet Connection Wizard dialogs:

- Your Name dialog
  - Display name—type in your full name as you want it displayed to other email users.
- Internet E-mail Address dialog
  - E-mail Address—type in your corporate email address. This is the email address that other people will use to reply to any voice messages that you forward on to them.
- E-mail Server Names dialog
  - IMAP—your incoming mail server for this email account is an IMAP server.
  - Incoming mail server—type the name of the Wave ISM on which your Voice Mail system resides.

- Outgoing mail (SMTP) server—type the name of your corporate email server. By specifying your corporate email server, you will be able to forward your Voice Mail messages to other email addresses.

- Internet Mail Logon dialog
  - Log on using IMAP account name—type your IMAP account name; your extension number. For example, 168.
  - Password—your password will be the same numeric password you use to access your Voice Mail through the telephone.

  Note: Do not send email through the Wave ISM; it will bounce.

- Friendly Name dialog
  - Internet mail account name—type the name with which you want this account to show up as in Outlook Express. For example, Voice Mail.

- Choose Connection Type
  - Connect using my local area network (LAN)—select this option.

  After you click Finish to complete the wizard, a dialog will appear asking you to download information for this account. Click Yes.

Your new account should now show up in Microsoft Outlook Express. Voice Mail messages are WAV attachments.

Listening to Voice Mail messages using Microsoft Outlook Express

To listen to Voice Mail messages in Microsoft Outlook Express:

1. Double-click the WAV attachment in a Voice Mail message.

   An audio player is launched.

2. Click the Play arrow in the audio player to listen to the message.

When you have listened to your messages, the message waiting indicator on your phone will be turned off.

Organizations

Configuring Organizations for OfficeAttendant

Organizations are logical groupings of user extensions that can be used in Wave client applications. In the Vertical Wave OfficeAttendant application, the user has access to tabs of Busy Lamp Field groups that allow the attendant to view the status of a group of stations at a glance. Use the Organizations applet to create the groups that appear in the Busy Lamp Field in the Vertical Wave OfficeAttendant application.

Typical uses for Organizations are:

- Placing and transferring calls to a member of a specific group.
- Grouping department head extension numbers (vice presidents, directors, and managers).

To create an Organization:

1. Open the Organizations applet.

   The applet contains two tabs:

2. Click **Add Organization**.
3. Enter a name for the Organization.

   The name you enter will appear on a tab in the OfficeAttendant Busy Lamp Field.

4. Check the check boxes to select extensions from the Organization Members list on the right.

   The extensions you select will appear in the OfficeAttendant Busy Lamp Field tab.

   You can click Select All to create a Busy Lamp Field tab containing all of the extensions and system ports in the Wave ISM.

5. Click Apply to save your changes, and click Done to return to the Management Console.

Part 3

Key Vertical Wave Concepts

Understanding Vertical Wave Trunks

CHAPTER CONTENTS

For configuration procedures related to the concepts in this chapter, refer to Chapter 5, Configuring Analog and Digital Trunks on page 1.

To better apply general trunking concepts to your specific situation, refer to your Service Confirmation Letter as you read this chapter. For samples of a Trunk Provisioning Information Form and a Service Confirmation Letter, see Chapter 35, Service Confirmation Letters and Provisioning Information Forms.

Trunk and channel terminology

Before reading more about Wave trunks, you should understand how we use the following terms in the documentation and user interface.

- **Channel**—A path of communication between two points, typically between the telephone company central office, your service provider, and you, the subscriber. In Wave, a channel carries one voice call or one data connection.
- **Trunk**—The transmission media by which the central office of your service provider sends your telephone and data signals, typically over cabling that plugs into various Wave hardware components.
    - **Analog trunk**—Transport a single channel of traffic and are commonly referred to as Plain Old Telephone Service (POTS) trunks (and sometimes known as *analog lines* or *analog channels*). These trunks are similar to the telephone lines running into your house.

In Wave terminology, we refer to analog trunks as either *trunks* or *channels* in the documentation, and as *channels* in the Management Console user interface.

- **Digital trunk**—Transport multiple channels of traffic. Each *digital channel* can carry a single voice call or up to 1.544 Megabits per second (Mbps) of data traffic.

- **Line**—See *channel*. Typically refers to analog, not digital.
- **Trunk group**—Indicates a grouping of analog or digital channels. These groupings can handle inbound calls, outbound calls, or both, depending on the trunk group or connection type, and they can handle *only* voice traffic.
- **Connection**—A Wave term used to indicate a grouping of digital channels configured to handle network traffic. These groupings can handle only data traffic.
- **Card, or module**—A Wave hardware component into which the cables carrying the signals from the central office (your trunks) plug.
- **Port**—The physical receptacles, one per trunk, on a card or module into which cables plug.

The following table depicts the relationships of these terms to analog and digital media.

Note: Card, module, and port are not included in the table, because the terms are identical across analog and digital media.

Table 26-1 Relationship of terminology across analog and digital media

Term	Analog	Digital
Channel	A single call; same as *trunk* and *line*	A single call or data connection
Trunk	A single channel, call; same as *channel* and *line*	Multiple channels carrying multiple calls or data connections
Trunk group	A named, specified group of voice channels, or trunks	A named, specified group of voice channels
Connection	N/A	A named, specified group of data channels

Analog and digital trunks

Wave supports both analog and digital trunks. Your Internet Service Provider provisions each of your trunks for specific handshake and signaling options, which they provide in your Service Confirmation Letter (see Chapter 35, Service Confirmation Letters and Provisioning Information Forms). You must enter these values in Wave for the trunks to operate properly with the equipment on the service-provider end of each trunk.

Before you configure trunks, ensure that your trunk groups are configured appropriately. For more information about trunk groups, see “Trunk groups” on page 26-4. For trunk group configuration procedures, see “Creating new trunk groups” on page 5-1.

Analog trunks

Depending on the type of Integrated Services Card in your Wave ISM, you have 6 analog trunk ports on your Integrated Services Card (ISC), 3 analog trunk ports on your Integrated Services Card (ISC), or a total of 11 analog trunk ports on your resource switch card (RS3A-C). In addition, your Wave Integrated Services Manager (ISM) might have additional 8-port analog trunk modules (e.g., Analog DID Trunk Module, Analog Universal Module). The Wave ISM supports up to 30 analog trunks concurrently. Each trunk can carry a single voice call or a single 56 Kbps modem data call.

Note: The Wave ISM supports a total of two concurrent 56 Kb modem calls using the two internal modems on the RS2-C. If you have an RS3-C, you only have one internal modem. You can connect additional modems externally to analog station ports.

For trunk configuration procedures, see “Configuring analog trunks” on page 5-5.

Digital trunks

The Wave ISM supports the following digital connections:

- **T-1**—Transports a stream of Digital Signal 1 (DS1) frames. Each frame transports up to 24 channels of traffic, with each channel supporting a single voice call or 56/64 kilobits (Kb) of data traffic. You can configure each of the 24 channels of the T-1 connection independently to transmit voice or data.

The Wave ISM supports data connections up to 1.544 Megabits per second (Mbps) and can switch voice and data traffic from four T-1 connections simultaneously.

For T-1 configuration procedures, see “Configuring digital trunks and channels” on page 5-10.

In addition, the T-1 card incorporates a T-1 / DS0 Multiplexor, also known as the DS0 Digital Access Cross-Connect Switch, that provides the capability**—in software and without additional hardware—**to individually cross-connect DS0s (a single channel) from one digital interface to another, allowing DS0s to pass through the Wave without terminating on an internal device. To do this, you assign the T-1 / DS0 Mux connection to the channels you want to cross-connect to another T-1 interface. You connect one of your T-1 ports to your incoming T-1 connection and another T-1 port to the external device (for example, another router).

For DS0 Mux configuration procedures, see “Configuring digital trunks and channels” on page 5-10.

- **ISDN PRI** —Transports data at 1.544 Megabits per second (Mbps). The Wave ISM supports ISDN PRI on any or all of the digital trunks on T-1. This includes support for Network Service Facility (NSF) codes for least cost routing on a call-by-call basis over an ISDN PRI trunk (if your trunk supports multiple services).

  You can specify the ISDN Type of Number (TON) and Numbering Plan Identifier (NPI) to enable connections to operate on different ISDN networks. When using ISDN PRI for a connection, you reduce the available channels by one per circuit.

  For ISDN configuration procedures, see “Configuring digital channels for ISDN” on page 5-21.

Trunk groups

By assigning analog or digital trunks to trunk groups, you enable the voice paths to the PBX subsystems of Wave. By assigning digital channels to data connections, you enable data paths to the network subsystems of Wave.

Before you work with analog or digital trunks on Wave, you might need to configure groupings of them. For trunk group configuration procedures, see “Creating new trunk groups” on page 5-1.

Note: The Wave system has a maximum of 20 groups, including hunt groups, trunk groups, and zone paging groups.

Voice and data traffic

Digital trunk groups can handle either voice or data traffic, and analog trunk groups can handle voice traffic.

- **Voice—Analog or digital** trunk groups configured for voice traffic direct inbound calls to a specific extension (station, hunt group, modem, or fax machine) and direct outbound calls from an extension to an available trunk of the trunk group.
- **Data—**Digital connections bind WAN data traffic to and from the Wave LAN segment(s) and direct data signals traveling via channels directly to logical router interfaces of the Microsoft Routing and Remote Access Service (RRAS). This is how Local Area Network (LAN) traffic is passed to and received from the connection.

  You can use the following connections to transport data between the Wave ISM and the WAN:

  - DS0/Mux
  - Serial, which enables you to cross-connect digital channels to a serial interface to an external router

Vertical Wave trunk groups and connections

Wave provides default groupings that you can use to quickly group a set of analog or digital channels. Table 26-2 lists the default analog and digital trunk groups and a brief description of each, and Table 26-3 lists the default data connections. The trunk groups appear in the Trunk Groups applet. The connections appear in the Trunk Configuration applet.

Table 26-2 Default analog and digital trunk groups

Default Group	Description
Voice Analog	Configured to direct incoming analog voice traffic to a default destination (attendant, extension 0).
Voice Digital	Not configured. A named, placeholder trunk group for you to configure.
DID Analog	Not configured. A named, placeholder trunk group for you to configure.
DID Digital	Not configured. A named, placeholder trunk group for you to configure.
Modem	Configured to direct data traffic traveling on either digital channels or analog trunks to an internal 56 Kbps modem in the Wave ISM (hunt group 570). This group routes data traffic for dial-up or dial-in computer client connections. The channel or trunk assigned to the Modem group should be dedicated lines (phone numbers). Calls directed by the Modem group are sent to extension 570 (the default modem hunt group).

Table 26-3 Default data connections

Default Connection	Description
T-1/DS0 Mux	Configured to provide the capability—in software and without additional hardware—to individually cross-connect DS0s from one digital interface to another, allowing DS0s to pass through the Wave without terminating on an internal device.

In most call routing scenarios you need not create additional groups; the defaults should provide you with the functionality you need.

You might need to create new trunk groups, however, to handle multiple-trunk call-termination scenarios. If so, you need all of the DID information available from your service provider, for example:

- The range of DID numbers
- Whether the DID T-1 channels and analog trunks are inbound or bidirectional (2-way)
- How many digits are they sending (usually 3 or 4)

If your call scenario requires additional groups, see “Creating new trunk groups” on page 5-1.

Trunk group hunt types

When users make outbound calls on Wave, the hunt type of the associated trunk group determines how an available analog trunk or digital channel is located. Trunk groups can hunt in either a linear or a circular fashion and either of those hunt types can be used in forward or reverse order.

- **Linear—**Looks for a free channel, always starting at the beginning of the list of trunk groups and searching to the end, or—for reverse-order hunting—always starting at the end of the list and searching to the beginning. Each channel is tried once.
- **Circular—**Looks for a free channel, starting where the last search left off. From this point (where the last search left off), forward-order hunting works forward through the list of available channels, and reverse-order hunting works backward through the list. Each channel is tried once.

When you configure trunk groups, you will set the hunt type for each. For trunk group configuration procedures, see “Creating new trunk groups” on page 5-1.

Minimizing GLARE

GLARE occurs when an incoming call and an outgoing call select the same channel simultaneously. For example, GLARE occurs when Wave receives a call from the network on a channel it has just selected to initiate an outbound call. In this case, Wave allows the inbound call to use that channel and retries the outbound call on a different channel.

Reverse-order hunting helps reduce collisions with the central office's incall hunt group. The central office will typically use incall hunt groups that are linear and start with the lowest trunk or channel.

To minimize GLARE:

1. Determine the central office (network side of the connection) hunt order.
2. Configure Wave (user side of the connection) for the opposite hunt order.

   For example, if the central office is configured for linear hunting, configure Wave for reverse linear hunting.

Note: When connecting two Wave ISMs together using ISDN, set the network side of the connection to the linear hunt type and the user side to the reverse linear hunt type.

Hunt type examples

Assume channels 1 through 5 belong to the same outbound trunk group.

Forward-order linear searching

- Request for external line: accepted by outbound connection
- Check digital channel, channel 1: busy
- Check digital channel, channel 2: busy
- Check digital channel, channel 3: available—call placed
- Request for external line: accepted by outbound connection
- Check digital channel, channel 1: busy
- Check digital channel, channel 2: available—call placed

In this example, each time a request for an external line is made (typically by the user dialing 9 to access an outside line) the trunk group members (individual digital channels) are searched in order.

Reverse-order linear searching

- Request for outside line: accepted by outbound trunk group
- Check digital channel, channel5: busy
- Check digital channel, channel 4: busy

- Check digital channel, channel 3: available—call placed
- Request for outside line: accepted by outbound trunk group
- Check digital channel, channel 5: busy
- Check digital channel, channel 4: available—call placed

Forward-order circular searching

- Request for outside line: accepted by outbound trunk group
- Check digital channel, channel 1: busy
- Check digital channel, channel 2: busy
- Check digital channel, channel 3: available—call placed
- Request for outside line: accepted by outbound trunk group
- Check digital channel, channel 4: busy
- Check digital channel, channel 5: available—call placed
- Request for outside line: accepted by outbound trunk group
- Check digital channel, channel 1: busy
- Check digital channel, channel 2: available—call placed

Reverse-order circular searching

- Request for outside line: accepted by outbound trunk group
- Check digital channel, channel 5: busy
- Check digital channel, channel 4: available—call placed
- Request for outside line: accepted by outbound trunk group
- Check digital channel, channel 3: busy
- Check digital channel, channel 2: busy
- Check digital channel, channel 1: available—call placed
- Request for outside line: accepted by outbound trunk group
- Check digital channel, channel 5: busy
- Check digital channel, channel 4: available—call placed

Understanding Wave IP Telephony

CHAPTER CONTENTS

Understanding Wave IP telephony

The Wave IP telephony sub-system allows you to route voice calls over your data network. The following topics help you understand IP telephony as it is implemented in the Wave system:

- What is IP telephony?
- DSP resources and licensing for IP telephony resources
- IP call routing
- IP telephones
- Bandwidth management
- IP call quality management

What is IP telephony?

IP telephony, also known as voice over IP, allows you to make telephone calls using segments of your data network rather than the traditional Public Switched Telephone

Network (PSTN). The two different types of calls are transmitted over different networks, as shown in Figure 27-1.

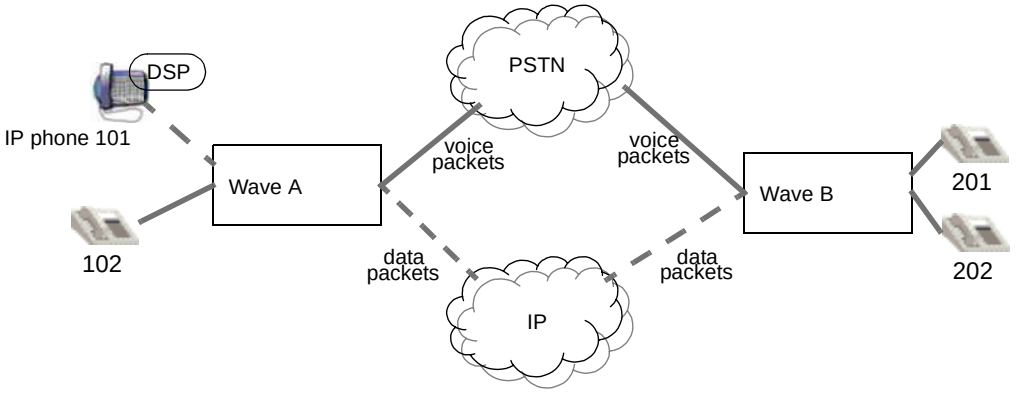


Figure 27-1 PSTN and data networks can each carry voice traffic

To transmit voice over the data network, a Digital Signal Processor (DSP), using a codec (a signal compression-decompression algorithm), splits up the voice signals into small parts, compresses them, and inserts them into data packets. The packets are addressed to the call recipient (an IP address) and sent out over the data network. The packets are reassembled by a DSP at the receiving end.

Using IP telephony, Wave users can:

- Call extensions on remote Wave sites over the data network (site-to-site IP calls)
- Save money on long distance calls by using a virtual tie-line to place calls through a remote Wave system (sometimes called tandem call routing).
- Accommodate remote workers and small satellite offices with IP telephones (telecommuters, small branch offices)

IP call scenarios supported on the Wave system

An IP call is a telephone call in which at least one portion of the voice signals are transported across a data network. The Wave system supports the following IP call scenarios:

- Site-to-site IP calls
- IP telephone calls

Site-to-site IP calls

A site-to-site IP call is a telephone call in which the segment of the call path between the Wave systems is on the data network, as shown in Figure 27-2.

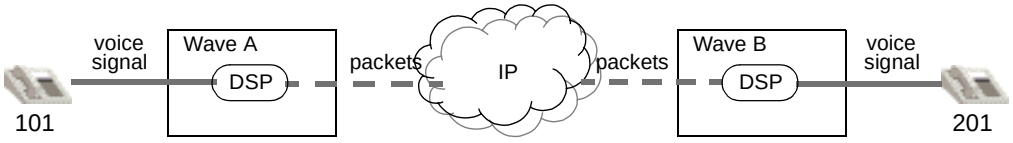


Figure 27-2 Site-to-site telephone call between Wave systems

For more information about the DSPs, licenses, and configuration required for this scenario, see the following sections of this document:

- "DSP resources required in a site-to-site scenario" on page 27-5
- "Direct site-to-site IP calls" on page 27-8
- "Site-to-site IP calls via gatekeeper" on page 27-8

IP telephone calls

An IP telephone is connected directly to the data network; therefore, a call involving an IP telephone uses the portion of the data network between the IP telephone and the Wave system. IP telephones can make calls to the PSTN (see Figure 27-3), internal analog and digital telephones (see Figure 27-4), and other IP telephones (see Figure 27-5).

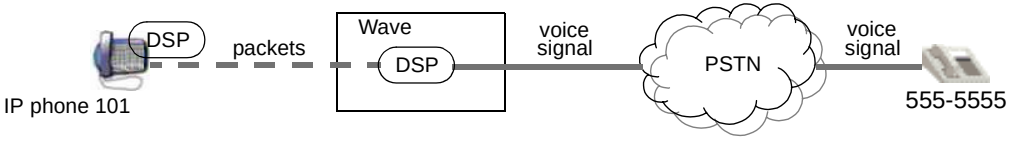


Figure 27-3 IP telephone call to a device on the PSTN

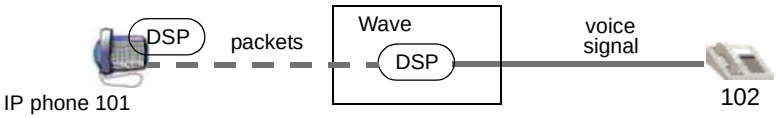


Figure 27-4 IP telephone call to a telephone connected to the Wave system

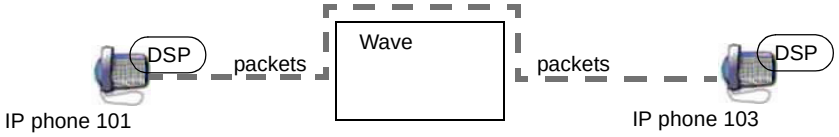


Figure 27-5 IP telephone call to another IP telephone

For more information about the DSPs, licenses, and configuration required for these scenarios, see the following sections of this document:

- "DSP resources required in scenarios with IP telephones" on page 27-5
- "IP telephones" on page 27-9

DSP resources and licensing for IP telephony resources

Digital Signal Processor (DSP) resources applied to IP telephony give the Wave system the capability to route voice calls over packet-switched (data) networks. DSPs can convert voice signals into data packets, and vice versa, using a codec.

The number of DSP resources you have available for IP telephony on your Wave system depends upon the hardware installed on your system and the IP Telephony Resource license you purchase.

IP telephony resources are available on your Wave system in two places:

- **Resource switch card**—The IP Telephony Resource license (4 or 8 resources) allows you to use the DSPs available on the Wave resource switch card for IP telephony.
- **DSP resource PCI Telephony Mezzanine Cards (PTMC)**—No IP telephony licenses are required to enable IP telephony ports on these devices. Each port is a multipurpose IP telephony, FAX, or TAPI/WAVE port.

How many DSPs do you need?

The more DSPs you allocate to IP telephony in the Resource Management configuration, the more concurrent IP calls your system can support. To estimate the number of DSPs you require at each site, remember that each time a transition is made

between TDM voice signals and packets in the voice path, a DSP is required to make the conversion.

Note: Calls between IP telephones do not require any DSPs on the Wave system.

Most IP calls will require two DSPs; one at each end of the IP segment of the call. The DSPs might be located on the Wave system, or they might be located on the IP telephones, depending on the calling scenario.

DSP resources required in a site-to-site scenario

Figure 27-6 shows the DSPs required in a direct site-to-site IP call scenario (see "Direct site-to-site IP calls" on page 27-8 for a detailed explanation of this scenario). In this scenario, the telephones are traditional TDM calling devices (the analog or digital telephones).

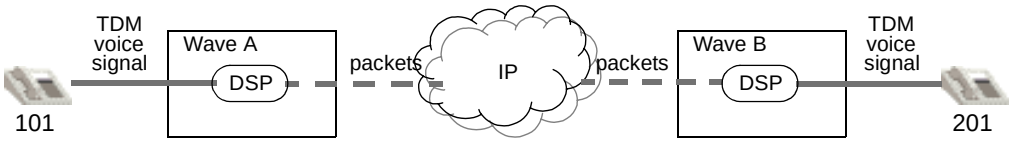


Figure 27-6 DSPs required in a site-to-site telephone call over a packet-switched network segment

A DSP on Wave A translates the voice signal (from the caller at extension 101) into packets that can be sent over the IP network. The receiving Wave B uses a DSP to translate the packets back into a voice signal that can be understood by the call recipient at extension 201, and vice versa. If you want to support four calls of this type at once, each Wave system would require four IP telephony DSP resources.

DSP resources required in scenarios with IP telephones

The DSPs required for telephone calls involving IP telephones may vary depending on how many IP telephones are involved in the call. Figure 27-7 and Figure 27-8 show the DSPs required to make a call from an IP telephone on an Wave system to a standard telephone (either a telephone on the PSTN (Figure 27-7) or a local extension (Figure 27-8).

As in the site-to-site scenario, two DSPs are required for each call, but only one DSP is required on the Wave system, since there is a DSP in the IP telephone.

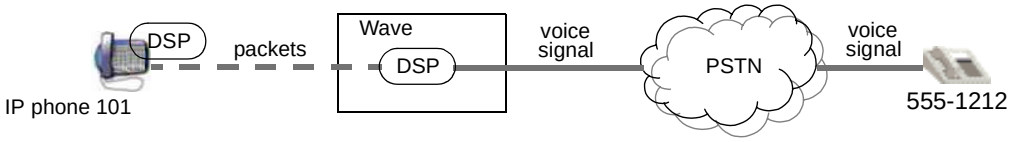


Figure 27-7 IP telephone call to a device on the PSTN

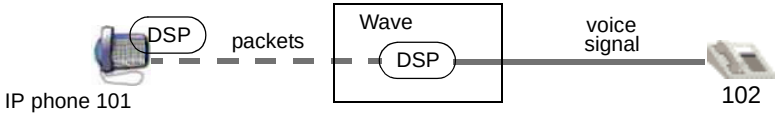


Figure 27-8 IP telephone call to a telephone connected to the Wave system

If you wanted to support four calls of this type simultaneously, the Wave system would require four IP telephony DSP resource licenses and four IP Telephony Client seats.

Figure 27-9 shows the DSPs required to make a call between two IP telephones on the Wave network. Note that no IP telephony resources are required on the Wave system in this scenario.

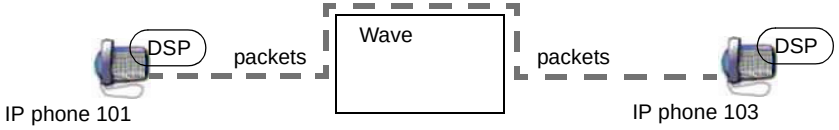


Figure 27-9 IP telephone call to another IP telephone

If all your Wave IP telephony DSP resources are in use making IP calls of types shown in the previous scenarios, you can still make internal calls between IP telephones on the LAN (as long as bandwidth is available).

Other DSP applications

DSP resources are also required by TAPI-based telephony applications, such as Voice Mail. Since TAPI applications and IP telephony cannot share the same DSP resource, you must distribute the DSP resources between TAPI applications and IP telephony

based on your business requirements. See “Managing Wave system resources” on page 24-33 for more information.

IP call routing

Call routing for IP telephony is similar to traditional call routing. This section assumes that you are familiar with Wave call routing mechanisms. Chapter 28, “Understanding Vertical Wave Call Routing,” in the *Wave Administrator’s Guide* provides information about how calls are routed in the Wave system.

For IP call routing configuration procedures, see “Configuring site-to-site call routing for IP telephony” on page 6-3.

Signaling Control Points

A Signaling Control Point is an IP telephony endpoint that is capable of originating and terminating IP calls. A Signaling Control Point is defined by an IP address and an IP telephony signaling protocol. Its traditional Wave call routing counterpart is the trunk group.

Signaling Control Points can be substituted for trunk groups in any of your outbound call routing scenarios. For inbound call routing, each Signaling Control Point configuration includes an inbound call routing table where you can specify how to handle calls from each source.

Each Signaling Control Point configuration includes the remote Wave system’s IP address, signaling protocol, and call routing parameters. Once the Signaling Control Points are configured you can include them as call destinations in your outbound call routing configuration. See Chapter 28, “Understanding Vertical Wave Call Routing,” in the *Wave Administrator’s Guide* for information about Wave call routing.

Default inbound routing

To specify how to route incoming IP calls from unknown sources (that is, a call from an IP address that is not included in your Signaling Control Point configurations), configure the call handling rules with the default inbound call routing settings. Refer to “Configuring default inbound IP call routing” on page 6-9 for more information.

Direct site-to-site IP calls

Direct site-to-site calling requires that every Wave site using IP telephony specifies a Signaling Control Point for every other IP telephony-enabled Wave system on the network as shown in Figure 27-10. In the figure, Wave system A has a Signaling Control Point configured for Wave system B, and vice versa.

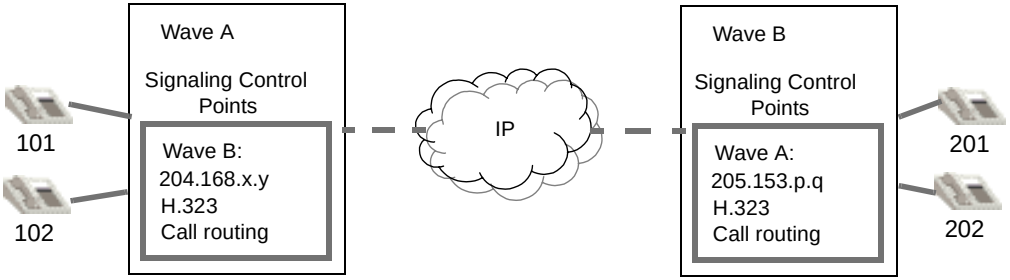


Figure 27-10 Signaling Control Points configured on each system

Site-to-site IP calls via gatekeeper

A centralized authority for routing IP calls may be more manageable for larger IP telephony networks. Site-to-site calling via an IP telephony gatekeeper requires only that each IP telephony-enabled Wave system configure one Signaling Control Point for the gatekeeper. The gatekeeper becomes the central repository for mapping telephone numbers to IP addresses.

This scenario involves placing calls using TDM telephones (analog or digital) over a packet-switched (IP) segment of the network.

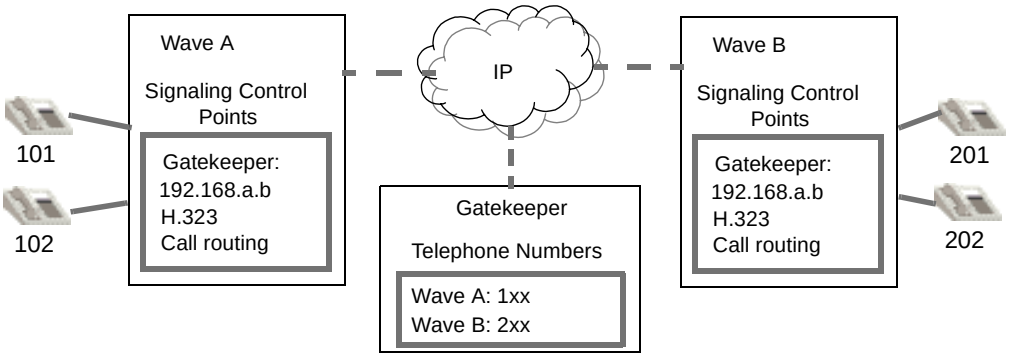


Figure 27-11 Gatekeeper keeps track of Wave systems on the network

The gatekeeper gets the call information (telephone number) from the calling Wave system and translates it into the IP address for the destination. The gatekeeper might negotiate the voice path and set up the call (Gatekeeper Routed), or it might return the information to the calling Wave system and let the Wave system set up the voice path (Gatekeeper Direct).

IP telephones

IP telephones are a convenient way to set up communications between a remote worker, such as a telecommuter, and the main office where an Wave system is running. IP telephones are also a cost effective alternative to setting up a PBX for a small satellite office with fewer than five users. IP telephones in each of these scenarios can be set up at the remote site, and the IP call routing is controlled by the Wave system at the main office.

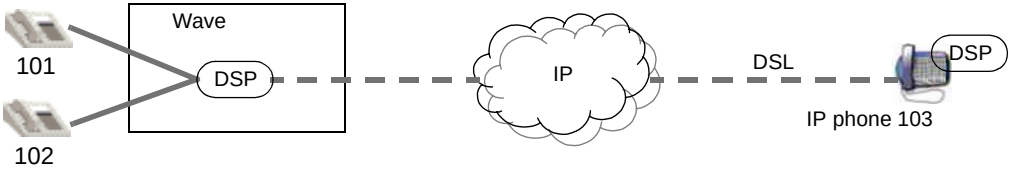


Figure 27-12 IP telephone for a remote worker or satellite office

IP telephones are configured much the same way as other Wave telephones are configured in the User Configuration applet. Each telephone gets a primary extension number and can use a wide variety of Wave PBX features. The physical telephone set

also requires some configuration to initiate communication with the Wave system. See “Configuring IP telephones” on page 6-12 for configuration procedures.

IP telephone client licenses

In order to use IP telephones with your Wave system, you must purchase and enable IP Telephony Client and IP Telephony Resource licenses. IP Telephony Client licenses are available in 1, 2, 4, 8, 16, 24, and 48 seats.

MAC addresses

IP telephones do not use station card ports like TDM telephones; instead they connect over the data network, so the Wave system relies on the MAC address as the unique identifier for each IP telephone.

Just as the Wave system uses a station card slot number and port number to associate an extension configuration with a TDM telephone, a MAC address is used to associate an extension configuration with an IP telephone.

IP addresses

In addition to a MAC address, IP telephones also need IP addresses for call routing purposes. IP addresses can be assigned to each telephone by a DHCP server, or the telephone can be configured with a static IP address.

Bandwidth management

To manage bandwidth across different segments of the network you must create zones that define your network boundaries for IP telephony. Configuring bandwidth management zones allows you to control how much IP call traffic goes across different parts of your data network. It prevents your IP telephony users from making more IP calls than the network connections are capable of supporting.

A bandwidth management zone is defined by a range of IP addresses. You can create as many zones as you have boundaries where you need to control bandwidth use. There are three types of configurable zones:

- **Home Zone**—This is the zone that controls IP call bandwidth on your local Wave system.
- **Remote Zone**—Remote zones control bandwidth usage on sets of IP address at a remote site, for example a branch office or home office.
- **Default Remote Zone**—This zone handles bandwidth management for IP calls from any IP address that is not defined in one of the other zones. A call from an undefined IP address is constrained by the properties configured in the default remote zone.

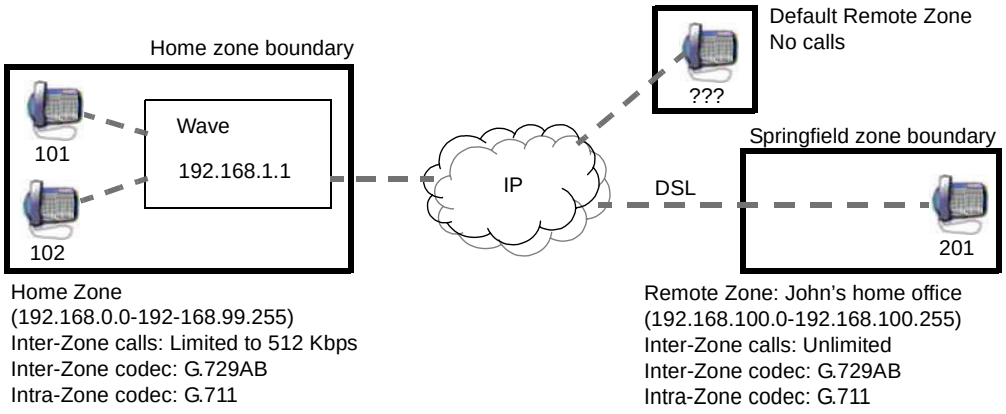


Figure 27-13 Bandwidth management zones

The bandwidth management zone parameters you can configure include the maximum amount of bandwidth used for all calls across a zone boundary, and the preferred codecs, desired transmit packet times, and desired silence suppression setting for inter-zone and intra-zone IP calls.

Intra-zone calls are calls made between telephones within a zone boundary. Inter-zone calls are calls that are made across zone boundaries. Codecs should be assigned such that you can maximize bandwidth on both inter-zone and intra-zone IP calls. Calls within a zone boundary are likely to have more bandwidth available to them than calls connected across zone boundaries.

IP call quality management

There are several advanced settings, in addition to the Bandwidth Management settings, that allow you to manage the quality of your IP calls.

- Jitter buffer
- Echo cancellation
- Comfort noise
- Gain
- DTMF transport settings
- WAN Quality Of Service settings

You should not adjust these settings unless you are an IP telephony expert. If you need help troubleshooting quality problems with your IP calls, contact your Wave product support vendor. Information about these settings is located in “Adjusting IP call quality parameters” on page 6-33.

Understanding Vertical Wave Call Routing

CHAPTER CONTENTS

This chapter contains information about the different types of call routing supported by Wave, and defines and describes the Wave ISM components used to route calls.

About call routing

There are two major steps in Wave call processing: digit collection and call routing. It is important to note that digit collection and call routing are two completely separate processes. In the digit collection process, the PBX collects the digits sent from the call source until it has enough digits to route the call. Once digit collection is complete, the PBX attempts to route the call. Figure 28-1 shows the Wave call routing system and all the major system components a call can pass through on its way to the destination.

All calls that go through Wave pass through the First Digit Table. The first step in all Wave routing decisions is made based on the first digit of the number dialed. The first digit determines whether the call is routed to an internal or external destination as explained in Table 28-1.

A call route is a path through Wave by which a call goes from a source to a destination. There are four types of call routes to consider:

- **Internal**—from an internal source to another internal source (usually extension to extension)
- **Outbound**—from an internal source to an external destination
- **Inbound**—from an external source to an internal destination
- **Tandem**—from an external source to an external source

Each section in this chapter describes and gives examples of each of the four call routing types.

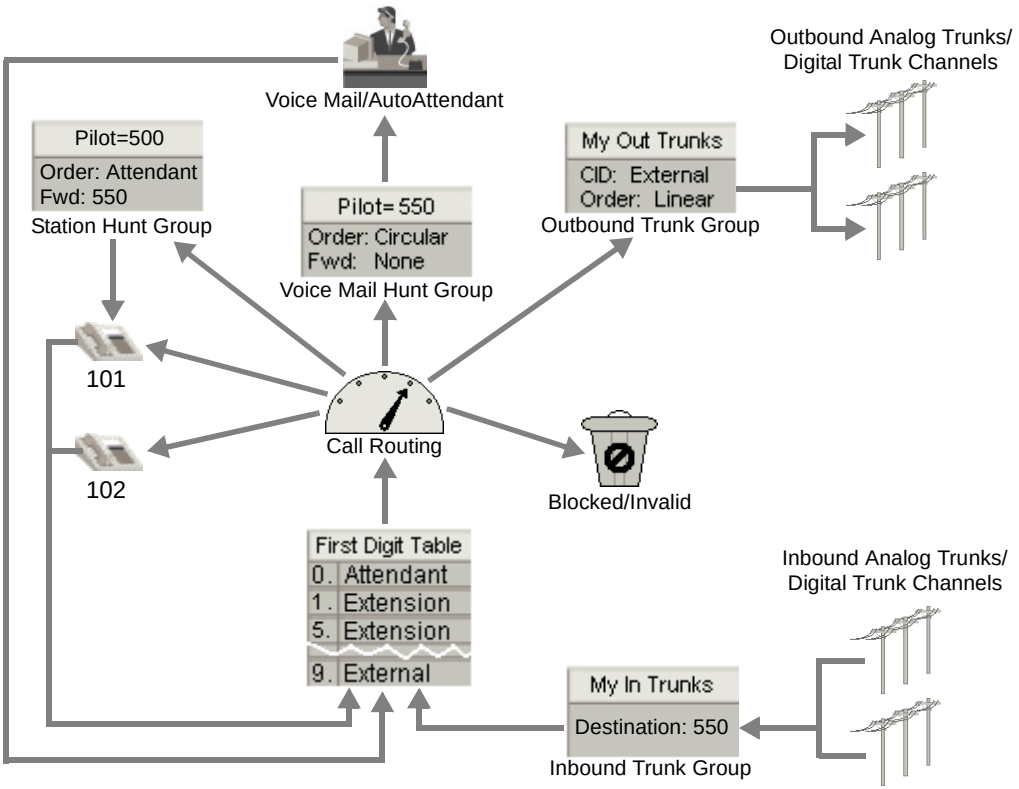


Figure 28-1 Simplified call routing diagram

Table 28-1 First digit types

First Digit Type	Description
Attendant	The Attendant digit serves two purposes: • If the caller dials (or transfers a call to) the Attendant digit from a phone connected to Wave, the PBX connects the caller to a member of the Attendant hunt group. • If the caller is connected to AutoAttendant and dials the Attendant digit, the caller is connected to the operator designated in the AutoAttendant schedule. Any digit—but only one—can be configured as the Attendant digit. The default is zero (0). If the Attendant digit is changed from the default of zero (0), the Attendant hunt group pilot number must also be changed, to ensure that the attendant will receive all calls routed to the attendant. **Caution:** *It is not recommended that you route inbound calls to zero because there can be no Voice Mailbox associated with this destination.*
Extension	The extension digit instructs the PBX to connect calls beginning with these digits to an extension number (or hunt group pilot number). The number of digits to collect following an extension digit is defined in the First Digit Table. The zero (0) digit cannot be configured for extensions. Default extensions begin with the digit 1 and 5, and are in the range 100-199 and 500-599. Hunt groups use extension numbers to pilot calls to the members of a hunt group. For example, Wave modems are preconfigured to be in hunt group 570.
External	An external digit at the beginning of a number instructs the PBX that an outbound, external call is beginning. You can define the external first digits (also known as destination access codes) as being one or two digits in length. Digit collection rules for numbers beginning with external digits are defined in the First Digit Table. The default external digit, 9, requires all users to press 9 on their telephone dial pad before dialing any external number to be routed to the public switched telephone network (PSTN).
Not configured	A digit that is not configured instructs the PBX that calls beginning with these digits are not valid. If a user dials an unconfigured first digit, the PBX plays a fast busy tone to indicate that the first digit dialed is invalid.

Internal call routing

Internal call routing refers to all calls that originate and terminate within Wave. Internal calls can include calls such as station-to-station, station-to-hunt group, station-to-Voice Mail, and station-to-Attendant hunt group. You can trace the routes of these types of calls in Figure 28-1. Figure 28-2 diagrams how a station-to-station internal call flow might look.

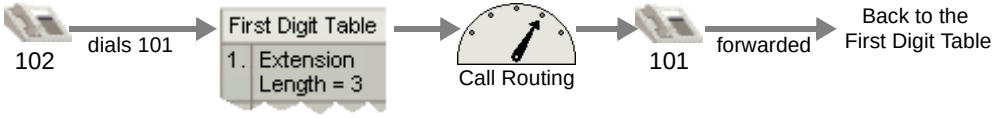


Figure 28-2 Station-to-station internal call routing scenario

Here is what is happening in Figure 28-2:

1. The user at extension 102 dials 1-0-1.
2. The first digit collected, 1, is specified in the First Digit Table as type Extension (and requires 2 additional digits to be collected before routing the call).
3. Once a three digit number beginning with 1 is collected, the PBX looks for extension 101.
4. Extension 101 exists, so the PBX routes the call to extension 101.
5. If the call to extension 101 is forwarded (or transferred), it goes through another round of call routing beginning with the First Digit Table.

Outbound call routing

Outbound call routing refers to calls that originate within Wave and terminate outside Wave (over a trunk connected to the Wave ISM). These calls can include outbound calls from telephone extensions, modems, and FAX machines. A simplified diagram of the outbound call flow is shown in Figure 28-3.

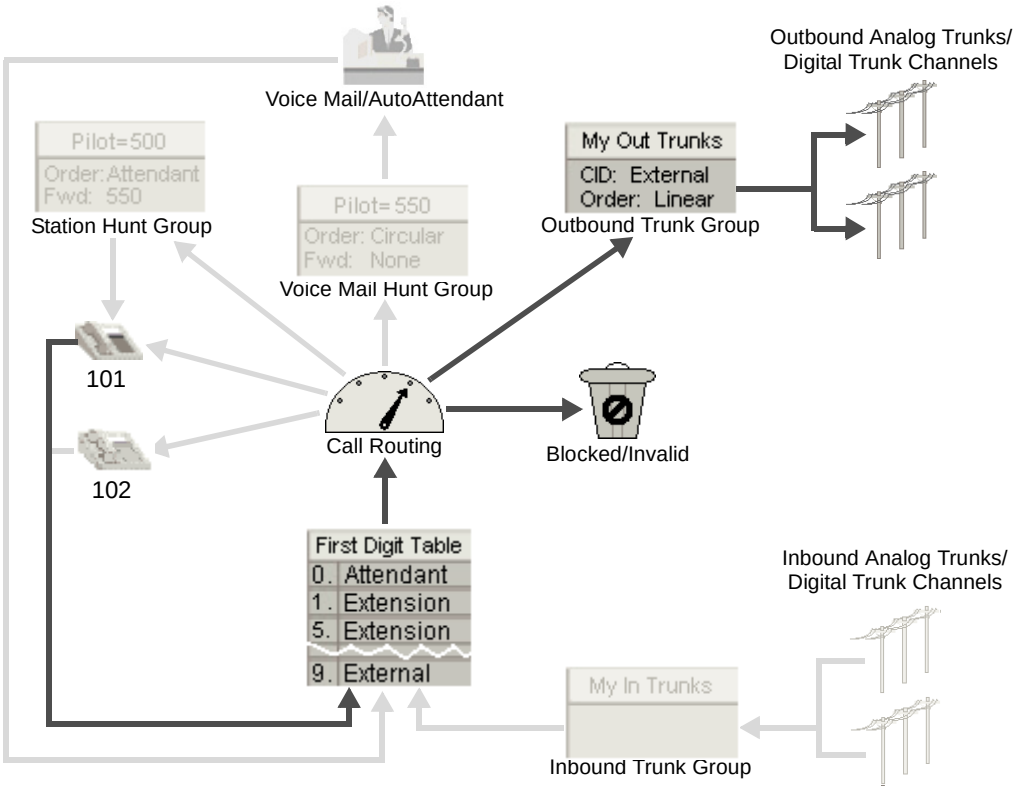


Figure 28-3 Simplified outbound call routing diagram

North American Numbering Plan

Wave collects digits using the North American Numbering Plan by default when processing calls using automatic route selection. The North American Numbering Plan requires telephone numbers to have 10 digits and identifies them using the following numbering scheme:

- a three-digit area code
- a three-digit local exchange (or central office code)
- a four-digit subscriber number

If Wave sees a number (following the external digit) beginning with a number other than a 1, it is identified as a local (7-digit or 10-digit) number. (If the local area codes for 10-digit dialing are included in the First Digit Table, then there is no need to dial a one to send calls to numbers in those area codes.)

If Wave sees a number beginning with a 1, it expects to collect 10 more digits before routing the call. If the number begins with 011, Wave expects a variable number of digits, and will route the call after the dialing time-out expires (or the user presses #).

Access profiles

Access profiles control the types of outbound calls that can be placed from different sources in Wave, such as specific telephones and trunks or channels. Using access profiles, calls can be routed or blocked based on rules you specify. Access profiles assigned to specific call sources can be overridden in the global access profile Special Digits Table and area code table.

For example, if a telephone is assigned an access profile that limits calls made from that telephone to internal extension numbers, and a user dials a number beginning with an external digit, such as 9, the call will be blocked (and the user will hear a fast-busy tone). However, if the Special Digits Table in the global access profile allows the number 911 to be routed to a trunk group, a call to 911 from the restricted telephone will be routed.

Outbound routing tables

Outbound routing tables are reusable, prioritized lists of outbound trunk groups (and IP telephony Signaling Control Points), and associated digit translation rules.

The routing tables allow you to set up outbound routing scenarios such as least cost routing, where Wave will first attempt to place a call over the cheaper trunk group. If the routing scenario fails, (because all the channels in that trunk group were in use, disabled, or disconnected,) the PBX attempts to place the call over the next trunk group specified in the next step in the routing table, and so on. See the example routing table, My Out Route, in Figure 28-4.

An outbound routing table also allows you to translate the dialed number in a different way for each trunk group. For example, some trunks may require long distance numbers to be 10 digits, some 11 digits.

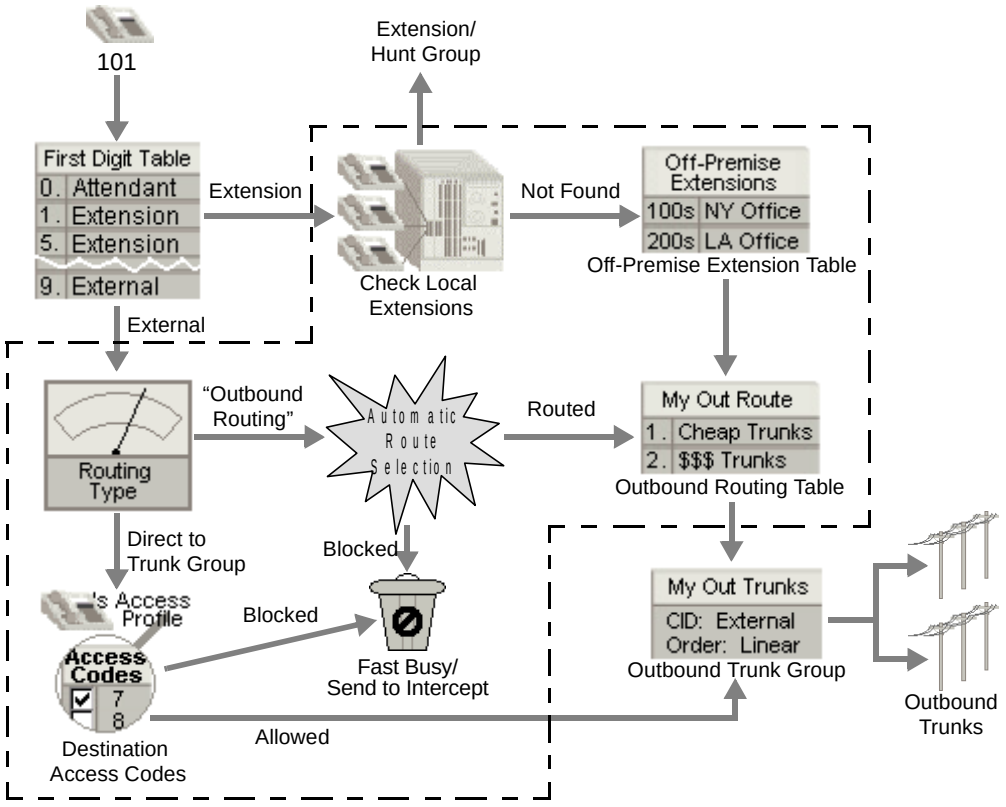


Figure 28-4 Outbound call routing detail

The call routing piece is actually much more complicated than is illustrated Figure 28-3. Figure 28-4 shows more detail in the outbound call routing process. The element labeled Call Routing in the figure in Outbound call routingFigure 28-3 is represented by everything inside the dashed line in the above figureFigure 28-4. As you can see there is more than one path an outbound call can take from the source to the trunk. Each path is described in detail in the following sections:

- Automatic route selection
- Off-premise extensions
- Destination access code / direct to trunk group

Automatic route selection

Use automatic route selection to route calls that connect to the central office. Automatic route selection is ideal when you want different types of outbound calls (local, long distance, toll free, international, etc.) to use different trunks. Automatic route selection allows you to:

- Restrict outbound calls based on call type or caller's privileges
- Select a trunk based on call type (least cost routing)
- Manipulate digits sent to the central office

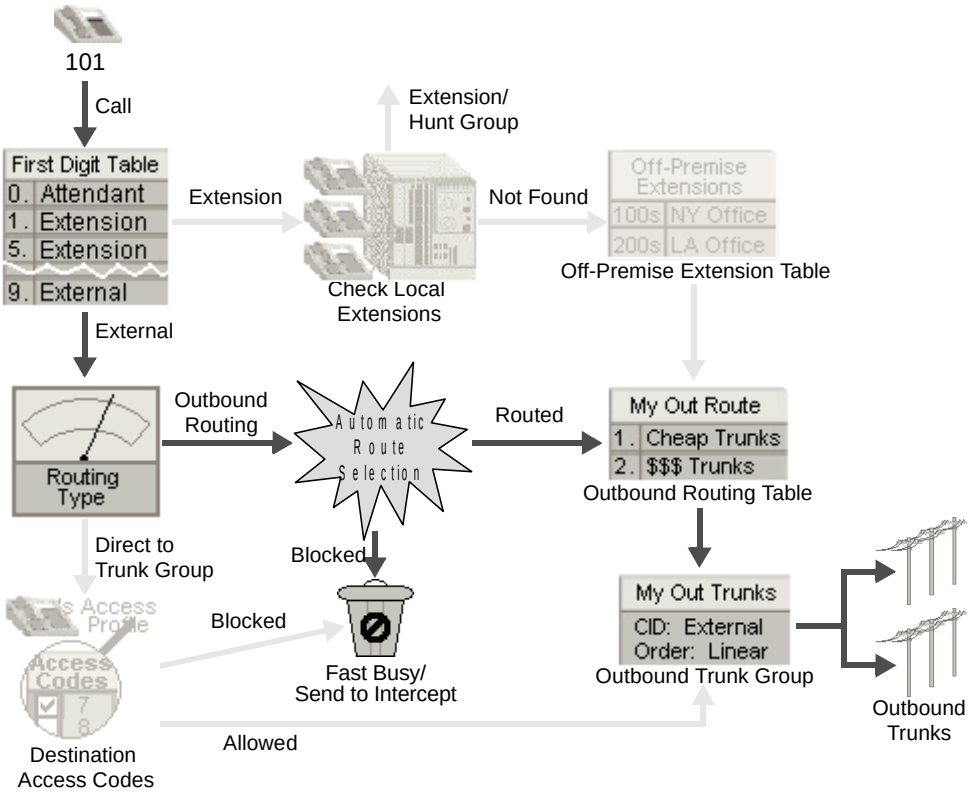


Figure 28-5 Simplified automatic route selection path

Figure 28-5 shows the path by which a call is sent through Wave using automatic route selection. After determining that the call is an external call (based on the first digit

collected), Wave looks up the routing type configured in the First Digit Table. In order to process a call using automatic route selection, the routing type must be **Outbound Routing**. Then the call is passed to the Automatic Route Selection process (detailed in Figure 28-6, and contained in the dashed line).

Special Digits Table

The Automatic Route Selection process first compares the dialed digits to the numbers in the Special Digits Table, which lists numbers that every telephone in Wave is permitted to call (such as 911). In the Special Digits Table, numbers can be blocked, redirected to an internal destination, or routed to an outbound routing table. If a number does not have a match in the Special Digits Table, Wave determines the call type, and sends the call to the next appropriate routing step.

For example, if the number 555-1212 is dialed, it would find no match in the Special Digits Table in Figure 28-6. Since this is a 7-digit number, Wave uses the North American Numbering Plan to determine that this is a local call, and sends the call to the next step in the process.

Home Area Code

When 7-digit numbers are sent to the automatic route selection process, Wave looks up the home area code and sends this information along with the dialed number to the global area code table for further routing attempts.

In our example, Wave looks up the home area code (408), and sends this information along with the dialed number to the next step in the process.

Area Code Tables

Dialed numbers are compared with the steps in the global area code table to find a match. Dialed numbers are first compared with area codes, then local exchange codes. If there is a match in the table for either code, the call is processed as instructed in the table (blocked or routed to an outbound routing table).

If there is no match in the global area code table, the dialed number is compared to the area code table assigned to the call source. If there is a match in this table, the call is processed (blocked or routed to an outbound routing table). Specific area codes tables should contain a rule that handles unmatched calls; blocking or routing them.

In our example, the area code, 408, is compared to the global area code table. Since neither the area code (408) nor the local exchange code (555) are in this table, the number is compared to the caller's specific access profile area code table, where the area code is matched and the accompanying instructions indicate that the call should use My Local Route.

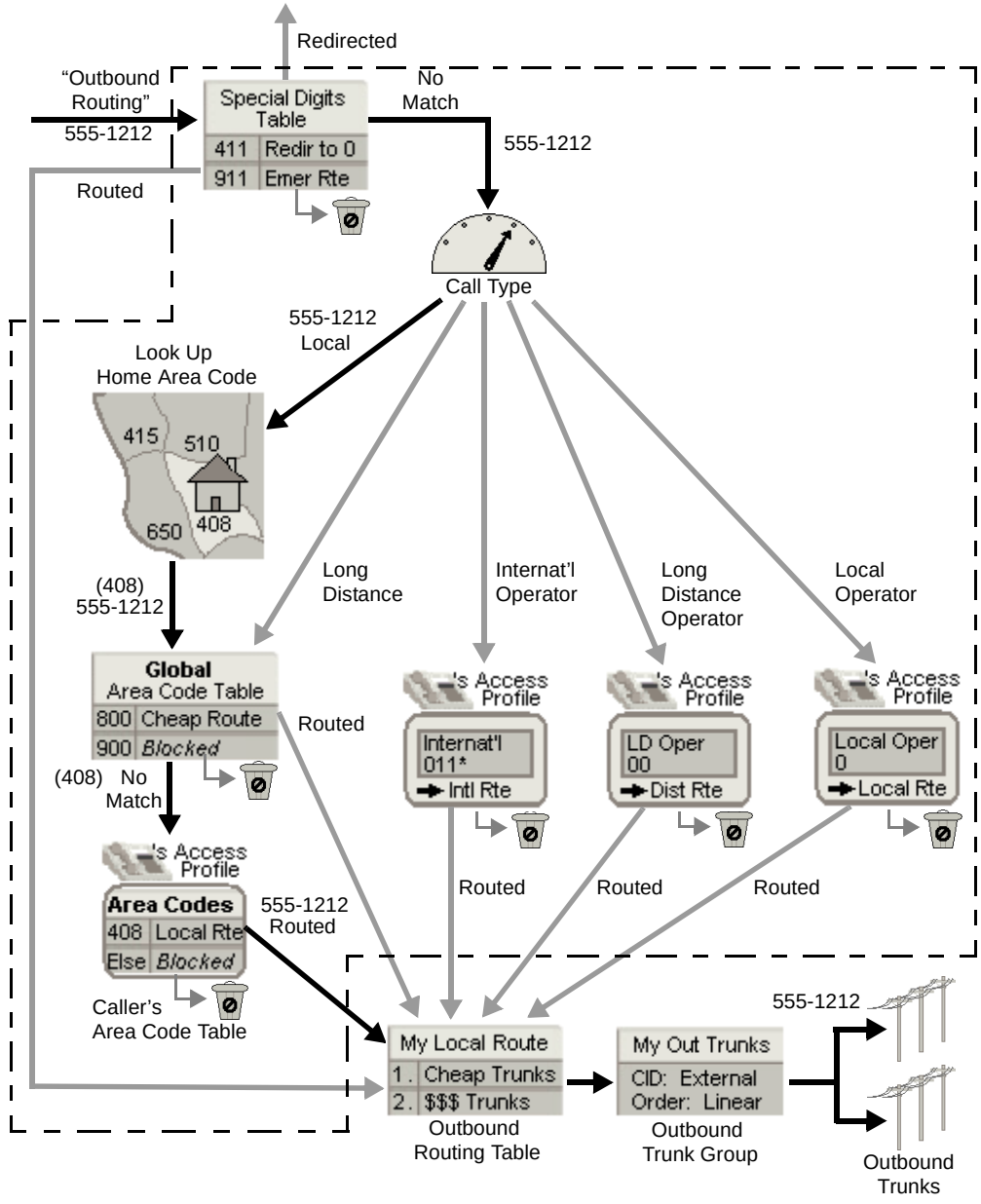


Figure 28-6 Automatic route selection detail showing a local call

Long Distance Calls

When long distance calls are processed using automatic route selection, the process is identical to the local call process, except that Wave skips the step of looking up the home area code.

Operator Calls

Calls to international, long distance, or local operators, can be restricted (or routed) in the call source's specific access profile.

Off-premise extensions

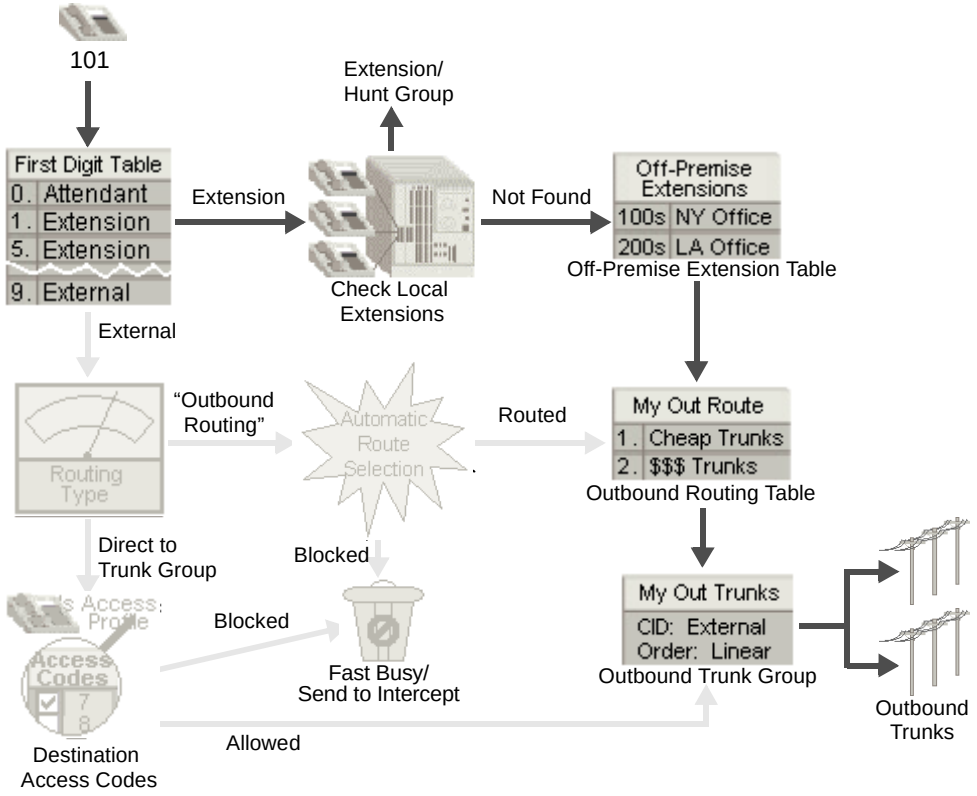


Figure 28-7 Off-premise extension path

Off-premise extensions allow you to route calls to extensions on other PBXs by dialing extension numbers.

Figure 28-7 shows the path by which a call to an off-premise extension is sent through Wave. After determining that the call is an internal one (based on the first digit collected), Wave looks up the local extension numbers.

If the extension number is not configured on the local Wave ISM, Wave checks the off-premise extension table for the number. If the number exists in the table, the call is routed (or blocked). If the number does not exist in the table, the call fails and the user hears a fast busy tone.

Off-Premise Extension Table

The off-premise extension table contains the ranges of extensions that exist on other PBXs (the range can include internal numbers). An outbound routing table is used to translate the number dialed and route the call to the trunk that will send it to the appropriate off-premise telephone (see “Outbound routing tables” on page 28-6). In the outbound routing table you can translate the extension number to the appropriate number that will ring the extension on the far end.

Destination access code/direct to trunk group

Use destination access code / direct to trunk group routing to connect to another PBX that will handle dialing restriction and digit translation. Destination access codes restrict calls per user, not per call type, and do not allow you to do any digit translation, blocking, or alternate routing based on the dialed number. All callers using a particular access code use the same trunk group and are allowed to dial any number on the PSTN.

It is very important that you set the digit collection rules for each destination access code properly in the First Digit Table (see “Creating destination access codes” on page 9-19). Collecting too many or too few digits will cause calls using the access codes to fail. Using the call numbering plan (North American Numbering Plan by default) can help you avoid problems with calls bound for the PSTN.

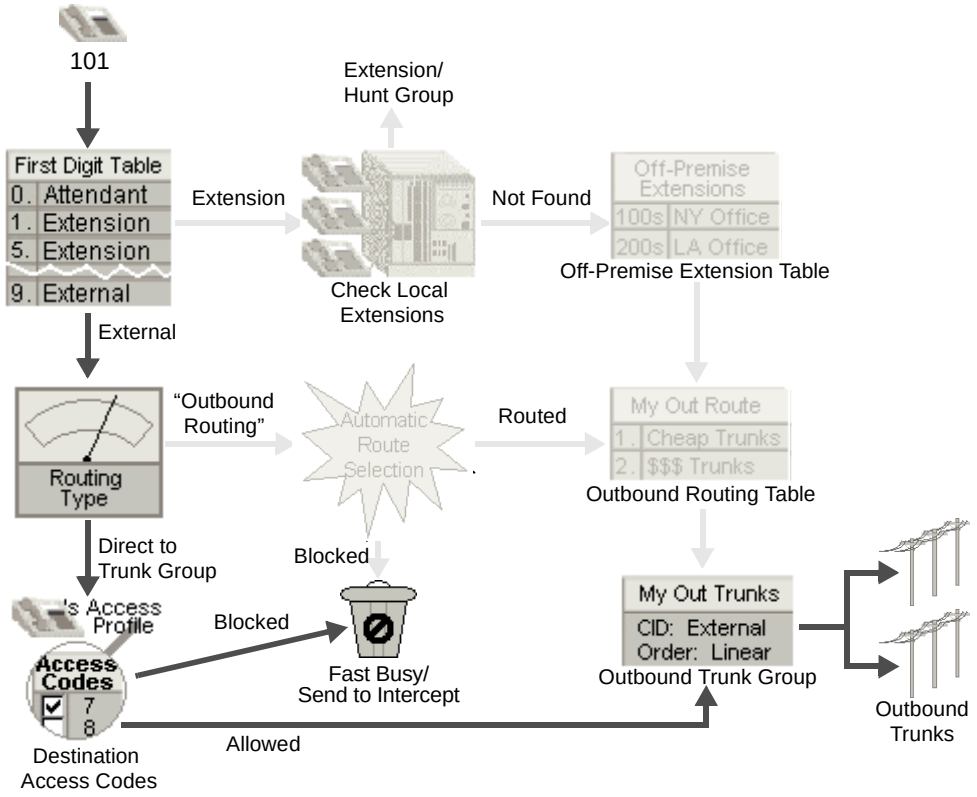


Figure 28-8 Simplified outbound call routing scenario highlighting destination access code / direct to trunk group routing

Destination Access Code Table

A destination access code table allows Wave to verify that a specific extension has permission to use a destination access code(see Destination Access Codes in Figure 28-8). Permission to use a destination access code is enabled in each of the destination access code tables associated with a specific access profile. Once an extension has permission to use the destination access code, the only restriction to the types of calls that can be made are the number of digits you collect.

Inbound call routing

Figure 28-9 illustrates the simple inbound call path from the inbound trunks to the extensions and voice applications.

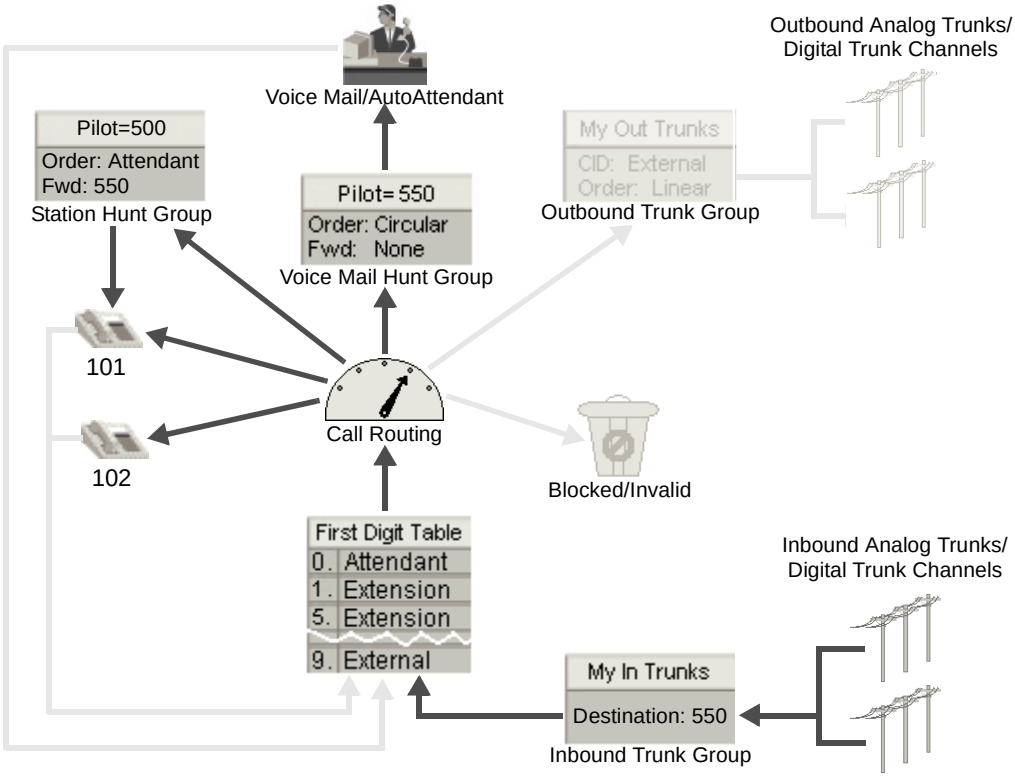


Figure 28-9 Simplified inbound call routing diagram

Inbound call routing must be configured differently depending on how the trunks are provisioned and what call information you receive from the far end (central office or another PBX). The digit collection and translation detail, between receiving calls on the trunks and routing those calls, is explained in each of the following sections:

- Trunks receive no digits
- Wink start DID trunks
- ISDN trunks

- Trunks receive digits from another PBX

Trunks receive no digits

When you configure inbound routing on trunks that receive no digits (usually analog trunks used for calls to the company main telephone number), you will either route all calls on these trunks to a single destination, or route calls to different destinations based on a schedule. To accomplish this, use an inbound routing table with the Scheduled Routing option.

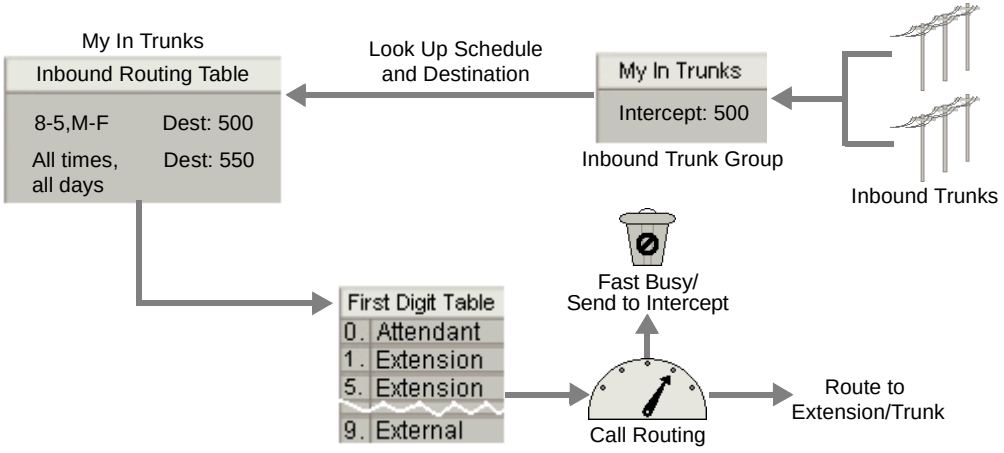


Figure 28-10 Scheduled routing inbound call routing detail

Inbound Routing Table

An inbound routing table is a prioritized list of digit- and schedule-matching translation rules for calls received on a particular trunk group. Inbound routing can be based on any of the following:

- dialed number (DID, DNIS, Lead TN)
- calling party number (Caller ID, ANI)
- time of day and day of week
- all of the above

Inbound routing tables interpret digits collected from trunks, and translate them to numbers that can be interpreted by the First Digit Table. After receiving digits from the central office, the PBX searches the inbound routing table for the *first* matching step.

If a match is found, the call will be translated and sent to the corresponding destination number listed in the table. Then the First Digit Table uses the information to determine the call type and start the call routing process. If there is no match in the table, the call cannot be routed and is sent to the intercept destination specified in the inbound trunk group configuration.

Observe the order that the steps appear in the inbound routing table in Figure 28-10. The first and second step overlap, in the days of the week and times of the day they cover. The first step overrides the second step during the overlap.

In this example, the first step is configured to route calls to a live operator during normal business hours. The second step is configured to route calls to the AutoAttendant during non-business hours. The first step overrides the second step between the hours of 8:00 A.M. and 5:00 P.M., Monday through Friday.

Wink start DID trunks

Wink start DID trunks receive digits from the central office, which are used to route calls to various destinations in Wave. Since this type of trunk receives digits, you will want to use an inbound routing table that specifies digit collection rules.

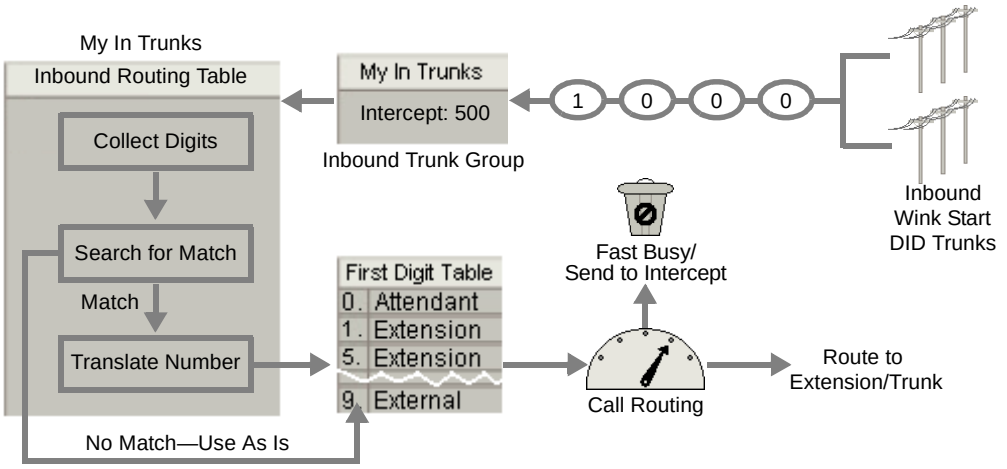


Figure 28-11 Wink Start DID inbound call routing detail

Digit Collection

On wink start DID trunks you will receive digits from the central office one at a time as shown abovein Figure 28-11. Wave keeps collecting digits until the number of digits collected matches the number of digits in the longest Dialed Number value in the inbound routing table.

Table 28-2 Sample inbound routing table

Step	Dialed Number	Destination	Description
1	1000	550	AutoAttendant
2	1xxx	2xxx	Extensions (2001-2075)

For example, if the inbound routing table has two values for Dialed Number (see Table 28-2), Wave will wait to collect four digits. If Wave receives more than four digits, only the first four digits are considered and the rest are ignored. If Wave only receives three digits, the digit collection times out after a period, and Wave attempts to place the call with the digits it received.

Digit translation

The collected digits are compared with the steps in the inbound routing table. You can specify a destination that uses digits in the dialed number by using x's in the

destination number. For example, if the dialed number is 1011, and the destination for numbers matching 1xxx is 2xxx, then the call is sent to extension 2011.

It is very important to place the steps in the order they must be considered by Wave . For example, if Wave has an inbound routing table that contains two steps (see Table 28-2), and it receives the digits 1-0-0-0, the first step is matched and the second step is not considered.

If you reverse the steps in Table 28-2, the call would not go to the AutoAttendant (550). Instead, Wave would attempt to locate extension 2000, which does not exist, and the call fails (or is routed to the intercept destination, if one is configured).

If there is no match between the number received and the steps in the table, the number is sent, as is, to the First Digit Table for further interpretation and routing. If the call cannot be routed, it will be sent to the intercept destination configured in the inbound trunk group.

Intercept destination

The intercept destination is used to intercept calls that cannot be routed. For example, if you have a block of DID numbers, 1000-1999, but you are only using 1001-1075, any call to numbers 1076-1099 will be sent to the intercept destination, if you specify one (commonly the AutoAttendant (550), or Attendant hunt group (0)). If you do not specify an intercept, the caller will hear a fast busy tone.

ISDN trunks

ISDN sends all the digits in the dialed number at once in the setup message (see Figure 28-12); however, the length of digits received may vary.

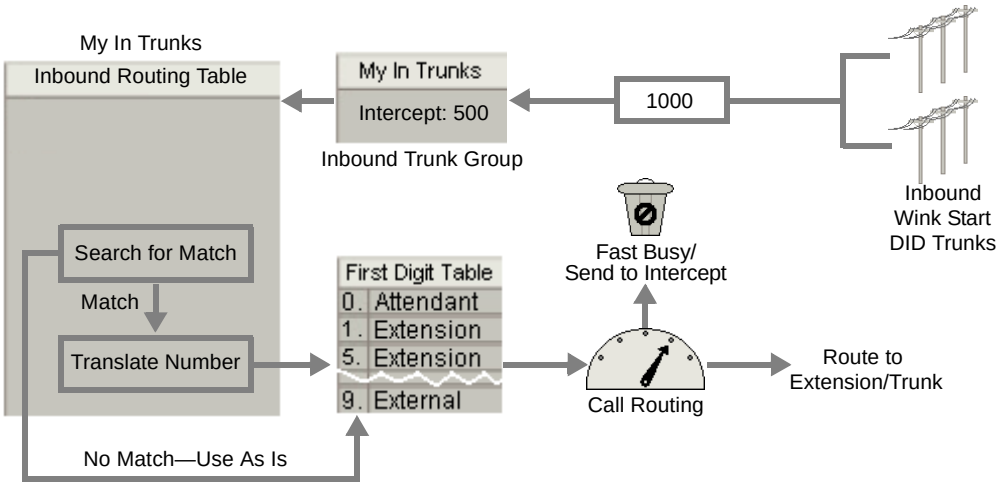


Figure 28-12 ISDN inbound call routing detail

In this case it is best to enter *Default* for the Dialed Number and *2xxx* for the Destination, as shown in Table 28-3. This tells the PBX to keep the last three digits and prepend a 2, regardless of how many digits are received.

Table 28-3 Sample inbound routing table

Step	Dialed Number	Destination	Description
1	Default	2xxx	AutoAttendant

Trunks receive digits from another PBX

When the inbound trunks receive digits from another PBX, digit translation should be handled by the PBX sending the digits, therefore no translation is necessary. In this case you should send the digits straight to the First Digit Table for digit collection and interpretation (see Figure 28-13).

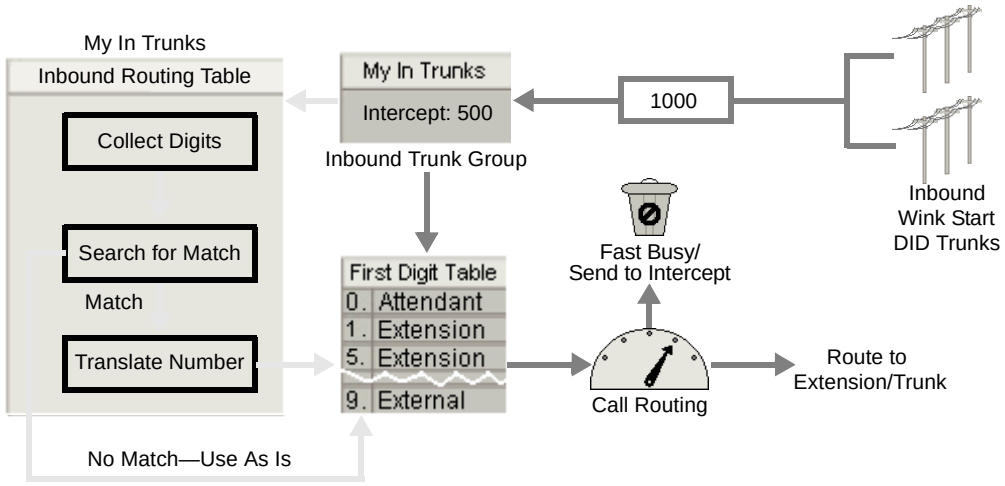


Figure 28-13 Receive digits from another PBX inbound call routing detail

Tandem call routing

A special flavor of inbound call routing is tandem call routing. Tandem calls are calls to Wave that are routed to external telephone numbers. Figure 28-14 illustrates the tandem call route. Scenarios include tie-line external calls (where another PBX is sending the digits for an external call), off-site call forwarding, off-site transferring, and conferencing where two or more parties are external.

This section only discusses the configuration for a tie-line external call. The tie-line external call variety of a tandem call is accomplished by relying on the calling PBX to send all the digits necessary to route the call, including the external access code (default 9), and then using the local Wave outbound call routing configuration to route the call back out on an outbound trunk group. You must configure the inbound trunk group to use the First Digit Table for digit interpretation, and specify an access profile for tandem calls. When the digits are passed to the First Digit Table, Wave picks up the associated access profile and attempts to route the call according to the call routing configuration associated with the first digit in the received number.

Other critical gateways are to enable the trunk-to-trunk connection and set the trunk-to-trunk connection time-out in the General Settings applet. See “External call routing restrictions” on page 18-13 for more information about these settings.

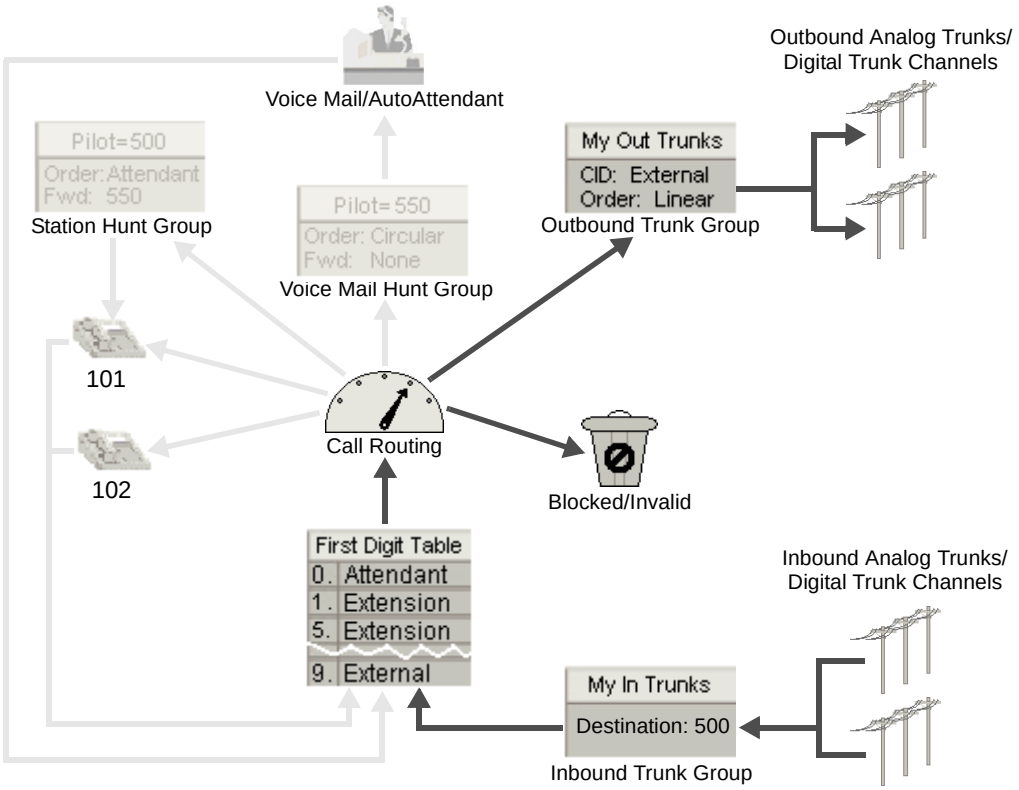


Figure 28-14 Simplified tandem call routing diagram

Hunt groups

A hunt group is a container extension (pilot number) that allows you to associate many user extensions or system ports to a single number that can be dialed or to which calls can be routed. When the hunt group pilot number is dialed, the hunt group configuration determines the order in which the member extensions or ports are dialed. For example, the Attendant hunt group has pilot number zero by default. If you dial zero, the member extensions of the Attendant hunt group telephones will ring in the defined order.

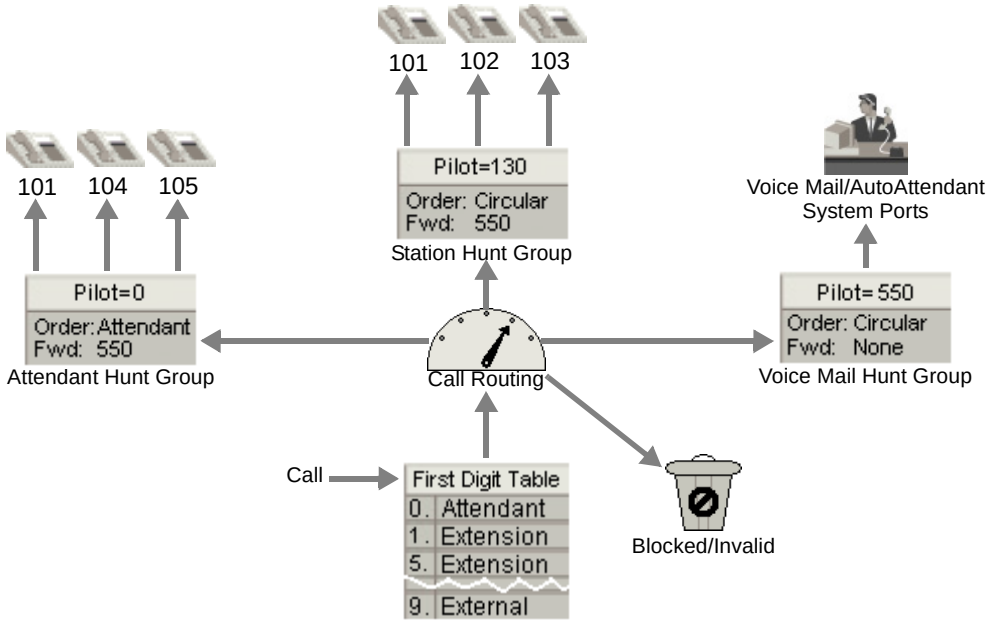


Figure 28-15 Hunt group

There are two types of hunt groups:

- **Station**—A collection of user extension numbers. You will typically use this hunt group type for all of the hunt groups in your office, such as a group of administrative assistants or a sales group (see Pilot=0 and Pilot=130 in Figure 28-15).

  You can include a member in more than one station hunt group. See extension 101 in the attendant and station hunt groups (pilot=0 and pilot=130) in Figure 28-15.

- **Application**—A collection of system ports for Voice Mail, or other Vertical Communications applications, such as Call Navigator (Call Navigator) (see Pilot=550 in Figure 28-15).

Note: The Wave system has a maximum of 20 groups, including hunt groups, trunk groups, and zone paging groups.

Hunt group hunt orders

The hunt order of a hunt group describes the order in which the member extensions ring. You can set linear, circular, ring, and attendant hunt orders.

- Linear—Rings the first available extension in the hunt group, always starting from the top of the hunt group list. If the first extension does not answer, the PBX rings the next available extension in the hunt group. If the second extension does not answer, the PBX rings the first extension again. If no one answers the call the caller is transferred to the hunt group's no answer forward destination. If all member extensions are unavailable the call is transferred to the busy forward destination.
- Circular—Rings the member extensions of the hunt group in order until the call is answered, or all available extensions are rung (see Pilot=130 in Figure 28-15). The next call to the hunt group call rings the extension following the last extension that answered a call (or the last extension before the call was transferred to the forward destination).

  For example, the station hunt group pilot number 130 in Figure 28-15 has three members: extensions 101, 102, and 103. When a call goes to hunt group 130, the PBX dials extension 101. If it is available, it will ring. If extension 101 answers the first call, the next time a call goes to hunt group 130, the PBX attempts to ring extension 102 first, then extension 103, and then extension 101 again. After each available extension is rung once, and no one answers the call, the call is forwarded to the no answer forward destination.
- Ring All—Rings all member extensions at the same time and connects the call to the first extension that answers.

  This hunt order is valid for station hunt groups only.
- Attendant—Hunt group members with the Attendant hunt order (see Pilot=0 in Figure 28-15) are typically stations that can handle multiple calls simultaneously, such as members running OfficeAttendant. If all members of a group have at least one call, the call is assigned to the first member found with the greatest number of available lines. In the case of a tie, the hunt group assigns the calls in a fashion similar to a hunt group with a Circular hunt order.

  Members running OfficeAttendant can receive up to eight calls. For example, a hunt group member running OfficeAttendant with six current calls will get additional calls before a hunt group member with one current call and not running OfficeAttendant. This is because the member running OfficeAttendant has two available lines, while the other has only one line available.

If a member using a standard telephone is in an Attendant hunt group and currently on a call, the member will hear a call waiting tone and the call will be queued to that extension.

This hunt order is valid for station hunt groups only.

Default hunt groups

The default hunt groups are preconfigured. These hunt groups use the default system and user extensions as their members. There are three default hunt groups:

- **Attendant (station)**—The Attendant hunt group uses the pilot number zero (0). The purpose of the Attendant hunt group is to direct calls to one or more extensions that serve as the receptionists in your organization. The Attendant hunt group hunts in a linear fashion.

  By default, the Attendant hunt group has no members. By adding the member extensions you want to serve as the receptionist(s) at your site, you can connect incoming trunks to the Attendant hunt group.

  Caution: *It is not recommended that you route inbound calls to zero because there can be no Voice Mailbox associated with this destination.*

- **Modem Hunt Group (station)**—This hunt group (pilot 570) is used to connect incoming trunks to the modem(s) on the Integrated Services Card by setting the 570 pilot number as the default destination for the Modem trunk group. This trunk group ensures that any trunk group using 570 as the default destination will ring the first available modem.

  For the RS2-C card, which includes two modems, the Modem hunt group contains two non-dialable member extensions. Each member extension rings one of the internal 56 Kbps modems on the Integrated Services Card. This means that users can dial one extension—570—to reach either modem. The Modem hunt group hunts in a circular fashion. For the RS3-C and RS3A-C cards, the Modem hunt group contains only one member extension.

- **Voice Mail (application)**—The Voice Mail hunt group (pilot 550) is a collection of system ports. Each member of the Voice Mail hunt group is a single Voice Mail port that is used to play Voice Mail menu prompts and messages. When anyone dials the Voice Mail hunt group pilot number, they are connected to a Voice Mail port. The Voice Mail hunt group hunts for system ports in a circular fashion.

Outside lines

Outside lines are ideal when users are used to a key system environment, or users want to see the status of trunks on their telephones. Outside lines connect a digital telephone directly to a trunk using an outside line key (button) and a mapping entity called an Outside Line. The routes created between the outside line keys on each digital telephone and trunks simulate a key system. Outside lines are used to make outbound and receive inbound calls.

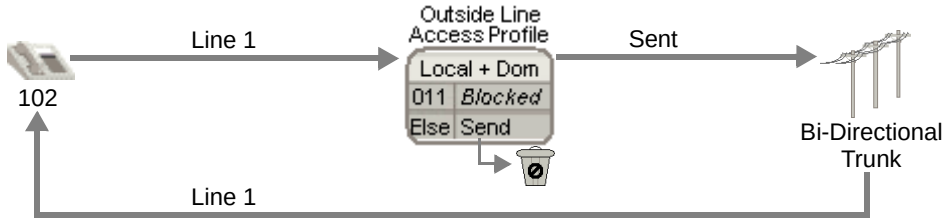


Figure 28-16 Outside line

As shown in Figure 28-17 and Figure 28-18, the outside line keys from each telephone are linked to one or more trunks. Outside lines have special outside line access profiles associated with them that determine what types of calls (local, long distance, domestic, etc.) can be placed on them, and provide digit translation.

Outside line keys can be associated with one or more trunk lines. The single call variant of an outside line requires one outside line key associated with one trunk. In the multiple call variant of an outside line, an outside line key is associated with more than one trunk. There is a significant difference in the user experience between the single and multiple call outside line variants.

Single call variant

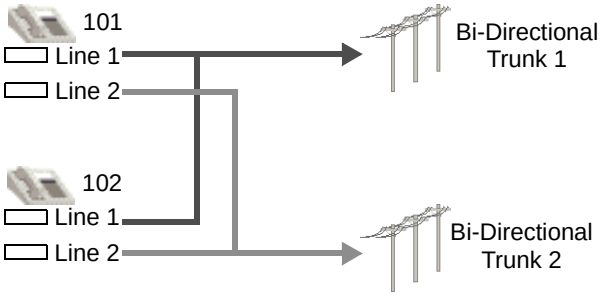


Figure 28-17 Outside line single call variant

In the single call outside line variant a single trunk is associated with an outside line key on the digital telephone. The LED next to the Outside Line key indicates when the trunk is in use by any telephone. For outbound calls, when a user presses the Outside Line key, the LED is lit red where it appears on other telephones, and cannot be used on any other telephone. Once the call is connected the LED indicates whether break-in is allowed. For inbound calls, the Outside Line key LED flashes yellow, and the telephone can be configured to ring. Once the call is answered the LED indicates whether break-in is allowed.

Multiple call variant

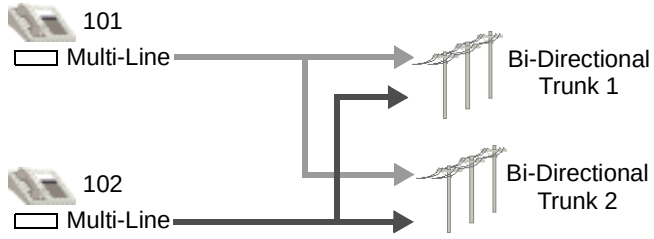


Figure 28-18 Outside line multiple call variant

In the multiple call outside line variant an Outside Line key on a digital telephone is associated with more than one trunk line. If any trunk line is available for outbound calls, the Outside Line key LED will not be lit on any telephones with the key. The LED next to the Outside Line key is red when all of the associated trunk lines are in use. For inbound calls, the Outside Line key LED flashes yellow, and the telephone can be

configured to ring. When the call is connected, if there are any available trunk lines the Outside Line LED will not be lit. If no trunks are available the LED is red. Break-in is not supported in the multiple call variant.

Automatic Line Selection

Automatic Line Selection changes the behavior of your digital telephone lines (primary line, secondary line appearances, and outside lines) by allowing you to automatically answer a call that is ringing on one of those lines, or providing dial tone on the first available line, without pressing the line keys.

The following rules apply to Automatic Line Selection:

- Your primary line is always subject to Automatic Line Selection behavior.
- Your lines configured for Automatic Line Selection are selected in the order they appear on the telephone. You can choose to have the primary line always selected first. See “Primary” on page 10-14.
- When one or more lines are ringing, and you lift the handset or press Speaker / Mute, the first ringing line configured for Automatic Line Selection is answered.
- When no lines configured for Automatic Line Selection are ringing, and you lift the handset, press a digit, or press a feature key (Speaker / Mute, Auto Dial, System Speed Dial, Redial, Message Waiting, or Flash) you receive dial tone on the first idle line configured for Automatic Line Selection.

If you have outside lines configured with Automatic Line Selection:

- Pressing an external access code (or using an Auto Dial key or System Speed Dial number including an external access code) provides dial tone on the first idle outside line configured for Automatic Line Selection.

Automatic Line Selection on line appearance keys

The examples that follow use the digital telephone line key configuration shown in Figure 28-19. The first key is the primary line key configured for extension number 100. The second key, 130, is a secondary line appearance that is not configured for Automatic Line Selection. The third key, 140, is a secondary line appearance that is configured for Automatic Line Selection (ALS).

Example 1: Secondary line without ALS ringing

In Figure 28-19, line 130 is ringing, and is not configured for Automatic Line Selection (ALS). Lifting the handset, or pressing Speaker / Mute, pressing Auto Dial, Redial, or Flash selects the primary line.

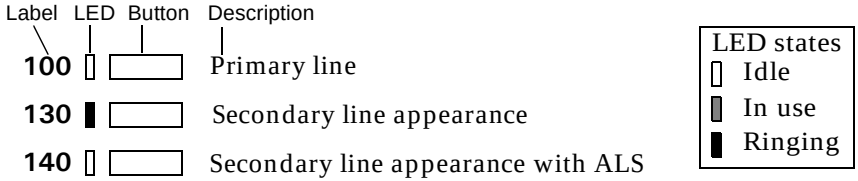


Figure 28-19 Secondary line 130 ringing

Example 2: Secondary line with ALS ringing

In Figure 28-20, both lines 130 and 140 are ringing. Lifting the handset, or pressing Speaker / Mute, answers the call on 140. Pressing Auto Dial, Redial, or Flash selects the primary line.

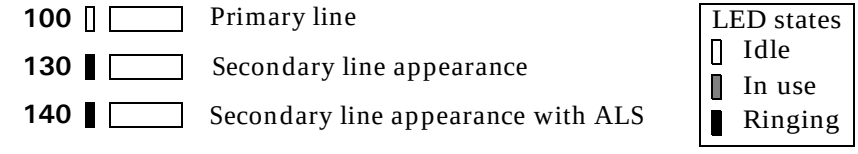


Figure 28-20 Secondary line with ALS ringing

Example 3: Primary line in use

In Figure 28-21, the primary line is in use by another telephone. Lifting the handset, or pressing Speaker / Mute, selects line 140. Pressing Auto Dial, Redial, or Flash also selects line 140. To select line 130, you must press 130.

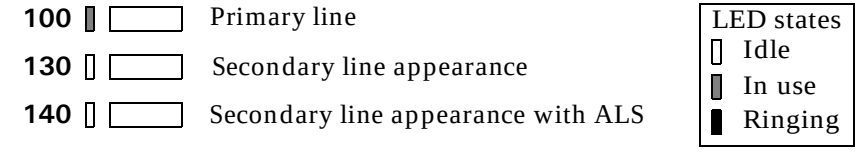


Figure 28-21 Primary line in use

Automatic Line Selection on outside line keys

The examples that follow use the digital telephone line key configuration shown in Figure 28-22. The first key is the primary line key configured for extension number 100. The second key, Line 1, is an outside line that is not configured for Automatic Line Selection. The third key, Line 2, is an outside line that is configured for Automatic Line Selection (ALS).

Example 1: Primary line in use

In Figure 28-22, the primary line is in use. Lifting the handset, pressing Speaker / Mute, or dialing the external access digit selects Line 2. Pressing Auto Dial, Redial, or Flash produces no result. To select Line 1, press Line 1.

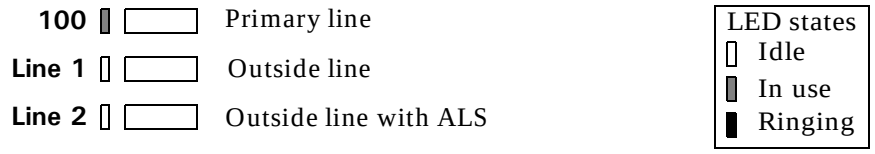


Figure 28-22 Primary line in use

Example 2: Outside line without ALS ringing

In Figure 28-23, Line 1 is ringing. Lifting the handset, or pressing Speaker / Mute gives you dial tone on extension 100. Pressing Auto Dial, Redial, or Flash also selects extension 100. Dialing the external access digit selects Line 2. To answer the call on Line 1, you must press Line 1.

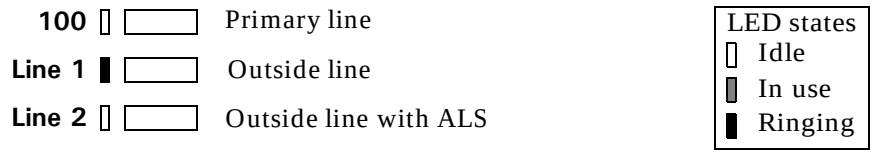


Figure 28-23 Line 1 ringing

Example 3: Outside line with ALS ringing

In Figure 28-24, Line 2 is ringing. Lifting the handset, or pressing Speaker / Mute answers the call on Line 2. Pressing Auto Dial, Redial, Flash, or dialing the external access digit selects extension 100. To select Line 1, you must press Line 1.

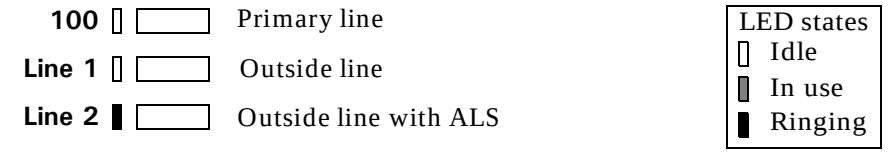


Figure 28-24 Line 2 ringing

Understanding Vertical Wave Data Networking

CHAPTER CONTENTS

This chapter explains data networking in Wave.

Overview of data networking in Wave

Wave provides full routing support. The network data subsystem interfaces with network-based applications, such as Web and email servers, and communicates with the Ethernet drivers. The Microsoft Windows server/operating system embedded in Wave integrates fully with core applications, processes, and hardware.

Wave combines the features of an Ethernet hub, a router, and a remote access server, supporting up to 84 LAN users (depending on the number of station cards in your system)

WAN technology

Using a single WAN trunk for voice, the Wave ISM provides multiple WAN services, including access through T-1 digital, ISDN PRI, and analog connections.

LAN technology

If you have an RS2-C Integrated Services Card

The Ethernet 10Base-T ports on the Integrated Services Card (ISC) form a shared LAN, typically supporting a single LAN user/node per installed Ethernet port. The Integrated Services Card has a 12-port Ethernet segment with a network interface to RRAS.

The first Ethernet hub card installed may merge with the Integrated Services Card to form a segment of 36 ports.

If you have an RS3-C Integrated Services Card

The Ethernet 10/100Base-T switched ports on the Integrated Services Card (ISC) form a shared LAN, typically supporting a single LAN user/node per installed Ethernet port. The Integrated Services Card has a 4-port Ethernet segment with a network interface to RRAS.

The first Ethernet hub card installed may merge with the Integrated Services Card to form a segment of 16 or 28 ports, depending on if your Ethernet hub card has 12 or 24 ports.

If you have an RS3A-C Integrated Services Card

The Ethernet 10/100Base-T switched ports on the Integrated Services Card (RS3A-C) form a shared LAN, typically supporting a single LAN user/node per installed Ethernet port. The Integrated Services Card combines the 4 ports on the RS3-C and the 8 ports on the RS3A-C for 12 total switched 10/100Base-T Ethernet ports with a network interface to RRAS.

Each subsequent 10/100Base-T Ethernet hub card can automatically switch across the Wave ISM backplane to form one 10/100Base-T LAN segment.

Network services

Wave uses the following Microsoft Windows services for communications routing:

- Routing and Remote Access Service (RRAS)

- Dynamic Host Configuration Protocol (DHCP)
- Windows Internet Name Service (WINS)
- Domain Name Service (DNS)

Microsoft's Routing and Remote Access Service (RRAS)

RRAS is Microsoft's open, extensible platform for routing and internetworking, offering LAN-to-LAN networking and remote office connectivity over private wide-area networks (WANs) or via the Internet using secure, virtual private networks (VPN).

You will configure much of Wave's data configuration via RRAS, including configuring RRAS *interfaces* (representations of connections over a network adaptor) and *adaptors* (representations of the physical point of attachment to a network segment).

Note: For detailed information about RRAS, see the Microsoft Windows NT *Routing and Remote Access Service Administrator's Guide*.

Ethernet terminology

The following Ethernet terms are relevant when setting up Ethernet hub cards in a Wave ISM:

- **Merged Segment**—The Integrated Services Card merges with the first Ethernet hub card to its right, creating a single merged Ethernet segment. A merged segment can be part of a broadcast domain.
- **Network Adapter**—Network adapters, also known as router interfaces, enable the router to perform packet routing between LAN segments. Each Ethernet segment must have its own network adapter.
- **Switch**—Each 10/100Base-T Ethernet hub card and Integrated Services Card is equipped with a switch, allowing it to switch packets over a high-speed uplink to other 10/100Base-T Ethernet hub cards installed in the Wave ISM. The 10/100Base-T Ethernet hub cards can be combined to form one Ethernet segment.

The Wave LAN, segments, and subnets

When a network is composed of hubs and routers, segments and subnets are essentially the same. When designing your network, follow these rules:

- If you have 10/100Base-T Ethernet hub cards, they switch across the backplane to join the nearest switched segment to its left. If there are no switched segments to its left, it looks to the right.
- Each port on a router has to be on the same subnet as all machines to which it is connected.
- A machine's subnet has to match that of the router closest to it.
- Only routed packets are propagated from one hub to another.

Note: A single switched Ethernet domain is faster and requires less system resources then routing between segments.

Note: It is acceptable to configure an Ethernet hub card with multiple IP addresses, and for the card to have multiple subnets. While it is sometimes useful to preserve a pre-Wave configuration, we recommend that you do not do this normally, as it can be confusing to administer.

Integrated Services Card

Depending on the type of Integrated Services Card installed in your Wave ISM, your Integrated Services Card will provide the following router ports for RRAS:

Integrated Services Card 2 (RS2-C)

- one LAN router interface supporting the 12 10Base-T Ethernet ports
- two 56 Kbps modem router ports that can be used as either asynchronous modem ports or as 56k/64k HDLC ports

Integrated Services Card 3 (RS3-C)

- one LAN router interface supporting the 4 10/100Base-T switched Ethernet ports

If an Ethernet hub card is installed in the Wave ISM, the RS3-C , merges with the closest Ethernet hub card to the right of the Integrated Services Card. This merge provides a single LAN router interface (network adapter) supporting all 16 or 28 Ethernet ports (4

on the RS3-C + 12 or 24 on the Ethernet hub card). The merged segment optimizes system throughput and augments performance.

Integrated Services Card 3A (RS3A-C)

- one LAN router interface supporting the 12 10/100Base-T switched Ethernet ports

If an Ethernet hub card is installed in the Wave ISM, the RS3A-C, merges with the closest Ethernet hub card to the right of the Integrated Services Card. This merge provides a single LAN router interface (network adapter) supporting all 24 or 36 Ethernet ports (12 on the RS3A-C + 12 or 24 on the Ethernet hub card). The merged segment optimizes system throughput and augments performance.

Note: You can prevent the Integrated Services Card from merging with the closest Ethernet hub card by re-enabling the network adapter using the Network Services and Adapters applet in the Management Console.

10/100Base-T Ethernet hub cards

Each 10/100Base-T Ethernet hub card provides 12 or 24 10/100Base-T Ethernet ports. If there is no LAN router interface installed, the 10/100 card switches over the backplane to join the first switched Ethernet segment formed by another 10/100 card to its left. If there is no other 10/100 card segment to the left, it looks to the right.

The Wave ISM auto-detects the slots in which the 10/100Base-T Ethernet hubs were installed and automatically switches them across the backplane to form a single switched 10/100Base-T Ethernet segment. The Wave ISM determines the network adapter to use by looking to the left of the card for a 10/100Base-T card with a network adapter; if there is no 10/100Base-T card to the left with a network adapter, it looks to the right.

Caution: *Do not install a cross-over Ethernet cable between two 10/100Base-T Ethernet hub cards. Instead of auto-partitioning the two cards, it will cause a switch loop between the cards and the Wave ISM will become inoperable.*

Dial-up and persistent connections

The Wave ISM supports various kinds of dial-up and persistent connections.

Dial-up connections

A *dial-up connection* is created and ended on an as-needed basis. A dial-up connection typically has a phone number associated with it. The connection is made only when a phone call connects the Wave ISM with an ISP or with a corporate headquarters over a WAN. A dial-up connection (also known as a switched connection) is the RRAS default.

Using ISDN or the modem port(s) on the Integrated Services Card, you can configure the Wave ISM for dial-up connections, routing data using Microsoft RRAS. Both Wave modems and ISDN serve as system resources for dial-in and dial-out calls.

Dial-in calls come from a remote office over a digital or analog trunk *to* Wave. Modems and ISDN are configured so that remote dial-in calls will automatically connect through the Wave ISM.

Dial-out calls are made *from* Wave over a digital or analog trunk to an Internet Service Provider or to another site. The type of dial-out calls made when a user requests an Internet connection, known as dial-on-demand or *demand-dial calls,* depends on trunk type and protocols in use, as well as modems, and can be set up through the RRAS administrator application.

Caution: *Do not set an interface for dial-on-demand if you intend to use it for continuous monitoring of the Wave ISM. If the monitoring traffic is high, the connection will never be disconnected. In addition, if you are monitoring the Wave ISM using SNMP over the dial-on-demand connection when the connection is disconnected, this will generate an SNMP trap causing the connection to be reconnected. The end result is that the connection will continually be going up and down.*

Note: The Wave ISM supports *dial-on-demand,* also called dial backup, over analog telephone lines. If the Fault Monitor settings have been configured (see "Accessing the Fault Monitor error log" on page 24-11) and a digital line fails, a dedicated 2400-baud modem automatically dials a pager over analog lines on system failure.

Wave dial-in connection default settings

The two 56 Kbps modems on the Wave ISM are set up for configurable dial-out functionality and to automatically answer incoming calls to the default Modems hunt group (extension 570). When a client machine dials in, the default Modem trunk group

rings the default Modems hunt group. The Modems hunt group rings the modems in a circular fashion until it finds a free modem extension to answer the dial-in call.

Note: For calls from outside Wave to connect, the Modems hunt group extension must be bound to a telephone number that can be reached from outside Wave.

Persistent connection

A *persistent connection* is always logically and physically active. It may also be referred to as a dedicated account. While the connection is intended to be constantly active, the physical connection may be disconnected if the Wave ISM is restarted.

The Wave ISM also supports a persistent ISDN connection.

A persistent connection may be a *permanent connection*—both physically and logically active—such as a digital line that goes to your ISP. All permanent connections are persistent.

Wave data routing

A *router* is a device that moves data packets between networks. A router can be used to link LANs together, locally or remotely, as part of a WAN. *Routing* is the process of delivering messages from the sender to the receiver using the most appropriate path through one or more networks.

The Wave ISM uses RRAS, a software router, as a LAN-to-LAN, LAN-to-WAN, and WAN-to-WAN router for IP traffic. RRAS IP routing is installed and enabled by default, so LAN routing configuration is, for the most part, automatic. Depending on your particular Wave configuration, you may need to configure routing protocols and / or LAN-to-WAN interfaces.

You can configure routing protocols, including the Routing Information Protocol (RIP) and Open Shortest Path First (OSPF), as well as default and static routes, on Wave when multiple routers are connected to your network. You can also configure Internet Packet Exchange (IPX), which uses the routing protocols RIP and SAP, as an alternative to IP.

Note: By default, these routing protocols are installed but not configured, as they are not required for typical configurations. If you need to configure these, see "Configuring network routing protocols" on page 22-2.

IP addressing

All network interfaces on Wave must have valid *static* IP addresses assigned, even if Wave is connected to a network server. In determining IP addresses, follow these guidelines:

- If you have a WAN connection and a reserved, registered address pool assigned through an Internet license, use the beginning or ending range for static IP addresses. For example, if you have a license with the range x.x.x.1 to x.x.x.254 assigned (x.x.x.0 and x.x.x.255 are reserved), you might use x.x.x.1, x.x.x.2, x.x.x.3, and so on, to assign static addresses to your network interface cards, and reserve x.x.x.245, x.x.x.246, x.x.x.247, and so on, for devices that are DHCP clients.
- If you are connecting to an Internet Service Provider (ISP) through a modem, but not otherwise routing to a WAN, and do not have a reserved, registered address pool of Internet Protocol (IP) addresses through an Internet license, use the IP address assigned by your ISP for the modem network interface.

  For your other network interfaces, use the standardized, unregistered, non-connecting IP addresses set aside in RFC 1918, "Address Allocation for Private Internets." RFC 1918 is published by the Internet Engineering Task Force (IETF); the IETF web address is http://www.ietf.org.

  RFC 1918 includes the following addresses:

  - 10.0.0.0 to 10.255.255.255
  - 172.16.0.0 to 172.31.255.255
  - 192.168.0.0 to 192.168.255.255
- If you do not have a connection to an ISP or a WAN, use the standardized, unregistered, non-connecting IP addresses set aside in RFC 1918 for your network interfaces. (In this situation, you *must* change the default IP address for the Integrated Services Card, and you can use Wave default IP addresses for your other network interfaces.)
- Do not assign IP addresses ending in .0 or .255 to individual machines, as these are the network and broadcast addresses for Class C addresses.

Each Integrated Services Card and 10/100Base-T Ethernet hub card in the Wave ISM is an Ethernet segment with a network interface to RRAS. Each network interface requires a valid static IP address and subnet mask number.

The Wave ISM is configured with a Integrated Services Card as an independent Ethernet segment on Wave ISMs that have only a Integrated Services Card installed. That card is configured with a default *static* IP address of 192.168.205.1 and a default Subnet Mask of 255.255.255.0.

Note: If you have 10/100Base-T Ethernet hub cards installed in the Wave ISM, only one Ethernet segment is created.

Note: You should have changed the default IP addresses of your Wave network interfaces during initial configuration. For details, see "Identifying your Wave ISM on the LAN" on page 3-2. You can continue to use the default IP addresses only if packets destined for the Internet first go through a separate machine—not part of Wave—which performs IP address translation, such as a proxy server or a Network Address Translator (NAT). For more information on using a proxy server in an Wave network, see "Using a proxy server with Wave" on page 29-10.

In determining what IP addresses to use, follow the guidelines in "Identifying your Wave ISM on the LAN" on page 3-2.

The following are additional guidelines for working with IP addresses and subnet masks:

- Router interface IP addresses typically end in .1. For example, if subnet 1 is 192.168.3.*, its network interface IP address would be 192.168.3.1; if subnet 2 is 192.168.4.*, its network interface IP address would be 192.168.4.1, and so on.
- Use the next logical number that is not currently assigned to assign new IP addresses.
- If your Wave ISM is connected to an external DHCP server, modify the Wave default IP addresses to use an IP address within the server's subnet range. For example, if the DHCP server address is 204.1.1.1, you might change the Integrated Services Card address from 192.168.1.245 to 204.1.1.245, and set the Wave IP address range from 204.1.1.2 to 204.1.1.244. You must set this address, because the Wave ISM cannot be a DHCP client.
- You can assign multiple IP addresses to any router port/network interface, as long as there are not two machines with the same address on the same network.

- In general, a host route subnet mask is 255.255.255.255 and is used for referring to a single machine; a default static route subnet mask is 0.0.0.0; and a subnet mask is in between the host and the default, typically with an address of 255.255.255.0.
- The default gateway address, which answers the question “Who do I contact when a machine is not on my subnet?,” is that of the closest router on the subnet. If the network interface address is x.x.3.1, the default gateway address is x.x.3.1. Ask your network administrator for the appropriate address.

Using a proxy server with Wave

Proxy servers convert private IP addresses to public IP addresses for sending packets over the Internet. If your network uses private IP addresses (such as the default Wave IP addresses), you can use a proxy server or a network address translator (NAT) to perform IP address translation.

- If your network has an existing proxy server, connect one network interface of the Wave ISM into the subnet containing the proxy.
- If you have no existing proxy server, create a subnet on which you put all your internet services—such as proxy server, mail server, and Web server—with official IP addresses. Set up a separate subnet for all machines using unofficial IP addresses as proxy clients.

Routing protocols

Routing protocols implement dynamic routing, modifying paths as needed, taking advantage of more efficient routes, and avoiding broken networks. Routing protocols are used by routers to communicate current routing information to other routers and to workstations using these routers. They allow an end-to-end path for packets to be chosen, while only requiring each router to know the path to the next router. The routing cost of a path is measured by a metric, and the least expensive path is always chosen.

As multiple routers or Ethernet subnets are added to a network, dynamic routing allows more efficient routing and error recovery. For example, if there are two Wave ISMs, only the first one needs to have an active dial-up connection to the ISP. The second Wave ISM can forward any ISP-bound packets to the first, instead of using its

one connection to dial the same ISP. Additionally, if the WAN card in the first Wave ISM failed, it could route all ISP-bound packets to the second Wave ISM.

Routing Information Protocol (RIP)

Routing Information Protocol, or RIP, is used to discover all the subnets on a network dynamically, communicate when a subnet goes down, and rediscover the subnet when it comes back up. Routers configured for RIP send announcements frequently to update routing tables. The RIP protocol can run on top of either IP or IPX. If you configure IPX, RIP is automatically configured for you.

Note: RIP version 1 is not aware of network masks (subnets), and instead uses class A, B, and C addresses to determine routing. If you are using RIP version 1, be sure to make all IP addresses parallel in size.

RIP uses the shortest number of hops to send a packet from point A to B, but does not take the speed of connection lines—digital versus modem versus ISDN, for example—into account when it is routing. Use RIP if you want Wave router interfaces to share routing information with other routers in your network, but not if you have enabled redundant paths on a very large network. In the latter case, OSPF is a better choice.

Open Shortest Path First (OSPF) routing protocol

The Open Shortest Path First (OSPF) dynamic routing protocol takes bandwidth into account when forwarding packets. OSPF will automatically choose a digital line over an ISDN line, for example. OSPF will route overloaded packets on the shortest path, and will use a second digital line when one is available, although you still have to calculate the metrics OSPF should use.

Use OSPF if the Wave ISM is part of a large, hierarchical network with redundant paths or backbone routers.

Internet Packet Exchange (IPX)

When you are running Novell NetWare services on your Wave network, you will need to configure Internet Packet Exchange (IPX) on Wave. IPX is Novell NetWare's native LAN communication protocol. All Microsoft Windows and NetWare interoperability services rely on IPX to communicate with NetWare servers.

IPX supports a simple address scheme that allows clients to communicate with servers residing in other logical networks, and lets routers determine what traffic needs to flow between different links. IPX does not dictate that each client and server have assigned addresses, other than the physical network adapter address. (In contrast, TCP/IP requires every client and network to have a unique assigned address, with both a network component and a system address.)

Microsoft Windows Server 2003 accommodates TCP/IP and IPX, individually or concurrently. What you configure depends on your particular network configuration.

Routing protocol metrics

All IP addresses, subnet masks, and metrics are stored in a routing table so that packets of information can be directed quickly to their destinations. If a client on a subnet sends a packet to another on the same subnet—x.x.3.3 to x.x.3.8, for example—the packet goes directly to its recipient. If a client on one subnet sends a packet to a client on a different subnet—x.x.3.3 to x.x.4.9, for example—the packet is sent through a router, and is routed along the shortest path from one point to another, based on routing protocol metrics.

Routing protocol metrics measure the cost of sending a packet between a source and a destination. By setting routing protocol metrics, you can define pathways and alternate pathways for routing packets.

Hint: The IP Routing Table in the RRAS administrator reports non-local metrics as one greater than they really are.

The RIP metric, for example, is measured in hop counts (the number of nodes, composed of routers and other devices).

If both a modem and a digital line connect to the ISP, configure RIP metrics so that the digital line will be used for all routing to the ISP. You can control the metric by defining a default static route and setting a shorter metric for the digital (1) than for the modem (2).

The OSPF metrics take bandwidth and load sharing (distributing bandwidth across equal paths) into account, making them both more advanced and more complex to configure than RIP metrics.

Note: Backup routing requires special configuration, since RRAS cannot detect link failures. The digital link must have RIP or OSPF configured, and the modem link must have a default or static route configured.

Static routes

In a small (single subnet) network environment, particularly with only one point of entry to the Internet, you can use static routing instead of configuring RIP or OSPF. In static routing, the routes do not change once you set them. However, this also means that if any network failures occur, there are no other paths available in the network to route around the failure.

The Wave ISM uses RRAS, a software router, as a LAN-to-LAN, LAN-to-WAN, and WAN-to-WAN router for IP traffic. RRAS IP routing is installed and enabled by default, so LAN routing configuration is, for the most part, automatic. Depending on your particular Wave configuration, you may need to configure routing protocols and / or LAN-to-WAN interfaces.

Routing protocols for static routes

The Wave ISM supports two protocols for dynamic routing: RIP and OSPF. Without RIP or OSPF enabled, IP only forwards packets between static routes on subnets. In addition, the Wave ISM supports IPX for routing between Novell NetWare servers.

For information about configuring RIP, see “Configuring routing information protocol (RIP)” on page 22-3.

Packet filtering

Packet filtering is a way of restricting network traffic on an interface to just those packets that match a given pattern. This is typically done to provide a level of security against untrusted networks (such as the Internet) or to conserve bandwidth on WAN interfaces.

Since the patterns are fairly simple, packet filtering does not afford the same level of security or configuration as a network firewall or proxy. However, it is sufficient for many environments, and can also be used in addition to more sophisticated methods. Packet filters in Wave only support the Internet Protocol (IP) and those that utilize IP, such as TCP, UDP, and ICMP.

The following sections describe packet filters and how to use them in different environments. In many cases, multiple environments might apply. For example, Wave can support one or more interfaces with filters for a private network, a DMZ network, the Internet, and port filters. Figure 29-1 shows an illustrative network, where Wave is connected to the Internet over a WAN, the private network consists of 192.168.1.0 and 192.168.2.0, and the DMZ is 222.222.222.0.

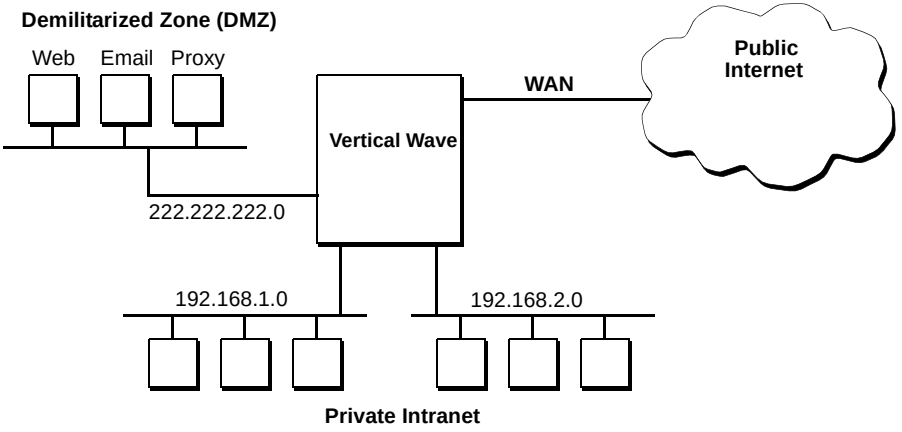


Figure 29-1 Example network with public, private, and DMZ areas

DMZ networks

A DMZ (De-Militarized Zone) network is where publicly-accessible servers are typically located, such as Web servers and email servers. More importantly, in an environment with a private network (see “Private networks”), only machines in the DMZ communicate directly with the Internet.

To enforce this security, properly constructed packet filters will:

- Allow the DMZ to communicate with the Internet
- Reject any direct communication between the private network and the Internet
- Optionally restrict communication between the DMZ and the Internet to particular services
- Optionally restrict communication between the DMZ and the private network to particular services

This section discusses the first two goals, which are enough for most environments. The latter two goals are covered in “Protocol and port filtering of common services” on page 29-17, and should be used in environments where security is an important issue.

To allow communication between the DMZ and the Internet, only two cases should be allowed:

- Packets sent by a DMZ address going out to the public Internet
- Packets sent to a DMZ address coming in from the public Internet

The following filters can be put into place on the WAN connection(s) with the filters set to “drop all except listed below.” The IP addresses in Table 29-1 are for the network in Figure 29-1; substitute the addresses for your own DMZ.

Table 29-1 DMZ network filters (drop all except listed below)

Direction	Filter Type	IP network address	Subnet mask
Input	Destination network	222.222.222.0	255.255.255.0
Output	Source network	222.222.222.0	255.255.255.0

Private networks

A private network (often referred to as an intranet) often uses RFC 1918-allocated, unregistered IP addresses—sometimes known as private networks—which are used by a large number of networks worldwide, with the understanding that they will never transmit those addresses on any public network. If a company wishes to then connect to the public Internet, a network proxy or Network Address Translator (NAT) is used to convert between the two sets of IP addresses. This is done both for security and to avoid obtaining public, registered IP addresses to simplify administration of the company's network. In an environment such as this, care should be taken to avoid communication between the two networks.

In a simple environment, routing information is not passed between the ISP and the private network. Therefore, the private network must have a default route (0.0.0.0 / 0.0.0.0) directed at the ISP. A side effect is that any traffic that is not terminated internally (such as traffic destined for a subnet that had just gone down) would be routed to the ISP.

Generally, the public Internet will not be able to handle the private IP addresses, and they will eventually be discarded by one of the ISP's routers. This alone ensures that there is no normal communication between the two networks.

However, there are a few reasons to place a firewall between the two networks:

- Increased security; while it is an extreme case, a hacker who has direct access to your ISP could get around the discarding of your private addresses
- Lessen the traffic across the WAN connection to the ISP
- Courtesy to your ISP in not giving them additional unnecessary traffic

Normally, however, the private intranet will use the services of a network proxy or NAT which is located in the DMZ network, and will never communicate with the untrusted Internet directly. Therefore, the DMZ packet filters will accommodate all of the above goals, and only those filters are needed.

To create a firewall between the public and private networks, four cases must be prevented from passing across the WAN. The latter two cases may seem redundant, but should be put in place to provide maximum security.

- Packets sent by a private network address going out to the public Internet
- Packets sent to a private network address going out to the public Internet
- Packets sent by a private network address coming in from the public Internet
- Packets sent to a private network address coming in from the public Internet

These filters can be put in place by either Wave or the ISP. If this firewall is a serious concern for your company, then the filters should be enabled on Wave; if you wish to lessen administration, let the ISP enable the filters.

The following filters can be put into place on the WAN connection(s), with the filters set to receive / transmit all except listed below. Each of these filters should be added as both input and output filters, thereby creating a total of 12 filters. You can use all of them, or just the subset matching your private addresses. These filters are listed with the IP network address and then the subnet mask.

Table 29-2 Outbound and inbound filters

Direction	Filter Type	IP Network Address	Subnet Mask
Input/Output	Source	10.0.0.0	255.0.0.0
Input/Output	Source	172.16.0.0	255.240.0.0
Input/Output	Source	192.168.0.0	255.255.0.0
Input/Output	Destination	10.0.0.0	255.0.0.0
Input/Output	Destination	172.16.0.0	255.240.0.0
Input/Output	Destination	192.168.0.0	255.255.0.0

Protocol and port filtering of common services

The most specific type of filtering is known as protocol filtering or port filtering. This allows only specific protocols on an interface. For example, you may wish to disallow FTP over your connection to the Internet. These types of filters can be complex to set up and maintain.

Wave packet filters can only perform simple filters on the protocols, since they are not dynamic nor do they track the state of the connection. A more sophisticated firewall or network proxy is needed for complex environments and protocols.

A common practice is to limit access to the Internet to only a few different services and ports. This is fairly straightforward if there are no Internet servers (such as web or email) located on-site. To do this, you would set up a "dump all except listed below" filter which allows only specific protocols and ports.

Typically, this list includes the TCP and UDP services listed in Table 29-3. This is a subset of what is referred to as **well-known port numbers**, which is documented in various places, such as STD 0002 (also known as RFC 1700). While most services' ports are valid for both TCP and UDP, in practice you will probably only see one or the other.

Table 29-3 Common ports for TCP and UDP

Service	Port	Full Name
DNS	53	Domain Name Services
FTP	20, 21	File Transfer Protocol
Gopher	70	Gopher
HTTP	80	World Wide Web HyperText Transfer Protocol
IMAP4	143	Interim Mail Access Protocol, Version 4
NNTP	119	Network News Transfer Protocol
POP3	110	Post Office Protocol, Version 3
PPTP	1723	Point-to-Point Tunneling Protocol*
Remote Desktop	3389	Remote Desktop
SMTP	25	Simple Mail Transfer Protocol
Telnet	23	Telnet

* See "PPTP filtering" on page 29-19 for additional information.

The list of desired services could also include the ICMP protocol, which allows ping and TRACERT to work. For simplicity, you can specify just the ICMP protocol and leave the type and code fields blank, which will allow all ICMP through. However, you could only allow ICMP type 8 (echo request) to be output and both ICMP type 0 (echo reply) and type 11 (time exceeded) to be input; this would allow you to ping the Internet, but no one on the Internet could ping you. A list of ICMP message types is supplied in Table 29-4.

Table 29-4 ICMP message types

Type	Description
0	Echo reply
3	Destination unavailable
4	Source quench
5	Redirect

Table 29-4 ICMP message types

Type	Description
8	Echo request
9	Router advertisement
10	Router solicitation
11	Time exceeded
12	Parameter problem
13	Time stamp request
14	Time stamp reply
15	Information request
16	Information reply
17	Address mask request
18	Address mask reply

As an example, you could create an environment where only web browsing was permitted, by filtering out all protocols except for DNS and HTTP. To do this, the following filters can be put into place on the WAN connection to the Internet, with the filters set to drop all except listed below.

Table 29-5 Protocol filters for Web browsing (drop all except listed below)

Direction	Filter Type	Protocol	Direction	Port
Input	Protocol	UDP	Source port	53
Input	Protocol	TCP	Source port	80
Output	Protocol	UDP	Destination port	53
Output	Protocol	TCP	Destination port	80

PPTP filtering

In some environments, a network may only be used for tunneling, but not for actual traffic. For example, a branch office may use PPTP to tunnel through the Internet to

headquarters, but may not use it for anything else. More commonly, the interface has protocol filters in place, and you can allow PPTP traffic, allowing home users to tunnel into the company's network.

Caution: *On the Advanced TCP/IP Protocol properties windows of the Microsoft Windows Network control applet, there is an Enable PPTP Filtering option. Do not select this option.*

There are three cases in which Wave allows for PPTP:

- Packets with TCP source port 1723
- Packets with TCP destination port 1723
- Packets using IP protocol number 47, which is the Generic Routing Encapsulation (GRE) protocol

A total of six additional filters must be in place (listed in Table 29-6) and the "drop all except listed below" option must be selected, for PPTP filters.

Table 29-6 Protocol filters for PPTP (drop all except listed below)

Direction	Filter Type	Protocol	Field	Value
Input	Protocol	TCP	Source port	1723
Input	Protocol	TCP	Destination port	1723
Input	Protocol	Other	Protocol	47
Output	Protocol	TCP	Source port	1723
Output	Protocol	TCP	Destination port	1723
Output	Protocol	Other	Protocol	47

Network services

Wave uses the following Windows services for network information services:

- Dynamic Host Configuration Protocol (DHCP)
- Domain Name Service (DNS)
- Windows Internet Name Service (WINS)

By default, Wave does not use DHCP and can be easily configured to be a client of WINS and DNS.

Wave as DNS client

The Internet and most private networks rely on DNS to provide name resolution service to all clients and servers. Since Wave has to know how to resolve outside Internet addresses, it needs the DNS service or a proxy server. Configure Wave as a DNS client when another server in your network performs DNS services.

Wave as WINS client

Configure Wave as a WINS client when you want the WINS server to resolve client-computer requests for names mapped to IP addresses for file, print, and application traffic.

DHCP relays

If your Wave ISM is connected to an external DHCP server, and you wish to use the DHCP server for the subnets connected to the Wave ISM, you must configure Wave as a DHCP relay.

The DHCP relay agent is a component of RRAS. The Relay Agent allows Wave to forward requests for IP address assignment, using DHCP, from a routed subnet on one Ethernet hub card to a separate DHCP server on another subnet.

Configure DHCP relays if your clients and the DHCP server are on a different routed subnet or network.

You do not need to configure the DHCP relay agent if you have a large network with DHCP servers on each subnet. DHCP Relay will not work if DHCP Server is running on the same system.

Part 4

Reference

Vertical Wave Reports

CHAPTER CONTENTS

The Call Detail Report

This section provides information about the Call Detail Report and how to use and manage the information. Refer to the following sections for detailed information:

- "About the Call Detail Report" on page 30-1, describes rules, formats and field descriptions for the Call Detail Report and the IP Telephony Voice Extension Record.
- "Configuring the Call Detail Report" on page 30-11, provides information about using the Call Detail Report.

About the Call Detail Report

The Call Detail Report (CDR) provides a daily summary log file of all Wave incoming and outgoing calls. It can be used for validating a newly installed telephone system, and for call accounting. Used in conjunction with a front-end call accounting package or a Microsoft Excel spreadsheet designed to provide the breakdowns you need, you can sort and chart records of customer traffic by extension, duration, time of use, and so on, for departmental or customer billing.

You will typically configure the Call Detail Report once, to set the outgoing short call duration, the number of daily summary log files to save, and the type of call detail records to capture.

By default, the CDR logs one day of calls in each file—approximately 650 KB, if an office makes an average of 2,000 calls per day. You set the number of files you want to save, and when Wave reaches that limit, the oldest files are deleted first. You can increase the number of files saved using the Call Detail Report applet. Use the following information to determine how many files to save:

- Each 1 MB stores approximately 2,600 call records.
- The default number of files stored is 60, or approximately 38 MB based on an average of 2,000 calls per day; the maximum number of files is 180, or approximately 114 MB, based on an average of 2,000 calls per day.

This section provides the following information about the call detail report:

- "Call Detail record and field rules" on page 30-2
- "Call Detail record formats" on page 30-3
- "CDR field descriptions" on page 30-3
- "IP telephony voice extension record" on page 30-9

Call Detail record and field rules

Wave CDR logs calls according to the following rules for records and fields:

- A record is logged when a call terminates.
- A single record is logged for a conference call.
- When an extension tries to make an outbound call and all trunks are busy, the call action column logs a B for all trunks busy.
- When multiple parties are involved in a call, such as a transfer, the calling party is the person initiating the call, the called party is the first person who answers the call, and the final party is the last person who answers the call. The Primary Call Record ID column provides a log of each call, tying these calls together. Call duration is the total time from the first person answering the call to the last person hanging up the call, including time spent on hold.
- In conference calls, the person who creates the conference is logged in the call ID column. One of the last two parties to leave the call is logged as the final party.
- Incoming calls begin when the attendant, Voice Mail, or the first extension answers a call.

- If outbound calls are shorter than the Outgoing Short Call Duration configured in the Call Detail Report applet, they are defined as unanswered, and are not recorded, unless the central office provides answer supervision. The default time is 45 seconds.

Note: Outgoing calls over analog loop start trunks do not provide answer supervision, which means that Wave cannot tell whether a call is answered when it is placed over a loop start trunk. The Outgoing Short Call Duration setting lets you establish a time after which such calls will be assumed to be connected, and will be recorded in the CDR.

Call Detail record formats

Wave CDR fields use the following formats:

- Records are delimited with carriage return
- Records are ASCII-based
- Fields are right-justified
- Fields are padded with blanks; the Duration and End TM fields are padded with zeros
- Fields are comma-separated

CDR field descriptions

Each CDR log begins with a header. The header fields are described in Table 30-1. Table 30-2 describes the Call Detail Record Log and Table 30-3 describes the IP Telephony Voice Extension Record.

Table 30-1 Call Detail Header Description

Field Name (example)	Description
<HEADER>	Indicates the beginning of the log header.
File ID (Cdr)	Identifies the type of file.
Version (4)	Specifies the revision of the file format.
Serial Number (123456)	The Vertical Wave serial number entered into the General Settings applet.

Table 30-1 Call Detail Header Description

Field Name (example)	Description
Hostname (IO3000)	The name of the Wave ISM.
IP Address (192.168.6.150)	The IP address of the Wave ISM.
Start Date (20010430)	The date the file was created.
Start Time (0:00:00)	The time the file was created.
<\HEADER>	Indicates the end of the log header.

Wave CDR field descriptions are enumerated in Table 30-2 and Table 30-3.

Table 30-2 Call Detail Record Log Description

Column (Excel*)	Field Name	Field Length†	CDR Head	Description
1 (A)	Call Record ID	8	Entry	An incrementing number that uniquely identifies each CDR record, or text that identifies restart-related, non-CDR records, which are identified with an asterisk (*). Clearing a CDR log does not reset incrementing record numbers. Non-CDR records such as the CDR header and restart information (start and stop times) will have a non-numerical value in this field. Restart-related, non-CDR records include: • Entry – Vertical Communications header; always the first entry in the file (no asterisk). • Cleared – Date and time that CDR record was cleared; always the second entry in the table. • Stop – Date and time Wave stopped. • Restart – Date and time Wave is able to process phone calls. • CM Stop – Date and time Wave stopped processing phone calls because the Connection Manager stopped.
2 (B)	Site ID	6	Site	System identification number, such as **VN0001**, the default. You can change the site ID; see "Configuring the Call Detail Report" on page 30-11.
3 (C)	Call Duration	8	Duration	The duration of the call in the format **ddhhmmss**. When multiple parties are involved, call duration is the total time from the moment the first person answers the call until the connection ends (one of the last two connected parties hangs up). Microsoft Excel strips leading zeros, so if the call was one minute, two seconds long, you would see **102**; if the call was two hours, one minute, two seconds long, you would see **20102**. Only if a call was more than 24 hours long would you see something like **1094451** (a duration of 1 day, 9 hours, 44 minutes, 51 seconds). If a call duration exceeds 100 days the field will contain **99235959**.

Table 30-2 Call Detail Record Log Description

Column (Excel*)	Field Name	Field Length†	CDR Head	Description
4 (D)	End Date	8	End date	The date the call ended in the format **yyyymmdd**, such as **20001130** for November 30, 2000. In a restart-related record, end date indicates system clear, stop, or restart date.
5 (E)	End Time	6	End TM	The time the call ended in the 24-hour format **hhmmss**, such as **140102** for 2:01:02 P.M. In a restart-related record, end time indicates system clear, stop, or restart time
6 (F)	Call Type	1	T	A single character that defines the type of call. Current types: Inbound=>; Internal=I; Outbound=<; Data=D.
7 (G)	Call Action	1	A	A single character that defines the action the call took. Actions, in highest to lowest precedence, with multiple action calls logging only the highest precedence action, include: C=Conference; O=Off-site forward; F=Forward; X=Transfer; B=All trunks busy; D=Direct trunk.
8 (H)	Access Code Dialed	4	TACD	Reserved. Not used in this release.
9 (I)	Access Code Used	4	TACU	Reserved. Not used in this release.
10 (J)	Call ID	8	Call ID	The extension number defined as the owner of this call. In conference calls, the Call ID is the person who creates the conference. Having a single location for this field makes database searching easier.
11 (K)	Calling Number	20	Calling Party	The number of the call source, either an internal extension or an external number.
12 (L)	1st Destination Number	25	Called Party	The first destination of the call, either an internal extension or an external number.
13 (M)	Final Destination Number	25	Final Party	The final destination of the call. If the call forwards multiple times, the final destination is where the call eventually connects. In conference calls, the final destination number is one of the last two parties to leave the call.
14 (N)	Account Code	16	Reserved	Reserved. Not used in this release.
15 (O)	Authorization Code	12	Authorize	Up to 12 digits of the user's dialed authorization code.

Table 30-2 Call Detail Record Log Description

Column (Excel*)	Field Name	Field Length†	CDR Head	Description
16 (P)	Incoming Trunk Group Number	8	In TKGP	The pilot number of the trunk group which received the incoming call.
17 (Q)	Incoming Circuit	8	In TRK	The number associated with the trunk used to accept an incoming call.
18 (R)	Outgoing Trunk Group Number	8	Out TKGP	The pilot number of the trunk group used to place the outgoing call.
19 (S)	Outgoing Circuit	8	Out TRK	The number associated with the trunk used to place an outgoing call.
20 (T)	Additional Call Record	2	AC	An 'x' in this field indicates that an additional call record related to this call record exists. The additional call record will indicate that this record is the primary record. Not used in Releases 1.0 through 4.x.
21 (U)	Incoming Trunk Group Access Code	4	TACI	Reserved. Not used in this release.
22 (V)	Tax	8	Tax	The number of meter pulses associated with this call, indicating the cost of the call. Also called “Advice of Charge.” Used only for international installations.
23 (W)	Currency	10	Currency	Currency used to determine the multiplier for this call. Used only for international installations. Default values for supported countries are: USD=United States MARK=Germany LIRA=Italy YEN=Japan CDN=Canada

Table 30-2 Call Detail Record Log Description

Column (Excel*)	Field Name	Field Length†	CDR Head	Description
24 (X)	Multiplier	4	Mult	Multiplier. The tax amount is multiplied by this value to determine the charge in the state currency. Used only for international installations. Possible values include: .001=x1 / 1000 .01=x1 / 100 .1=x1 / 10 1=x1 10=x10 100=x100 1000=x1000
25 (Y)	TGU	5	TGU	Time Granularity Units. Unit of time used to charge the call. Used only for international installations. Possible values include: .001s=.001 second .01s=.01 second .1s=.1 second 1s=1 second 10s=10 seconds 1m=1 minute 1h=1 hour
26 (Z)	Primary Call Record ID	8	Primary	A call record linked to this call record, caused by transferring or parking the call.
27 (AA)	Extension Record Descriptor	1	E	Identifies how the remaining record will be interpreted. Valid values are: 0=No Extension Record; 1=IP Telephony Audio Extension Record; 2=IP Telephony T.38 Fax Extension Record; 3=IP Telephony Video Extension Record. Refer to IP Telephony Voice Extension Record for information about the IP Telephony CDR Extension.

* In a Microsoft Excel spreadsheet, columns are indicated by letters.
† Field length indicates number of characters used. Microsoft Excel does not display leading zeros by default.

IP telephony voice extension record

The Extension Record Descriptor (ERD) determines how the extension record portion of the CDR should be interpreted. The only valid values for the IP Telephony Extension Record ERD are 0 and 1, which indicate that the extension record should be ignored (0) or analyzed as an IP telephony voice extension record (1). The comma separated value file has fixed length records. If ERD is 0, then applications should skip over the commas and blanks that compose the remainder of the CDR record.

This extension record contains two symmetrical sections for the origination and the termination sides of the call. Note that the ORIGINATION section corresponds to the DSP codec closest to the Calling Party and that the TERMINATION section corresponds to the DSP codec closest to the Called Party.

Table 30-3 describes the fields in the ORIGINATION and TERMINATION sections of the IP Telephony Voice Extension Record.

Table 30-3 IP Telephony Extension Record Descriptor

Column (Excel*) Orig/Term	Field Name	Length	Record Heading Orig/Term	Description
28 (AB) / 42 (AP)	Media Endpoint IP Address	15	OIP / TIP	IP address of the device terminating the RTP stream. If it is an IP telephone, this is the IP address of the IP telephone. If it is a TDM endpoint (e.g., an analog telephone), this is the IP address of the interface being used on the Wave ISM. IP address is in `aaa.bbb.ccc.ddd` format (leading zeros are omitted).
29 (AC) / 43 (AQ)	Media	2	OM / TM	Specifies the media: 1 = Audio 2 = Fax (future) 3 = Video (future) 4 = Modem Termination (future) 5 = Fax Termination (future)

Table 30-3 IP Telephony Extension Record Descriptor

Column (Excel*) Orig/Term	Field Name	Length	Record Heading Orig/Term	Description
30 (AD) / 44 (AR)	Codec	2	OC / TC	Specifies the codec used on the receiving direction from the endpoint perspective. If Media = 0 (Audio): 0 = G.711 u-law PCM 64kbps 1 = G.711 A-law PCM 64kpbs 2 = G.729A 3 = G.723.1 5.3kbps 4 = G.723.1 6.3kbps If Media = 1 (Fax): 0 = Telogy Fax 1 = T.38 Fax
31 (AE) / 45 (AS)	Packet Time	3	OPT / TPT	Amount of voice information contained per packet (in milliseconds).
32 (AF) / 46 (AT)	Bandwidth—Average	4	OBWA / TBWA	Average bandwidth (in Kbps) used for the call, from the perspective of the receiving direction.
33 (AG) / 47 (AU)	Bandwidth—Peak	4	OBWP / TBWP	Peak bandwidth (in Kbps) used for the call, from the perspective of the receiving direction.
34 (AH) / 48 (AV)	Latency—Average	4	OLA / TLA	The average round trip delay during the call, in milliseconds, calculated per PFC 1889.
35 (AI) / 49 (AW)	Latency—Peak	4	OLP / TLP	The peak round trip delay during the call, in milliseconds, calculated per PFC 1889.
36 (AJ) / 50 (AX)	Jitter—Average	4	OJA / TJA	The average jitter during the call, in milliseconds, calculated per RFC 1889.
37 (AK) / 51 (AY)	Jitter—Peak	4	OJP / TJP	The peak jitter during the call, in milliseconds, calculated per RFC 1889.
38 (AL) / 52 (AZ)	Packets Received	10	OPKTRX / TPKTRX	Count of the total packets received.
39 (AM) / 53 (BA)	Octets Received	10	OOCTRX / TOCTRX	Count of the total octets received.

Table 30-3 IP Telephony Extension Record Descriptor

Column (Excel*) Orig/Term	Field Name	Length	Record Heading Orig/Term	Description
40 (AN) / 54 (BB)	Packets Lost—Total	10	OPKTLT / TPKTLT	Total number of packets lost during the call.
41 (AO) / 55 (BC)	Packets Lost—Peak	10	OPKTLP / TPKTLP	Maximum number of packets lost in any sample period during the call.

* In a Microsoft Excel spreadsheet, columns are indicated by letters.

About the Call Detail Report

Call Detail record formats

CDR field descriptions

Call Detail record and field rules

Configuring the Call Detail Report

The following procedure describes how to configure the Call Detail Report.

To configure the Call Detail Report:

Click

1 Open the Call Detail applet.

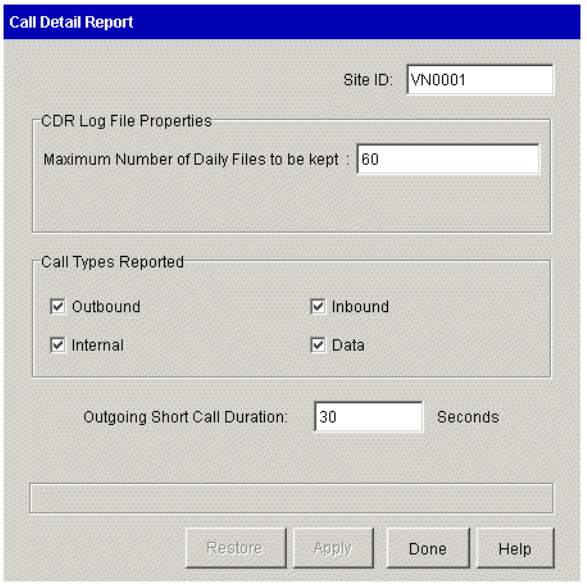


Figure 30-1 Call Detail Report applet

2 Enter a Site ID.

Entering a name or number in the Site ID field is only necessary if you have multiple systems and want to distinguish call detail reports between systems. Up to six alphanumeric characters are allowed.

3 Type the maximum number of daily report files you want stored in the Maximum Number of Files field.

The number of files is limited by the size of hard-disk storage. When Wave reaches the limit you set, the oldest files are deleted first.

Note: You might want to set the Maximum Number of Files field based on your billing cycle. For example, you are probably billed monthly, and if you take billing lag time into consideration, you might set Wave to save 60 files. You can then correlate your bill with the CDR log.

4 Check the types of calls you want reported in the Call Types Reported group box.

5 If you want to change the 45 second Outgoing Short Call Duration (default), type a different number in the Seconds field.

This number is used by Wave to determine when to record outbound calls over trunks that do not provide answer supervision (such as analog loop start trunks). Such calls are not recorded if they are shorter than the Outgoing Short Call Duration set.

Setting a minimum duration distinguishes busy/ring no answer calls from completed calls in the CDR. The default is 45 seconds. The possible range is 0 to 60 seconds. If you use a lower setting, such as 30, Wave will record all outbound calls, on trunks without answer supervision, that last 30 seconds or more.

6 Click Apply to save your changes.

7 Click Done to return to the Management Console.

Note: Changes to calls types and duration settings, as well as log file property settings, are applied when you click Apply or Done; site ID is applied after you restart the Wave ISM.

Note: You can download the CDR, if you wish. See "Downloading reports" on page 30-25 for instructions.

The Report Generator

The Report Generator enables you to generate reports from the most recently configured Wave data. You can generate the following reports:

- Authorization Codes
- Digital Phone Labels
- First Digit Table
- Hunt Group
- Network Settings
- Outbound Routing
- Station Port
- System Distribution Lists
- System Speed Dial

- Templates
- Trunk Group
- Trunk statistics
- User Configuration
- User Details
- Voice Mail
- Zone Paging
- Zone Bandwidth Statistics

To generate and view a report:

Click

1 Open the Report Generator applet.

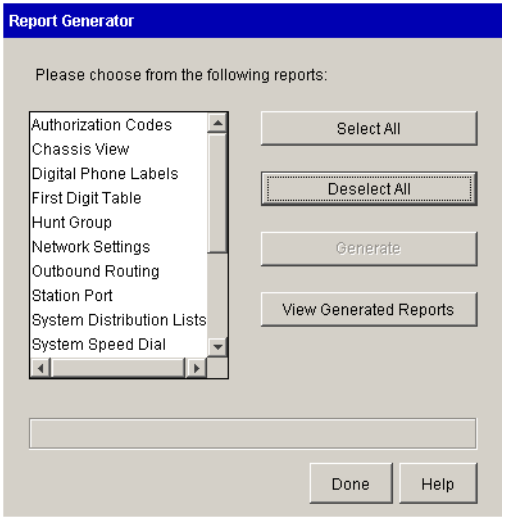


Figure 30-2 Report Generator applet

2 Select the desired report(s) from the list, and click Generate.

To select multiple reports, hold the Ctrl key while selecting.

3 Click View Generated Reports.

If an error occurs while Wave generates a report, an error.txt file is created.

4 Click a report to view its contents.

The previously generated Trunk Statistics report, if there is one, is overwritten.

Generated reports reside on the Wave ISM. To copy a report to a client PC, select File>Save As while viewing the report, then select your client PC from the Save In options.

After a report is generated, you can access it through its URL, skipping the Report Generator applet.

5 Click the Back button on your browser to return to the list of reports.

6 Close the browser window containing the list of reports to return to the Report Generator applet.

7 Click Done to return to the Management Console.

Trunk statistics

This section provides information about the Trunk Statistics Report and how to use and manage the information. Refer to the following sections for detailed information:

- “Generating the Trunk Statistics Report” on page 30-16, provides information about using the Trunk Statistics Report.
- “About the Trunk Statistics Report” on page 30-17, describes rules, formats and field descriptions for the Trunk Statistics Report.
- “About the Trunk Statistics log” on page 30-19, describes rules, formats and field descriptions for the Trunk Statistics Log, the raw data from which the report is generated.

Generating the Trunk Statistics Report

To generate the Trunk Statistics Report:

Click 

1 Open the Report Generator applet.

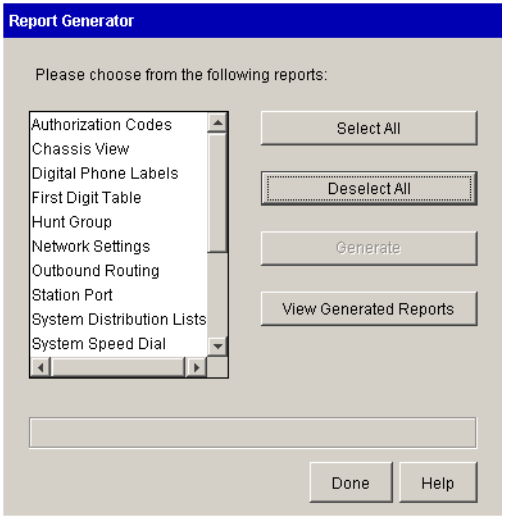


Figure 30-3 Report Generator applet

2 Select Trunk Statistics from the list of reports, and click Generate to open the Trunk Statistics Report Criteria dialog box.

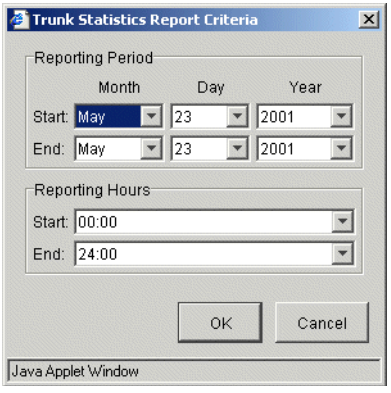


Figure 30-4 Trunk Statistics Report Criteria dialog

3 Select the starting and ending dates of the period for which you'd like the report, as well as the time range within those dates, and click OK.

For example, you might select dates from May 1, 2001 through May 15, 2001 and times from 08:00 to 12:00. The generated report will contain records on May 1 from 08:00 to 12:00, May 2 from 08:00 to 12:00, etc.

The generated report is saved and named TrunkStatistics.html.

Caution: *The previously generated Trunk Statistics report, if there is one, is overwritten.*

4 Click View the Generated Reports for a directory listing of all generated reports for Wave.

5 Click TrunkStatistics.html to view the report you generated.

6 Click Done to return to the Management Console.

About the Trunk Statistics Report

The Trunk Statistics Report provides a generated listing of call statistics for all trunk groups in Wave. This report is generated from information gathered by Wave and saved in the Trunk Statistics Log (see "About the Trunk Statistics log" on page 30-19 for more information).

Note: If you change the configuration—either the name of a trunk group and / or the number of channels assigned to a trunk group—during the reporting period, you might get unexpected results. For example, if you change the name of the trunk group or the number of channels assigned to the trunk group, you will see two records. If you change the name, you will see one record under each name. If you change the number of channels, you'll see two records with the same name but with different data.

The columns in the generated report are enumerated and described in the following table.

Table 30-4 Trunk Statistics Report columns

Column Name	Description
Trunk Group	The trunk group name.
Size	The total number of analog trunks and digital trunk channels in the group.

Table 30-4 Trunk Statistics Report columns

Column Name	Description
Direction	The direction (In, Out, or Both) currently configured (at the time the report is generated) for the trunk group with the given name. **Note:** If the trunk group direction has changed, only the most recently configured direction will appear in the report. If the trunk group name has changed or the trunk group has been deleted, "Unknown" will appear in the report.
Busy Hour	The hour (0000, 0100, …, 2300) during which the total usage (inbound and outbound) is greatest. For example, the report would show 1300 as the peak hour if the total use (inbound and outbound) for 13:00, 13:15, 13:30, and 13:45 on all days during the reporting period was greater than the total use for any other hour. If the trunk group was never used, it will report blank for the busy hour.
Calls In	The total number of inbound attempts for this trunk group during the reporting period.
Calls Out	The total number of outbound attempts for this trunk group during the reporting period.
Total Calls	The sum of the computed Calls In and Calls Out values, described above.
Usage In (mins)	The total inbound use in minutes, rounded up to the nearest minute.
Usage Out (mins)	The total outbound use in minutes, rounded up to the nearest minute.
Total Usage (mins)	The sum of the computed Usage In and Usage Out values, described above
% ATB	The percentage of time during which all channels in this trunk group were busy.
% Out Blk	The percentage of outbound calls that were blocked.
Out Svc	The total number of trunks / channels associated with this trunk group that have ever gone out of service during the reporting period.

About the Trunk Statistics log

Wave gathers trunk and trunk group statistics that are written to the Trunk Statistics Log file every 15 minutes on the hour, quarter hour, half hour, and three-quarter hour. The log file contains the raw data from which the Trunk Statistics Report is generated. The log is saved in C:\Program Files\InstantOffice\logs\Reports\.

Each Trunk Statistics log begins with a header. The header fields are described in Table 30-5. Subsequent tables describe the main fields of the Trunk Statistics Log.

Table 30-5 Trunk Statistics Header Description

Field Name (example)	Description
<HEADER>	Indicates the beginning of the log header.
File ID (TrunkStatistics)	Identifies the type of file.
Version (4)	Specifies the revision of the file format.
Serial Number (123456)	The Wave Integrated Services Manager (ISM) serial number entered into the General Settings applet.
Hostname (IO3000)	The name of the Wave ISM.
IP Address (192.168.6.150)	The IP address of the Wave ISM.
Start Date (20010430)	The date the file was created.
Start Time (0:00:00)	The time the file was created.
<\HEADER>	Indicates the end of the log header.

The Trunk Statistics Log field descriptions for each type of record in the report are enumerated in the tables in the following sections.

Interval record

Each interval posted begins with an interval record.

Table 30-6 Interval record fields

Field Name	Description
I	Identifies this record as an interval record
YYYYMMDD or MMDDYYYY	The date of the start of the interval in either North American or European format
HH:MM	The start time of the interval

Trunk group header record

Each trunk group record is preceded by a trunk group header.

Table 30-7 Trunk Group Header record fields

Field Name	Description
hG	Identifies this record as an trunk group header record
Trunks In Group	The number of trunks in the group at the end of the interval
Group Name	The name of the trunk group
OOS	The number of trunks in a trunk group that were OOS (Out of Service) at any time in the interval
Inbound Begin	The number of trunks with incoming calls in progress at the beginning of the interval
Inbound End	The number of trunks with incoming calls in progress at the end of the interval
Inbound Attempts	The number of incoming calls attempted by this trunk group
Inbound Answered	The number of incoming calls by this trunk group that were answered
Inbound Seconds	The total number of seconds that trunks in a trunk group were in the connected state for an incoming, answered call
Outbound Begin	The number of trunks with outgoing calls in progress at the beginning of the interval
Outbound End	The number of trunks with outgoing calls in progress at the end of the interval

Table 30-7 Trunk Group Header record fields

Field Name	Description
Outbound Attempts	The number of outgoing calls attempted by this trunk group
Outbound Answered	The number of outgoing calls by this trunk group that were answered
Outbound Seconds	The total number of seconds that trunks in a trunk group were in the connected state for an outgoing, answered call
Outbound Blocked	The number of outgoing calls that were blocked due to All Trunks Busy (ATB) and / or Out of Service (OOS) Trunks and / or Integrated Services Access (ISA)
ATB Seconds	(All Trunks Busy) The total number of seconds that all trunks in the trunk group are busy and / or out of service

Trunk group record

Each trunk group record follows the trunk group header record.

Table 30-8 Trunk Group record fields

Field Name	Description
G	Identifies this record as an trunk group record
Trunks In Group	The number of trunks in the group at the end of the interval
Group Name	The name of the trunk group
OOS	The number of trunks in a trunk group that were OOS (Out of Service) at any time in the interval
Inbound Begin	The number of trunks with incoming calls in progress at the beginning of the interval
Inbound End	The number of trunks with incoming calls in progress at the end of the interval
Inbound Attempts	The number of incoming calls attempted by this trunk group
Inbound Answered	The number of incoming calls by this trunk group that were answered

Table 30-8 Trunk Group record fields

Field Name	Description
Inbound Seconds	The total number of seconds that trunks in a trunk group were in the connected state for an incoming answered call
Outbound Begin	The number of trunks with outgoing calls in progress at the beginning of the interval
Outbound End	The number of trunks with outgoing calls in progress at the end of the interval
Outbound Attempts	The number of outgoing calls attempted by this trunk group
Outbound Answered	The number of outgoing calls by this trunk group that were answered
Outbound Seconds	The total number of seconds that trunks in a trunk group were in the connected state for an outgoing answered call
Outbound Blocked	The number of outgoing calls that were blocked due to All Trunks Busy (ATB) and / or Out of Service (OOS) Trunks and / or Integrated Services Access (ISA)
ATB Seconds	The total number of seconds that all trunks in the trunk group were busy and / or out of service

Trunk header record

Each trunk header record follows the trunk group record. There is one trunk header record per trunk group.

Table 30-9 Trunk Header record fields

Field Name	Description
hT	Identifies this record as a trunk header record
Trunks Name	The name of the trunk

Trunk record

Each trunk record follows the trunk header record. There is one trunk record for each trunk in the group.

Table 30-10 Trunk record fields

Field Name	Description
T	Identifies this record as an trunk header record
Trunks Name	The name of the trunk
Group Name	The name of the trunk group
OOS	Indicates whether the trunk was OOS (Out of Service) at any time during the interval; the value is either 1(TRUE) or 0(FALSE)
Inbound Begin	Indicates whether the trunk had an incoming call in progress at the beginning of the interval
Inbound End	Indicates whether the trunk had an incoming call in progress at the end of the interval
Inbound Attempts	The number of incoming calls attempted by this trunk
Inbound Answered	The number of incoming calls by this trunk that were answered
Inbound Seconds	The total number of seconds that the trunk was in the connected state for an incoming answered call
Outbound Begin	Indicates whether the trunk had an outgoing call in progress at the beginning of the interval
Outbound End	Indicates whether the trunk had an outgoing call in progress at the end of the interval
Outbound Attempts	The number of outgoing calls attempted by this trunk
Outbound Answered	The number of outgoing calls by this trunk that were answered
Outbound Seconds	The total number of seconds that a trunk was in the connected state for an outgoing answered call

Digital telephone labels

Using Wave and DESI's label-creation software, called DESI, you can create professional, printed telephone labels for the digital telephones connected to Wave. To create labels, complete the following sub-tasks:

1 Generate the Digital Phone Labels Data File (see “Generating the digital telephone labels data file” on page 30-24).

2 Import the generated data file into DESI’s label-creation software.

Note: For information about DESI’s label creation software, contact your Vertical Communications reseller.

Generating the digital telephone labels data file

To generate the labels data file for a digital telephone:

Click

1 Open the Report Generator applet.

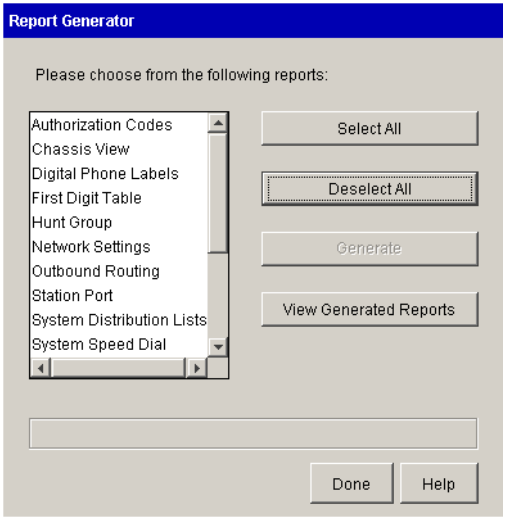


Figure 30-5 Report Generator applet

2 Select Digital Phone Labels from the list of reports, and click Generate.

You will see a message when the report generation is complete.

3 Click View the Generated Reports for a directory listing of all generated reports for Wave.

4 Click DigitalPhoneLabels.txt to view the data file you generated.

5 Click Done to return to the Management Console.

Downloading reports

To download reports:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the Download icon, located in the General Administration section.

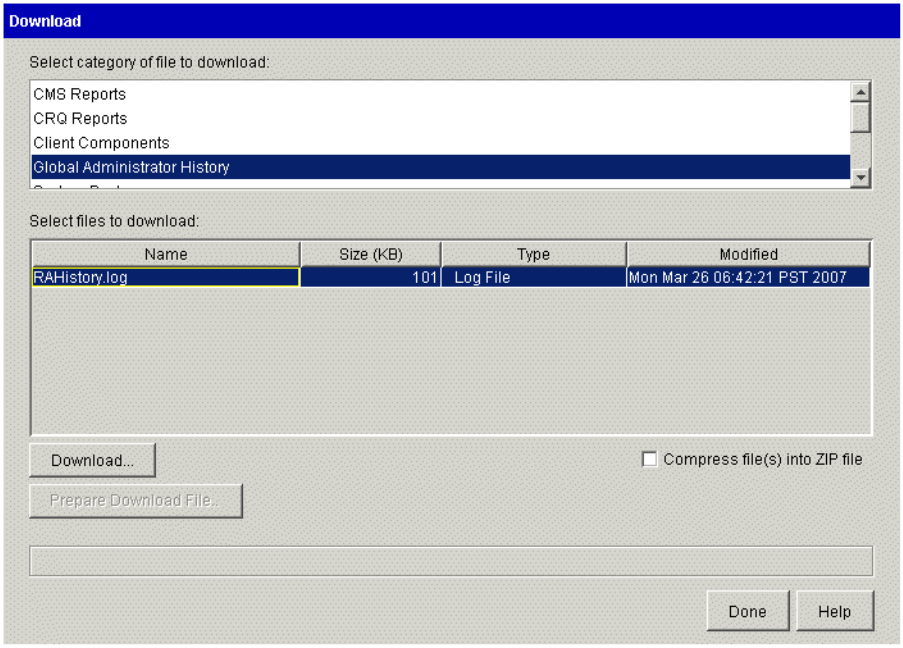


Figure 30-6 Download applet

3 Select the type of file you want to download.

You will see a list of files available to download.

To download a CDR file, select Vertical Wave Reports.

4 Select the file(s) you want to download, and click Compress file(s) into ZIP file, if you want the file compressed.

Hint: You can select contiguous files by holding the Shift key, and you can select non-contiguous files by holding the Ctrl key.

5 Click Download, and save the file.

6 Click Done to return to the Management Console.

SNMP Agents

CHAPTER CONTENTS

About SNMP agents

Simple Network Management Protocol (SNMP) can be used to monitor and diagnose the Wave ISM, notifying you about any unsolicited events, which are also known as traps. The events detected by SNMP agents are based upon telephony and network standards, such as the IEEE 802.3 Ethernet standard. All MIBs reside on the Wave ISM in the following directory: C:\Program Files\SNMP\MIBs.

SNMP agent and alarm configuration

Wave provides two panels for configuring and monitoring SNMP: the SNMP Configuration and SNMP Alarms panels. The SNMP Configuration applet lets you configure trap destinations from Wave agents, and permits the following functions:

- Define valid (up to seven) community strings
- Identify destination managers who will receive traps (notification about any unsolicited events)

The SNMP Alarms applet lets you monitor current and review previous alarms. For further information about using the SNMP Alarms and SNMP Configuration applets, see “Configuring and using SNMP” on page 24-15.

Vertical Communications SNMP agents

This Wave software release supports the following SNMP agents:

- Environment
- Event Log
- Interfaces
- IP Telephony
- ISDN
- Repeater Private
- Station Private
- Self Test Daemon (STD)
- IOSystem
- T-1 Private

Each of these agents is described in detail in the sections starting on page 3.

Environment

The Environment agent is responsible for reporting status information about the cooling fans, power supplies, and the fault monitor. This agent also generates appropriate traps to notify Wave of changes in fan status, power supply status, and the status of the fault monitor.

The Environment MIB is structured into the following groups:

Table 31-1 Environment MIB groups

Group	Description	Tables contained
The Fan Table	Describes status information about all the Wave ISM cooling fans.	The Fan Table
The Power Supply Table	Describes status information about all the Wave ISM power supply units.	The Power Supply Table
The Fault Monitor Group	Contains information about the fault monitor status.	None.
The Trap Info Group	Contains information about the last fan, power supply, and fault monitor traps.	None.
Traps	Generates traps when the status of the fans, power supplies, or fault monitor changes	None.

The Fan Table

The Fan Table defines objects that describe the status information about each cooling fan in the Wave ISM. Table 31-2 describes each of these objects.

Table 31-2 Environment SNMP agent, Fan Table

MIB Variable	Access	Definition	Syntax	Value
fanIndex	R	The numeric index of the cooling fan within the Wave ISM.	Integer	
fanOperStatus	R	Specifies the current operational status of the cooling fan. Valid values are: • running: the normal operational status • stopped: the fan is stopped • unknown: the agent is unable to get the status for this fan	Integer	running=1 stopped=2 unknown=3

The Power Supply Table

This table defines objects that describe the status information about each power supply unit in the Wave ISM. Table 31-3 describes each of these objects.

Table 31-3 Environment SNMP agent, Power Supply Table

MIB Variable	Access	Definition	Syntax	Value
psIndex	R	The numeric index of the power supply unit.	Integer	
psOperStatus	R	Specifies the current operational status of the power supply unit. Valid values are: • on: the normal operational status • off • unknown: the agent is unable to get the status for the power supply unit	Integer	on=1 off=2 unknown=3

The Fault Monitor Group

This group contains information about the fault monitor status. This group contains just one object, as described in Table 31-4.

Table 31-4 Environment agent, Fault Monitor Group

MIB Variable	Access	Definition	Syntax	Value
ioFaultMonitorStatus	R	Describes the operational status of the Fault Monitor. Valid values are: • NotResponding—the fault monitor is not responding • ModemFailed—the fault monitor modem has failed • Ok—the normal operational state	Integer	RAMFull=1 NotResponding=2 OK=3 ModemFailed=4

The Trap Info Group

This group contains information about the last fan, power supply, and fault monitor traps. Table 31-5 describes the objects in this group.

Table 31-5 Environment SNMP agent, Trap Info group

MIB Variable	Access	Definition	Syntax	Value
ioLastFanTrap	R	This object describes, in more detail, the last fan trap event that occurred. Since traps for all fans are combined into one trap, this string describes each fan status just after the trap condition.	String	

Table 31-5 Environment SNMP agent, Trap Info group

MIB Variable	Access	Definition	Syntax	Value
ioLastPowerSupplyTrap	R	This object describes, in more detail, the last power supply trap event that occurred. Since traps for all power supplies are combined into one trap, this string describes each power supply status just after the trap condition.	String	
ioLastFaultMonitorTrap	R	This object describes, in more detail, the last fault monitor trap event that occurred. Since traps for all fault monitor events are combined into one trap, this string describes each event (RAMFull, NotResponding, or ModemFailed) that caused this trap.	String	

Traps

This agent generates appropriate traps when the status of one or more fans, or the status of one or more power supplies or the status of the fault monitor system change. Table 31-6 describes the traps in detail.

Table 31-6 Environment SNMP agent, Traps

Trap #	Trap Name	Description	Pertinent MIB Data
47	ioFanStatus	This notification is sent when one (or more) cooling fans changes state (i.e., it goes from a running state to a stopped state or vice versa). Even if more than one fan changes state, only one trap is sent. Information about the new state of all the fans is sent in the trap data (IOLastFanTrap).	ioLastFanTrap
48	ioPowerSupplyStatus	This notification is sent when one (or more) power supply units changes state (i.e., it goes from an ON state to an OFF state, or vice versa). Even if more than one power supply changes state, only one trap is sent. Information about the new state of all the power supplies is sent in the trap data (IOLastPowerSupplyTrap).	ioLastPowerSupplyTrap
49	ioFaultMonitorStatus	This notification is sent when the following Fault Monitor events occur: • RAM full • Fault Monitor Not Responding • Modem Failed Information about these events is contained in the trap data (IOLastFaultMonitorTrap).	ioLastFaultMonitorTrap
83	ioSchedulerInfo	This notification is sent whenever an information (including success notification) pertaining to the IOScheduler operation needs to be sent out. Specific information regrading this trap is contained in the Trap data (ioLastIOSchedulerInfoTrap).	ioLastIOSchedulerInfoTrap
84	ioSchedulerWarning	This notification is sent whenever a warning pertaining to the IOScheduler operation occurs. Specific information regarding this trap is contained in the Trap data (ioLastIOSchedulerWarningTrap).	ioLastIOSchedulerWarningTrap

Table 31-6 Environment SNMP agent, Traps

Trap #	Trap Name	Description	Pertinent MIB Data
85	ioSchedulerError	This notification is sent whenever an error pertaining to the IOScheduler operation occurs. Specific information regrading this trap is contained in the Trap data (ioLastIOSchedulerWarningTrap).	ioLastIOSchedulerErrorTrap
92	ioTrapInfoGroup	This notification is sent when one or more temperature sensors measure a temperature outside the normal operating range. Subsequent traps will be generated for each degree of decrease below or increase above the normal operating range. Information about the current state of all the temperature sensors is sent in the Trap Data (ioLastTemperatureOutsideRangeTrap).	ioLastOutsideRangeTemperatureTrap
93	ioTrapInfoGroup	This notification is sent when one or more temperature sensors return to normal operating temperature range. Information about the current state of all the temperature sensors is sent in the Trap Data (ioLastTemperatureInsideRangeTrap).	ioLastInsideRangeTemperatureTrap
94	ioTrapInfoGroup	This notification is sent when one or more DC power supply sensors measure a voltage outside the normal operating range. The power supplies monitored are +2.5, +3.3, +5, +12, and CPU core. Information about the current state of all the DC power supply sensors is sent in the Trap Data (ioLastDCPowerSupplyOutsideRangeTrap).	ioLastOutsideRangeDCPowerSupplyTrap
95	ioTrapInfoGroup	This notification is sent when one or more DC power supply sensors return to normal operating voltage range. Information about the current state of all the power supplies is sent in the Trap Data (ioLastDCPowerSupplyInsideRangeTrap).	ioLastInsideRangeDCPowerSupplyTrap

Event Log

The Event Log agent is responsible for generating traps when specific Microsoft Windows events are logged. These events can be either application specific, system, or

security related. Each of the generated traps contains data specific to the event logged similar to that shown in the event viewer.

The Event Log MIB contains one group, described in Table 31-7.

Table 31-7 Event Log MIB group

Group	Description	Tables Contained
Event Log Trap Info Group	Contains more information about the last event log trap that was generated.	None.

Event Log Trap Info Group

Table 31-8 Event Log SNMP agent, Trap Info Group

MIB Variable	Access	Definition	Syntax	Value
lastTrapLogType	R	This object describes the log type of the last event log trap event that occurred. The following are valid values: • **system**—Windows system log • **security**—Windows security log • **application**—the Application log • **unknown**—the Unknown log	Integer	system=1 security=2 application=3 unknown=4
lastTrapEvent Type	R	This object describes the event type of the last event log trap that occurred. The following are valid values: • **error**—error events indicate significant problems that the user should know about. Error events usually indicate a loss of functionality or data. For example, if a service cannot be loaded as the Wave ISM boots, it can log an error event • **warning**—warning events indicate problems that are not immediately significant, but that may indicate conditions that could cause future problems. For example, an application can log warning events if disk space is low. • **information**—information events indicate infrequent but significant successful operations. • **audit-success**—success audit events are security events that occur when an audited access attempt is successful. For example, a successful log on attempt is a success audit event. • **audit-fail**—failure audit events are security events that occur when an audited access attempt fails. For example, a failed attempt to open a file is a failure audit event. • **unknown**—indicates an event type other than those described above.	Integer	error=1 warning=2 information=3 audit-success=4 audit-fail=5 unknown=6
lastTrapInfoString	R	This object describes, in more detail, the last event log trap even that occurred. This string contains details of the event like the event id, computer name, time generated, and event specific messages similar to the one seen with the event view application.	String	

Event Log Traps

This agent generates the traps, described in Table 31-9, when the appropriate events are logged.

Table 31-9 Log Event agent, Traps

	Trap Name	Description	Pertinent MIB Data
53	eventLog_FailedToStartSTD	This notification is sent when an attempt to start the Self Start Daemon fails. This event has a Log Type of “application” and an Event Type of “error”.	lastTrapLogType lastTrapEventType lastTrapInfoString
54	eventLog_FailedToStopSTD	This notification is sent when an attempt to stop the Self Start Daemon fails. This event has a Log Type of “application” and an Event Type of “error”.	lastTrapLogType lastTrapEventType lastTrapInfoString
55	eventLog_CannotCreate UserTracePipe	This notification is sent when an attempt to create the User Trace request pipe fails.	lastTrapLogType lastTrapEventType lastTrapInfoString
56	eventLog_CannotConnect UserTracePipe	This notification is sent when an attempt to connect to the User Trace Pipe fails. This event has a Log Type of “application” and an Event Type of “error”.	lastTrapLogType lastTrapEventType lastTrapInfoString
57	eventLog_VoiceMailDiskFull	This notification is sent when the allotted Voice mail disk capacity is reached. This event has a Log Type of “application” and an Event Type of “error”.	lastTrapLogType lastTrapEventType lastTrapInfoString
58	eventLog_SystemDiskIsFull	This notification is sent when the specific disk capacity is reached. This event has a Log Type of “system” and an Event Type of “warning”.	lastTrapLogType lastTrapEventType lastTrapInfoString

Table 31-9 Log Event agent, Traps

	Trap Name	Description	Pertinent MIB Data
59	eventLog_SecurityError	This notification is sent when an audited access attempt fails. This event has a Log Type of “security” and an Event Type of “audit-fail”.	lastTrapLogType lastTrapEventType lastTrapInfoString
60	eventLog_SecuritySuccess	This notification is sent when an audited access attempt is successful. This event has a Log Type of “security” and an Event Type of “audit-fail”.	lastTrapLogType lastTrapEventType lastTrapInfoString
61	eventLog_GenericEventLog Trap	This notification is sent whenever an error or warning event, other than the ones described above, is written to the Event Log. More information about this event can be found in the trap data.	lastTrapLogType lastTrapEventType lastTrapInfoString

Interfaces

The Interfaces agent describes some of the devices installed in the Wave ISM and reports their operational status. This agent implements Vertical's private interfaces MIB (interfaces_private.mib), which is based on the Interfaces Table of MIB II.

The devices reported by this agent are:

- T-1 interfaces
- Analog station ports and trunks
- 10/100 Ethernet ports
- DDS ports
- Repeater Ethernet ports
- Serial interface on T-1 module (reported as Other Interface)

The Interfaces MIB contains one group, described in Table 31-10.

Interfaces Group

Table 31-10 Interfaces MIB group

Group	Description	Tables contained
Interfaces Group	This group is a place holder for the Interfaces Table, which describes each Wave interface (device) in more detail and also shows its operational status. In addition, this group contains one variable, ifNumber, which basically specifies the number of interfaces displayed in the interfaces group.	The Interfaces Table

IP Telephony

Table 31-11 Interfaces Table

MIB Variable	Access	Definition	Syntax	Value
vifNumber	R	The number of Wave devices (regardless of their current state) present on this system. Size of the integer is 1-'7fffffff'h	Integer	
vifIndex	R	A unique index identifying this interface (device).	Integer	
vifDescr	R	This object describes the interface in more detail. It also specifies the slot number occupied by the interface. Size of the string is 0-255 characters.	String	
vifType	R	This object describes the type of this interface. The type of interface is distinguished according to the physical/link protocol(s) immediately below the network layer in the protocol stack. The values for these types are taken from the similar table in MIB II. Only the following apply to Wave: • **ds1**—T-1 interface • **other**—all other interfaces	Integer	other=1 ds1=18

Table 31-11 Interfaces Table

MIB Variable	Access	Definition	Syntax	Value
vifOperStatus	R	This object describes the current operational status of the interface. The following are valid values: • **up**—normal operation state • **down**—the device is not functional • **testing**—in a test mode	Integer	up=1 down=2 testing=3
vifSpecific	R	This object refers to the Object Identifier branch of the MIB tree that describes this particular interface in more detail. For example, for T-1 interfaces, ifSpecific should specify Vertical's T-1 MIB branch, i.e., 1.3.6.1.4.1.2338.3	OID	

The IP Telephony agent is used to monitor IP Telephony trunks.

IP Telephony Trunk Summary Table

Table 31-12 IP Telephony Trunk Summary Table

MIB Variable	Access	Definition	Syntax	Value
IpTelTrunkSize	R	Number of trunks.	Integer	
TrunkIndex	R	Trunk number in the trunk table.	Integer	
TrunkState	R	The state of the trunk.	Integer	not-configured=0 out_of_service=1 Initializing=2 Idle=3 Outgoing=4 Incoming=5 Connected=6 Disconnecting=7
CalledParty	R	Number of the called party.	String	
CallingParty	R	Number of the calling party.	String	

Table 31-12 IP Telephony Trunk Summary Table

MIB Variable	Access	Definition	Syntax	Value
RemoteGateway	R	Remote gateway number.	String	
LocalAlarmThreshold	R	Current levels of thresholds reached. It is a bit field indicating the following thresholds: BitDescription 0Jitter 1NetworkLost 2Network To Host Errors 3Host To Network Errors 4DSP To Host Errors 5Host To DSP Errors	Integer	
RemoteAlarmThreshold	R	Current levels of thresholds reached. For a description of the bit fields see LocalAlarmThreshold.		

Traps

Table 31-13 IP Telephony agent, Traps

Trap #	Trap Name	Description	Pertinent MIB Data
64	IpTelReconfigComplete	This notification is sent when the reconfiguration command completes.	IptelTrunkSize
65	IpTelTrunkFailure	This notification is issued when the specified trunk fails	TrunkIndex
66	IpTelTrunkAlarmInfo	Informational alarm associated with some parameter threshold being reached.	TrunkIndex LocalAlarmThreshold RemoteAlarmThreshold

ISDN

The ISDN agent is used to manage Vertical Communication's ISDN interfaces, including information for managing the Bearer B channels and signaling channels. The ISDN agent is based on Vertical's private ISDN MIB (isdn_private.mib), using the definitions of SNMP v2 ISDN MIB (RFC 2127) with the syntax changed to reflect SNMP

v1. The relative tree structure in this MIB has been retained. In order to manage ISDN interfaces, the following information is necessary:

- Information for managing the physical interface (the T-1 line)

  This information is already provided by the T-1 standard (RFC 1406) and the T-1 private MIB; the respective agents for these MIBs implement the management functionality.

- Information for managing the Bearer B channels

  This information is implemented by this agent.

- Information for managing signaling channels

  This information is implemented by this agent.

The following information is optional:

- Information for managing Terminal Endpoints (TE), for example, the link layer connection to the switch

  Since this is required only if there are non-ISDN endpoints defined for a given D channel, Wave does not implement this.

- Information for managing a list of directory numbers for each signaling channel

  This is not currently implemented by the agent.

Each interface in the system has a unique interface index. In a typical Wave ISM, there would be a unique interface index for the following:

- Each T-1 physical interface of the system
- Each B channel of the system
- The Data link layer (LAPD) of each D channel
- The Network layer (Terminal Endpoint, also called the signaling channel) of each D channel

  Each D channel is subdivided into two layers, the data link and the network layer.

- All other interfaces in the system.

How do all these interface fit together? The Interfaces MIB (see “Interfaces” on page 31-12) defines an Interface Table that contains generic descriptive, status, and statistical information about all the interfaces in the system. In a typical management scenario, an alarm received on an interface is reflected by the agent for the interface.

The Manager can look up specific alarm information from the interface's own MIB, note the Interface Index for this interface, and obtain general statistics for this interface (for example, the number of Octets received on this interface, or the bandwidth of this interface) by looking up the Interface Table (corresponding to this index) of the Interfaces MIB.

For the T-1 scenario, the Wave implementation of various layers of interfaces is shown in Figure 31-1.

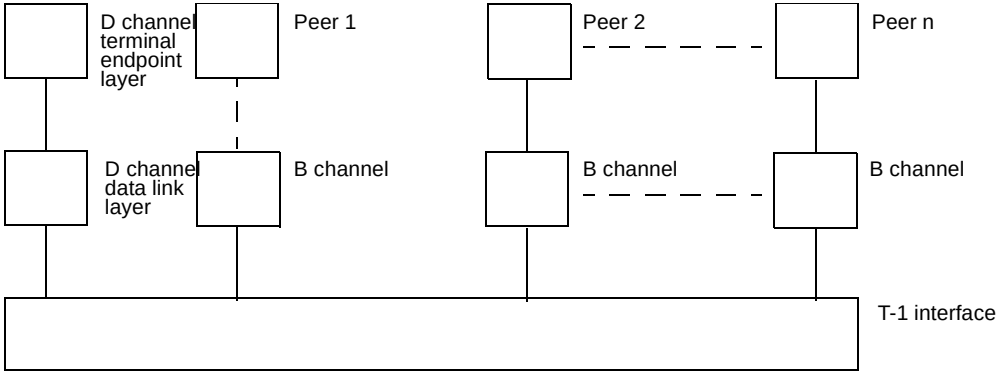


Figure 31-1 Wave T-1 interface layers implementation

Implementation of the ISDN agent is based on Vertical Communication's private ISDN MIB. The private ISDN MIB (isdn_private.mib) uses the definitions of SNMP version 2 ISDN MIB (RFC 2127), with the syntax changed to reflect SNMP version 1. The relative tree structure in this MIB has been retained.

The ISDN private MIB is organized into three groups, as shown in Table 31-14.

Table 31-14 ISDN private MIB groups

Group	Description	Tables contained
The Bearer Group	Used to control B (bearer) channels. Contains configuration parameters as well as statistical information related to B channels.	Bearer Table

Table 31-14 ISDN private MIB groups

Group	Description	Tables contained
The Signaling Group	Used to control D (Delta) channels. Contains information for ISDN Network layer as well as the Data Link Layer (LAPD) configuration and statistics.	Signaling Table Signaling Stats Table Lapd Table
The Directory Group	Used to specify a list of directory numbers for each signaling channel. This group has not been implemented yet.	Not implemented yet

Detailed information about each instrumented variable can be found in the MIB, isdn_private.mib. This agent does not generate any traps.

The Bearer Group

The Bearer Group's sole table, the Bearer Table (Table 31-15), has as many entries as there are bearer channels in the whole system (the total of all bearer channels for all devices in the system). Each entry in the table defines configuration as well as statistical parameters required to control one bearer channel.

Examples for these include the bearer channel type (leased vs. dial-up (visdnBearerChannelType)), the bearer channel operator status (idle, connecting, connected, active (visdnBearerOperStatus)). Each entry in this table is indexed by the unique interface index (ifIndex) of the B channel in the system.

Table 31-15 ISDN agent, Bearer table

MIB Variable	Access	Definition	Syntax	Value
visdnBearerChannelType	R	The B channel type.	Integer	Dialup = 1, Leased = 2
visdnBearerOperStatus	R	The current call state of the channel.	Integer	Idle =1, Connecting =2, Connected =3, Active =4
visdnBearerChannelNumber	R	The B channel number.	Integer	1-30

Table 31-15 ISDN agent, Bearer table **(continued)**

MIB Variable	Access	Definition	Syntax	Value
visdnBearerPeerAddress	R	The ISDN address the current or last call is or was connected to.	String	
visdnBearerPeerSubAddress	R	The ISDN subaddress that the current or last call is or was connected to.	String	
visdnBearerCallOrigin	R	The call origin for the current or last call.	Integer	Unknown=1, Originate=2, Answer=3, Callback=4
visdnBearerInfoType	R	The information transfer capability of the last call. Speech refers to a non-data connection, whereas audio31 and audio7 refers to data mode connections. If there is no call on this interface since system startup, this object has a value of unknown(1).	Integer	Unknown=1, Speech=2, UnrestrictedDigital=3, UnrestrictedDigital56=4, RestrictedDigital=5, Audio31=6, Audio7=7, Video=8, PacketSwitched=9
visdnBearerMultirate	R	This flag indicates if the current or the last call used multirate.	Boolean	True=1, False=2
visdnBearerCallSetupTime	R	The value of the sysUpTime when the ISDN setup message for the current or last call was sent or received.	Time Stamp	
visdnBearerCallConnectTime	R	The value of the sysUpTime when the ISDN connect message for the current or last call was sent or received.	Time Stamp	
visdnBearerCallChargedUnits	R	The number of charged units for the current or last connection.	Gauge	

The Signaling Group

The Signaling Group is used to control D (delta) channels. The Signaling Group consists of three tables:

- The Signaling Table (Table 31-16) contains configuration and operational parameters for the Terminal Endpoint layer interface of each D channel.
- The Signaling Stats Table (Table 31-17) contains statistical information for the same interfaces.
- The LAPD table (Table 31-18) contains configuration and statistical information for each D channel Data Link layer (LAPD) interfaces of the system.

Note: The Directory Group, used to specify a list of directory numbers for each signaling channel, is not currently implemented.

Table 31-16 ISDN agent, Signaling table

MIB Variable	Access	Definition	Syntax	Value
visdnSignalingIfIndex	R	The ifIndex value of the interface associated with this signaling channel.	Integer	1-65535
visdnSignalingProtocol	R	The particular protocol type supported by the switch providing access to the ISDN network to which this signaling channel is connected.	Isdn Signaling Protocol	Other=1, Ds1=2, Swissnet3=25
visdnSignalingCallingAddress	R	The ISDN address to be assigned to this signaling channel.	String	
visdnSignalingSubAddress	R	The ISDN subaddress to be assigned to this signaling channel.	String	
visdnSignalingBchannelCount	R	The total number of B channels managed by this signaling channel.	Integer	1-65535
visdnSignalingInfoTrapEnable	R	Indicates whether isdnMibCallInformation traps should be generated for calls on this signaling channel.	Integer	Enabled=1, Disabled=2

Table 31-17 ISDN agent, Signaling Stats table

MIB Variable	Access	Definition	Syntax	Value
visdnSigStatsInCalls	R	The number of incoming calls on this interface.	Counter	
visdnSigStatsInConnected	R	The number of incoming calls on this interface that were actually connected.	Counter	
visdnSigStatsOutCalls	R	The number of outgoing calls on this interface.	Counter	
visdnSigStatsOutConnected	R	The number of outgoing calls on this interface that were actually connected.	Counter	
visdnSigStatsChargedUnits	R	The number of charged units on this interface since system startup.	Counter	

Table 31-18 ISDN agent, LAPD table

MIB Variable	Access	Definition	Syntax	Value
visdnLapdPrimaryChannel	R	If true, this D channel is the primary D channel if backup D channel is active. Defaults to True.	Boolean	True=1, False=2
visdnLapdOperStatus	R	The operational status of this interface: • **Inactive**: all layers inactive. • **L1Active**: layer1 activated, layer 2 datalink not established. • **L2Active**: layer1 activated, layer 2 datalink established.	Integer	Inactive=1, L1Active=2, L2Active=3
visdnLapdPeerSabme	R	The number of peer SABME frames received on this interface, for example, the number of peer initiated new connections on this interface.	Counter	
visdnLapdRecvdFrom	R	The number of LAPD FRMR response frames received on this interface, for example, the number of framing errors on this interface.	Counter	

Repeater Private

The repeater hub agent monitors and manages all repeater devices within the Wave system. The Wave implementation is based on Vertical Communication's private repeater MIB (repeater_private.mib). The private MIB module combines the syntax of

SNMP version 1 definition for IEEE 802.3 repeaters (RFC 1516) with the additional features defined in the SNMP version 2 (RFC 2108). The structure of the private MIB closely follows that of the definition in RFC 2108, with the relative tree structure of the variables unchanged.

Note: For descriptions of each statistical variable in the repeater hub agent tables, see ASN.1 definitions in the Vertical Communications private repeater MIB (repeater_private.mib).

The repeater private MIB consists of four main groups. Descriptions and the table contained in these groups are identified in Table 31-19.

Table 31-19 Repeater private MIB groups

Group	Description	Tables contained
The Basic Package Group	Describes objects that are applicable to all repeaters within the system: status, parameter, and control objects for each repeater within the managed system, for the port groups within the system, and for the individual ports themselves.	Group Table Port Table Info Table
The Monitor Group	Contains definitions for monitoring statistics for each repeater within the system as well as for individual ports within the system.	Monitor Port Table Monitor 100Port Table Monitor Repeater Table Monitor 100Repeater Table
The Address Tracking Group	Includes objects for tracking the MAC addresses of the DTEs attached to the ports within the system. This is an optional group and has not been implemented.	None
The TopN Group	Includes objects for tracking the ports with the most activity within the system. This is an optional group and has not been implemented at present.	None

The Basic Package Group

The Group Table (Table 31-20) contains status information about each group of ports within the system, such as the Operation Status of the group (operational, malfunctioning, notPresent) (vrptrGroupOperStatus), the port capacity of this group (vrptrGroupPortCapacity).

Table 31-20 Group table, Repeater hub agent

MIB Variable	Access	Definition	Syntax	Value
vrptrGroupIndex	R	Identifies the group within the system for which this entry contains information.	Integer	1-2147483647
vrptrGroupObjectID	R	The vendor's authoritative identification of the group.	OID	
vrptrGroupOperStatus	R	An object that indicates the operational status of the group. A status of notPresent (4) indicates that the group is temporarily or permanently, physically and / or logically, not a part of the repeater. It is an implementation-specific matter as to whether the agent effectively removes notPresent entries from the table.	Integer	other=1, oparational=2, malfunctioning=3, notPresent=4, underTest=5, resetInProgress=6
vrptrGroupPortCapacity	R	The vrptrGroupPortCapacity is the number of ports that can be contained within the group. Within each group, the ports are uniquely numbered in the range from 1 to vrptrGroupPortCapacity.	Integer	1-2147483647
vrptrGroupSlotNumber	R	The slot number in which this repeater device resides.	Integer	1-18
vrptrGroupBroadcast domainNumber	R	This object indicates the repeater's broadcast domain. This value will be 0 if the broadcast domain number is unknown.	Integer	1-18

Table 31-20 Group table, Repeater hub agent **(continued)**

MIB Variable	Access	Definition	Syntax	Value
vrptrGroupNetwork AdapterNumber	R	This object indicates the identification number of the Wave network adapter associated with the repeater, if any. This value will be 0 if the repeated domain number is unassociated or unknown.	Integer	1-255
vrptrGroupLedStatus	R	This object indicates the status of the card LEDs. The Led status is shown for any card that has an Ethernet interface. A status of unknown (1) indicates that the LED status is not available from the hardware. All 10Mb cards will return a value of unknown for its LEDs since the LED information for 10Mb cards are not available. A status of none (2) indicates neither the green nor the red LED is ON. A status of greenRed (5) indicates that both the green and the red LEDs are ON.	Integer	unknown (1) none (2) green (3) red (4) greenRed (5)

The Port Table (Table 31-21) contains status information about each managed repeater port in the system, for each repeater hub in the system. Examples of these are the administrative status of the port (enabled, disabled (vrptrPortAdminStatus)), the operational status of the port (operational, notPresent (vrptrPortOperStatus)).

Table 31-21 Port table, Repeater hub agent

MIB Variable	Access	Definition	Syntax	Value
vrptrPortGroupIndex	R	Identifies the group containing the port for which this entry contains information.	Integer	1-2147483647
vrptrPortIndex	R	Identifies the port within the group for which this entry contains information. This identifies the port independently from the repeater it may be attached to.	Integer	1-2147483647
vrptrPortAdminStatus	R/W	Setting this object to disabled(2) disables the port.	Integer	Enabled=1, Disabled=2

Table 31-21 Port table, Repeater hub agent **(continued)**

MIB Variable	Access	Definition	Syntax	Value
vrptrPortAutoPartitionState	R	This flag indicates whether the port is currently partitioned by the repeater's auto-partition protection.	Integer	notAutoPartitioned=1 autoPartitioned=2
vrptrPortOperStatus	R	This object indicates the port's operational status.	Integer	Operational=1, NotOperational=2, NotPresent=3
vrptrPortRptrId	R	Identifies the repeater to which this port belongs.	Integer	1-2147483647
vrptrPortLinkState	R	Specifies whether there is a link on this port or not.	Integer	link = 1 noLink = 2
vrptrPortSpeed	R	Specifies the Ethernet speed of this particular port.	Integer	unknown (1) 10Mbps (2) 100Mbps (3)
vrptrPortSpeedSelect	R	Indicates the selection used by the port for negotiating the Ethernet speed. If automatic is selected, the highest supported speed will be negotiated.	Integer	speed-select-auto (1) speed-select-10 (2) speed-select-100 (3)
vrptrPortDuplex	R	Indicates the duplex of the Ethernet port	Integer	unknown (1) half (2) full (3)
vrptrPortDuplexSelect	R	Indicates the selection used by the port for negotiating the Ethernet duplex. If automatic is selected, the best supported duplex will be negotiated.	Integer	duplex-select-auto (1) duplex-select-half (2) duplex-select-full (3)
vrptrPortPolarity	R	Indicates the polarity of the Ethernet cable. If the polarity is crossed, the repeater may compensate for it, but it indicates a wiring problem with the attached Ethernet device.	Integer	unknown (1) straight (2) crossed (3)

The Info Table (Table 31-22) contains status information about each repeater hub within the system.

In Wave implementation, a Group is the same as a separate repeater, so the information in the Info Table and the Group Table complement each other. These tables have been kept separate in keeping with the MIB structure in RFC 2108.

Table 31-22 Info table, Repeater hub agent

MIB Variable	Access	Definition	Syntax	Value
vrptrInfoId	R	Identifies the repeater for which this entry contains information.	Integer	1-2147483647
vrptrInfoRptrType	R	Identifies the CSMA / CD repeater type. The value of 5 (tenMbOrOnehundredMb) is a Vertical Communications extension specifying 10 / 100 Mb repeater which contains mixed 10 Mb and 100 Mb ports.	Integer	other=1, tenMb=2, onehundredMbClassI=3, onehundredMbClassII=4 tenMbOrOnehundredMb=5
vrptrInfoOperStatus	R	Indicates the operational state of the repeater.	Integer	Other=1, Ok=2, Failure=3
vrptrInfoReset	R	Setting this object to reset(2) causes a transition to the START state. Setting to noReset(1) has no effect.	Integer	NoReset=1, Reset=2
vrptrInfoPartitionedPorts	R	Returns the number of ports in the repeater that are in the autoPartitioned state.	Integer	0-24
vrptrInfoLastChange	R	The values of syUpTime when any of the following conditions occurred: • Agent cold or warm started • This instance of repeater was created • A change in rptrInfoOperStatus • Ports were added or removed • Any of the counters in this repeater had a discontinuity	Integer	

The Monitor Group

The Monitor Port Table (Table 31-23) contains performance and error statistics for each port in the system.

Table 31-23 Monitor port table, Repeater hub agent

MIB Variable	Access	Definition	Syntax	Value
vrptrMonitorPortGroup Index	R	Identifies the group containing the port for which this entry contains information.	Integer	1-2147483647
vrptrMonitorPortIndex	R	Identifies the port within the group for which this entry contains information.	Integer	1-2147483647
vrptrMonitorPort ReadableFrames	R	The number of frames of valid frame length that have been received on this port.	Integer	
vrptrMonitorPort ReadableOctets	R	The number of octets contained in valid frames that have been received on this port.	Integer	notSupported (-1) supported (0)
vrptrMonitorPortFCS Errors	R	The number of frames with FCS error signal asserted on this port.	Integer	notSupported (-1) supported (0)
vrptrMonitorPort AlignmentErrors	R	The number of frames with FCS and Framing error signals asserted.	Integer	notSupported (-1) supported (0)
vrptrMonitorPortFrame TooLongs	R	The number of frames with OctetCount greater than maxFrameSize.	Integer	notSupported (-1) supported (0)
vrptrMonitorPortShort Events	R	This counter is incremented by one for each CarrierEvent on this port with ActivityDuration less than ShortEventMaxTime.	Integer	
vrptrMonitorPortRunts	R	Usually indicates collision fragments.	Integer	notSupported (-1) supported (0)
vrptrMonitorPort Collisions	R	This counter is incremented by one for any CarrierEvent signal on any port for which the CollisionEvent signal on this port is asserted.	Integer	notSupported (-1) supported (0)
vrptrMonitorPortLate Events	R	This counter is incremented by one for each CarrierEvent on this port in which the CllIn(X) variable transitions to the value SQE.	Integer	
vrptrMonitorPortVery LongEvents	R	This counter is incremented by one for each CarrierEvent on this port whose ActivityDuration is greater than the MAU Jabber Lockup Protection timer TW3.	Integer	

Table 31-23 Monitor port table, Repeater hub agent **(continued)**

MIB Variable	Access	Definition	Syntax	Value
vrptrMonitorPortData RateMismatches	R	Data Rate mismatches as per the definitions in the MIB (repeater_private.mib).	Integer	notSupported (-1) supported (0)
vrptrMonitorPortAuto Partitions	R	This counter is incremented by one each time the repeater has automatically partitioned this port.	Integer	
vrptrMonitorPortTotal Errors	R	The total number of errors which have occurred on this port.	Integer	
vrptrMonitorPortLast Change	R	The value of syUpTime when any of the following conditions occurred: • Agent cold or warm started. • The row for the port was created. • Any of the counters in this repeater had a discontinuity.	Integer	
vrptrMonitorPortSent Frames	R	This object is the number of frames of valid frame length that have been sent on this port. This counter is incremented by one for each frame sent on this port whose OctetCount is greater than or equal to minFrameSize and less than or equal to maxFrameSize.	Integer	
vrptrMonitorPortSent Octets	R	This object is the number of octets contained in valid frames that have been sent on this port. This counter is incremented by one for each frame sent on this port which has been determined to be a readable frame (i.e., including FCS octets but excluding framing bits and dribble bits). For ports receiving traffic at a maximum rate in a 100Mb/s repeater, this counter can roll over in less than six minutes. Since that amount of time could be less than a management station's poll cycle time, in order to avoid a loss of information a management station is advised to also poll the rptrMonitorPortUpper32SentOctets object, or to use the 64-bit counter defined by rptrMonitorPortHCReadableOctets instead of the two 32-bit counters.	Integer	

Table 31-23 Monitor port table, Repeater hub agent **(continued)**

MIB Variable	Access	Definition	Syntax	Value
vrptrMonitorPort DroppedFrames	R	This counter is incremented by one for every time the switch dropped a frame due to a buffer full event.	Integer	
vrptrMonitorPortOther Errors	R	This counter is incremented by one every time the repeater detects an error that is not reported in any other error counter. The frame may or may not be lost due to the error.	Integer	

Monitor 100 Port Table

Table of additional performance and error statistics for 100Mb/s ports, above and beyond those parameters that apply to both 10 and 100 Mbps ports. Entries exist only for ports attached to 100 Mbps repeaters.

Table 31-24 Monitor port table, Repeater hub agent

MIB Variable	Access	Definition	Syntax	Value
vrptrMonitorPort Isolates	R	This counter is incremented by one each time that the repeater port automatically isolates as a consequence of false carrier events.	Counter	
vrptrMonitorPort SymbolErrors	R	This counter is incremented by one each time when valid length packet was received at the port and there was at least one occurrence of an invalid data symbol. This can increment only once per valid carrier event.	Counter	

Table 31-24 Monitor port table, Repeater hub agent **(continued)**

MIB Variable	Access	Definition	Syntax	Value
vrptrMonitorPortUpper 32Octets	R	This object is the number of octets contained in valid frames that have been received on this port, module 2**32. That is, it contains the upper 32 bits of a 53-bit octets counter, of which the lower 32 bits are contained in the rptrMonitorPortReadableOctets object. This two-counter mechanism is provided for those network management protocols that do not support 64-bit counters (e.g., SNMP V1) and are used to manage a repeater type of 100Mb / s.	Counter	
vrptrMonitorPortUpper 32SentOctets	R	This object is the number of octets contained in valid frames that have been sent on this port, modulo 2**32. That is, it contains the upper 32 bits of a 64-bit octets counter, of which the lower 32 bits are contained in the rptrMonitorPortSentOctets object.	Counter	

Monitor Repeater Table

The Monitor Repeater Table (Table 31-25) shows performance and error statistics for 10 MB repeaters within the system.

Table 31-25 Monitor repeater table, Repeater hub agent

MIB Variable	Access	Definition	Syntax	Value
vrptrMonTxCollisions	R	This counter is incremented every time the repeater state machine enters the TRANSMIT COLLISION state from any state other than ONE PORT LEFT.	Integer	notSupported(-1) supported(0)
vrptrMonTotalFrames	R	The number of frames of valid frame length that have been received on this port for which the FCSError and CollisionEvent signals were not asserted.	Counter	
vrptrMonTotalErrors	R	The total number of errors which have occurred on all the ports of this repeater.	Counter	

Table 31-25 Monitor repeater table, Repeater hub agent **(continued)**

MIB Variable	Access	Definition	Syntax	Value
vrptrMonTotalOctets	R	The total number of octets contained in valid frames that have been received on ports in this repeater.	Integer	notSupported(-1) supported(0)
vrptrMon100Table	NA	A table of additional information about each 100 Mb/s repeater, augmenting the entries in the rptrMonTable. Entries exist in this table only for 100 Mb/s repeaters.	Sequence of VRptrMon 100Entry	
vrptrMon100Entry	NA	An entry in the table, containing information about a single 100 Mbps repeater.	VRptrMon 100Entry	
vrptrMonUpper32Total Octets	R	The total number of octets contained in the valid frames that have been received on the ports in this repeater, modulo 2**32. That is, it contains the upper 32 bits of a 64-bit counter, of which the lower 32 bits are contained in the rptrMonTotalOctets object. If an implementation cannot obtain a count of octets as seen by the repeater itself, the 64-bit value may be the summation of the values of the rptrMonitorPortReadableOctets counters combined with the corresponding rptrMonitorPortUpper32Octets counters for all the ports in the repeater.	Counter	
vrptrMonHCTotalOctet s	R	The total number of octets contained in the valid frames that have been received on the ports in this group. If an implementation cannot obtain a count of octets as seen by the repeater itself, this counter may be the summation of the values of the rptrMonitorPortReadableOctets counters for all of the ports in the group.		

Monitor Repeater 100 Table

A table of additional information about each 100 Mb/s repeater, augmenting the entries in the rptrMonTable. Entries exist in this table only for 100 Mb/s repeaters.

Table 31-26 Monitor repeater 100 table, Repeater hub agent

MIB Variable	Access	Definition	Syntax	Value
vrptrMonUpper32Total Octets	R	The total number of octets contained in the valid frames that have been received on the ports in this repeater, modulo 2**32. That is, it contains the upper 32 bits of a 64-bit counter, of which the lower 32 bits are contained in the rptrMonTotalOctets object. If an implementation cannot obtain a count of octets as seen by the repeater itself, the 64-bit value may be the summation of the values of the rptrMonitorPortReadableOctets counters combined with the corresponding rptrMonitorPortUpper32Octets counters for all the ports in the repeater.	Counter	
vrptrMonHCTotalOctets	R	The total number of octets contained in the valid frames that have been received on the ports in this group. If an implementation cannot obtain a count of octets as seen by the repeater itself, this counter may be the summation of the values of the rptrMonitorPortReadableOctets counters for all of the ports in the group.	Counter	

Station Private

The Station agent is used to monitor, configure and control all station devices within the Wave system. Additionally, this agent can be used to configure the First Digit Table (which contains settings for each digit that is dialed as the first digit), as well as to configure an interface with an external Voice Mail system.

This MIB is structured into four groups:

- **The Common Group**—Contains status and configuration information that are common to all Station devices within the system.
- **The Station Card Group**—Contains status, control, and configuration information about all cards containing station devices within the system. This information is arranged into three tables: the Card Table, the Device Table, and the Channel Table.

- **The Digit Table Group**—Contains configuration information of digits that can be dialed. Currently this group contains just one table, the First Digit Table, which contains settings for each digit (0-9) dialed as the first digit.
- **The External Voice Mail System Group**—Contains configuration information used to interface with an external Voice Mail system. Currently there is one subgroup: the ATT_System_25 subgroup.

The Common Group

Table 31-27 Common Group table, Station agent

MIB Variable	Access	Definition	Syntax	Value
vStationFirstDigitTimeout	R	Specifies the maximum number of seconds to wait for the first digit.	Integer	
vStationDigitTimeout	R	Specifies the maximum number of seconds to wait between digits.	Integer	
vStationOffHookTimeout	R	Specifies the maximum number of seconds to wait for the user to hang up after a call disconnects or the user executes an invalid operation. Howler tone is applied at time-out.	Integer	
vStationNumStationCards	R	Specifies the number of station cards installed in the system.	Integer	
vStationExternalDialDigit	R	Identifies the starting digit for making an external call.	String	SIZE (0-1)

The Station Card Group

The Station Card Group consists of The Card Table, The Device Table, and The Channel Table.

The Card Table

Table 31-28 Station Card Group, Card table, Station agent

MIB Variable	Access	Definition	Syntax	Value
vStationCardSlotNumber	R	Physical slot in the system in which the card is installed.	Integer	1-14
vStationCardType	R	The Vertical Communications card type.	Integer	0=card-type-NOT-CONFIGURED 2=card-type-24-CHANNEL-STATION 3=card-type-BRIDGE1
vStationCardIOPort Address	R	The ISA bus base address for the card.	Integer	0-'7fffffff'h
vStationCardState	R	The current status of the card.	Integer	0=diabled 1=enabled 255=removed
vStationCardErrorLED	R	All Vertical Communications cards have an Error LED and a Ready LED. The combined value of these LEDs are as follows: Error Ready Value Definition off off (0 0) invalid on off (1 0) powering up on on (1 1) initializing off on (0 1) normal	Integer	0-1
vStationCardReadyLED	R	See vStationCardErrorLED.	Integer	0-1

The Device Table

Table 31-29 Station Card Group, Device table, Station agent

MIB Variable	Access	Definition	Syntax	Value
vStationDeviceSlot Number	R	Physical slot in the system in which the card containing the device is installed.	Integer	0-255
vStationDeviceDevice Number	R	The logical device number for this station device in its card.	Integer	0-255

Table 31-29 Station Card Group, Device table, Station agent **(continued)**

MIB Variable	Access	Definition	Syntax	Value
vStationDeviceIfIndex	R	The Interface index for this device. The value for this object correlates to the IfIndex found in MIB-II	Integer	1-'7fffffff'h
vStationDeviceBaseIO Address	R	The ISA bus base address for this card.	Integer	0-'7fffffff'h
vStationDeviceEnabled	R	Setting this variable to Disabled will disable this particular station device.	Integer	0=disabled 1=enabled
vStationDeviceInterrupt	R	Interrupt Request level for this card.	Integer	1-2147483647
vStationDeviceNum Channels	R	The ISA bus address for this card.	Integer	1-'7fffffff'h
vStationDeviceMVIP StartingChannel	R	Vertical Communications card revision level.	Integer	0-255
vStationDeviceMVIP Stream	R	Vertical Communications card identification number.	Integer	0-255
vStationDeviceType	R	Specifies the type of device: 0=undefined 8=station	Integer	0=devUndef 8=devSation
vStationDeviceChange Pending	R	Interrupt Request level for this card / trunk.		0-'7fffffff'h

The Channel Table

Table 31-30 Station Card Group, Channel table, Station agent

MIB Variable	Access	Definition	Syntax	Value
vStationChannelIndex	R	This is the logical channel number of the channel within its station device. For 12 channel station devices, it is between 1 and 12. For 24 channel station devices, it is between 1 and 24.	Integer	1-24
vStationChannelSlot Number	R	The logical number of the slot in which the card containing the channel is located.	Integer	0-255

Table 31-30 Station Card Group, Channel table, Station agent **(continued)**

MIB Variable	Access	Definition	Syntax	Value
vStationChannelDevice Number	R	The logical device number of the device containing this channel within its slot, that is, vstationDeviceDeviceNumber.	Integer	0-255
vStationChannelChannel Type	R	The Channel Type.	Integer	1=loopStart 2=groundStart
vStationChannelMWI Type	R	Defines the type of message waiting indicator.	Integer	0=notConfigured 1=stuuter 2=lamp
vStationChannel OperationMode	R	Defines the operation mode of the channel.	Integer	0=notConfigured 1=station 2=voiceMail 3=notConfigured
vStationChannelState	R	Indicates the operational state of this channel.	Integer	0=disabled 1=enabled
vStationChannelType	R	The phone type for this particular channel.	Integer	1=basic 2=callerID 3=enhanced-Call Waiting

Table 31-30 Station Card Group, Channel table, Station agent **(continued)**

MIB Variable	Access	Definition	Syntax	Value
vStationChannelCallState	R	Indicates the phone call state of this channel. call-state-VOID (0) call-state-IDLE (1) call-state-DIALING (2) call-state-COLLECT-FIRST-DIGIT (3) call-state-COLLECT-DIGITS (4) call-state-CALL-OFFERED (5) call-state-PROCEEDING (6) call-state-RINGING (7) call-state-ALERTING (8) call-state-CONNECTED (9) call-state-DISCONNECTING (10) call-state-FAILED (11) call-state-UNAVAILABLE (12) call-state-OFFHOOK (13) call-state-INITIALIZE (14) call-state-INITIALIZING (15) call-state-DIAL-REQUEST (16) call-state-HELD (17) call-state-FEATURE-INVOKED (18) call-state-OFFHOOK-IDLE (19) call-state-OFFHOOK-ACTIVE (20) call-state-OUT-OF-SERVICE (21) call-state-OUTPULSING (22)	Integer	0-22
vStationChannelCalled PartyNumber	R	The called party's number, either an internal extension or external telephone number.	String	0-32

Table 31-30 Station Card Group, Channel table, Station agent **(continued)**

MIB Variable	Access	Definition	Syntax	Value
vstationChannelCalling PartyNumber	R	The calling party's number, either an internal extension or external telephone number.	String	0-32
vStationChannelChange Pending	R	Indicates that a change to the channel values have been made to the registry. The interpretation of the values are: 1=The change is made to the registry, but not yet incorporated in the device. 0=The device changes the value to 0 from 1, after it incorporates the value from the registry.	Integer	0-1

The Digit Table Group

The Digit Table Groups consists of The First Digit Table.

The First Digit Table

Table 31-31 Digit Table Group, First Digit table, Station agent

MIB Variable	Access	Definition	Syntax	Value
vStationDigitIndex	R	The index to an entry in the First Digit Table.	Integer	1-10
vStationDigitString	R	The first digit string.	String	SIZE (0-1)

Table 31-31 Digit Table Group, First Digit table, Station agent **(continued)**

MIB Variable	Access	Definition	Syntax	Value
vStationDigitCallType	R/W	Type of call generated by this digit. Valid values are: 0=fc-VOID 1=fc-HOLD-CALL 2=fc-PARK-CALL 3=fc-STATION-CALL 4=fc-LONG-DISTANCE-CALL 5=fc-INTERNATIONAL-CALL 6=fc-LOCAL-CALL 7=fc-OPERATOR-CALL 8=fc-RECEPTIONIST-CALL 9=fc-CAMP-ON-CALL	Integer	0-9
vStationDigitMoreDigits	R/W	The number of additional digits to collect after the matched digits.	Integer	0-32
vStationDigitStripDigits	R/W	The number of leading digits to strip from the digits collected before they are reported up to the connection manager.	Integer	0-32

The External Voice Mail System Group

This group contains configuration information used to interface with an external Voice Mail system. This group is subdivided into subgroups depending on the type of Voice Mail system used. The External Voice Mail System Group consists of the ATT System 25 Subgroup.

ATT System 25 Subgroup

The ATT System 25 subgroup contains the Voice Mail Call Handle table.

Table 31-32 ATT System 25 Subgroup, Voice Mail Call Handle table, Station agent

MIB Variable	Access	Definition	Syntax	Value
vStationMWILampON	R	Command expected from the external Voice Mail system to switch on the station's message waiting indicator lamp.	String	SIZE (0-10)
vStationMWILampOFF	R	Command expected from the external Voice Mail system to switch off the station's message waiting indicator lamp.	String	SIZE (0-10)
vStationVMCallHandle Type	R	Indicates the type of access to Voice Mail port made. 1=An external caller coming directly into the Voice Mail port. 2=An external caller calling an extension, and forwarded to the Voice Mail port. 3=An internal caller coming directly into the Voice Mail port. 4=An internal caller calling an extension, and forwarded to the Voice Mail port.	Integer	1=directExternal 2=forwardExternal 3=directInternal 4=forwardInternal
vStationVMCallHandle Opcode	R	The Opcode string for this operation.	Octet String	SIZE (0-32)
vStationVMCallHandle SRCNumber	R	The source number format string. It contains a C type '%s' where the source number would be filled in.	Octet String	SIZE (0-32)
vStationVMCallHandle DSTNumber	R	The destination number format string. It contains a C type '%s' where the destination number would be filled in.	Octet String	SIZE (0-32)

Traps

Table 31-33 Station Private agent, Traps

Trap #	Trap Name	Description	Pertinent MIB Data
12	vStationCannotPlayTone	This notification is sent when the specific channel cannot play a tone.	vStationChannelSlotNumber vStationChannelDeviceNumber vStationChannelIndex
13	vStationCannotCancelTone	This notification is sent when the specific channel cannot cancel a tone.	vStationChannelSlotNumber vStationChannelDeviceNumber vStationChannelIndex
14	vStationCannotAttachDigit Collector	This notification is sent when the specific channel cannot release digits collected.	vStationChannelSlotNumber vStationChannelDeviceNumber vStationChannelIndex
15	vStationCannotReleaseDigitCollector	This notification is sent when the specific channel cannot release digits collected.	vStationChannelSlotNumber vStationChannelDeviceNumber vStationChannelIndex
16	vStationRECONFIG-COMPLETE	This notification is sent when the specific station device successfully reads and incorporates the values from the registry.	vStationChannelSlotNumber vStationChannelDeviceNumber
17	vStationRECONFIG-ERROR	This notification is sent when the specific station device fails to incorporate the values read from the registry.	vStationChannelSlotNumber vStationChannelDeviceNumber

Self Test Daemon (STD)

The Self Test Daemon agent is responsible for showing status and control information for Vertical Communications' Self Test Daemon (STD). The Self Test Daemon is responsible for starting and monitoring each Wave component (executable, service, and drivers). The status of each component (started, stopped, paused, disabled, etc.) as well as the status of the system as a whole is made available.

In addition, since the Self Test Daemon controls the Upgrade and Restore process, this agent generates appropriate traps to notify the various stages of the Upgrade and the Restore (in case the upgrade is unsuccessful) process. Detailed information about each of these traps is available in Table 31-38.

The STD MIB is structured into two groups, as described in Table 31-34.

Table 31-34 Self Test Daemon MIB groups

Group	Description	Tables contained
The System Group	Describes status information about the Wave system as a whole.	None.
The Component Group	Contains status information of each component (executable, service, or driver) within the system.	STDComponentTable

The System Group

The System Group contains just two objects as described in Table 31-35. This group does not have any tables.

Table 31-35 System Group Objects

MIB Variable	Access	Definition	Syntax	Value
sysOperStatus	R	Specifies the current operational status of the Wave ISM. Valid values are: • running—the normal operational status, all components are up and running • startUpInProgress—the STD is starting up the system • upgradeInProgress—the STD is attempting to upgrade the system • restoreInProgress—the STD is attempting to restore the system from a previous installation, after an upgrade attempted failed • error—one or more components failed to start. More information can be found from the components table	Integer	running=0 startUpInProgress=2 upgradeInProgress=3 restoreInProgress=4 error=5
sysCurrentVersion	R	Specifies the current Wave version of the system.	String	

The Component Group

The Component Group contains just one table, the Component table. The Component table defines objects that describe the status information about each component in the system. Table 31-36 describes each of these objects.

Table 31-36 STD MIB, Component table

MIB Variable	Access	Definition	Syntax	Value
compIndex	R	Specifies the numeric index of this component	Integer	
compName	R	Specifies the name of this component	String	

Table 31-36 STD MIB, Component table

MIB Variable	Access	Definition	Syntax	Value
compType	R	Specifies the component type.	Integer	type-driver=1 type-service=16 type-executable=2000 type-non-vni-driver=2001 type-non-vni-service=2002 type-non-vni-executable=2003
compInstallStatus	R	Describes the installation status of this component.	Integer	uninstalled=100 installed=1
compOperStatus	R	Describes the operational status of this component.	Integer	stopped=1 start-pending=2 stop-pending=3 running=4 continue-pending=5 pause-pending=6 paused=7 unknown=8 disabled=1025
compEnabled	R	Determines whether this component is enabled or disabled	Integer	enabled=100 disabled=1
compLastStart	R	Specifies the date-time stamp when this component was last restarted	String	

STD Agent Traps

This agent generates appropriate traps when a trappable condition occurs. Traps generated by this agent fall into two categories:

- Traps that are related to the components controlled by STD (like ComponentFailedToStart, ComponentRestartComplete, etc.)
- Traps that are related to the Upgrade and Restart process. Trap are generated at appropriate stages of the entire upgrade / restore process so that any connected manager will be able to trace the entire sequence of the Upgrade and Restore process (in case the upgrade is unsuccessful). The stages of an upgrade and restore process and the traps generated during this stage are described in Table 31-37.

Table 31-37 STD SNMP Agent, Upgrade and Restore stages

When …	Then …
An upgrade request comes in	• CAB file is pushed • stdUpgradeStarted trap is sent
Unpacking of the CAB file is done	• stdUnpackingFiles trap is sent • Multiple stdUpgradeInProgress traps are sent during this period
Unpacking is complete	• stdUnpackingComplete trap is sent
A system reboot is done	• stdRebootingMachine trap is sent
Upgrade is applied	• stdUpgradeBeingApplied trap is sent • Multiple stdUpgradeInProgress traps are sent during this period
System is rebooted again	• stdRebootingMachine trap is sent
All components are started	• stdVerifyingSystem trap is sent
• If success	• stdUpgradeComplete trap is sent, all is well
• If failed	• stdUpgradeError trap is sent • A restore operation is attempted
Restore is attempted	• stdRestoreStarted trap is sent • Multiple stdRestoreInProgress traps are sent at this point
A system reboot is done	• stdRebootingMachine trap is sent
All components are started	• stdVerifyingSystem trap is sent
• If success	• stdRestoreComplete trap is sent
• If failed	• stdRestoreError trap is sent • STD quits

Table 31-38 STD SNMP Agent, Traps

Trap #	Trap Name	Description	Pertinent MIB Data
26	stdCompFailedToStart	This trap is generated when a component fails to start during initial start up. The Self Test Daemon will attempt to restart this component five times (once each minute), after which it gives up.	sysCurrentVersion compName
27	stdCompAttemptRestart	This trap is generated when the Self Test Daemon attempts to restart a component.	sysCurrentVersion compName
28	stdCompFailedToReStart	This trap is generated when a n attempt to restart a component fails.	sysCurrentVersion compName
29	stdCompRestartComplete	This trap is generated when a component is restarted successfully.	sysCurrentVersion compName
30	stdUpgradeStarted	This trap is generated when an Wave upgrade is started.	sysCurrentVersion
31	stdUnpackingFiles	This trap is generated when unpacking of the generated CAB files starts	sysCurrentVersion
32	stdUnpackingComplete	This trap is generated when unpacking of the upgraded CAB file is complete.	sysCurrentVersion
33	stdUpgradeBeingApplied	This trap is generated when an Wave upgrade is about to be applied. This is done after the CAB file is unpacked and a system reboot is done.	sysCurrentVersion
34	stdUpgradeInProgress	This trap is generated when an Wave upgrade process is under way.	sysCurrentVersion
35	stdUpgradeComplete	This trap is generated when an Wave upgrade is successfully completed.	sysCurrentVersion

Table 31-38 STD SNMP Agent, Traps

Trap #	Trap Name	Description	Pertinent MIB Data
36	stdUpgradeError	This trap is generated when an Wave upgrade attempt fails. A Restore operation would be done immediately.	sysCurrentVersion
37	stdRestoreStarted	This trap is generated when a previous version of Wave is about to be restored. A Restore operation is typically carried out after a failed upgrade attempt.	sysCurrentVersion
38	stdRestoreInProgress	This trap is generated when a previous version of Wave is being restored.	sysCurrentVersion
39	stdRestoreComplete	This trap is generated when a previous version of Wave is successfully restored	sysCurrentVersion
40	stdRestoreError	This trap is generated when a Restore to a previous version of Wave fails. STD normally quits at this point.	sysCurrentVersion
41	stdRebootingMachine	This trap is generated just before an Wave reboot is done, typically due to an upgrade/restore request.	sysCurrentVersion
42	stdVerifyingSystem	This trap is generated when the Wave system is brought up (all components are started) after an Upgrade or a Restore process.	sysCurrentVersion
50	stdIOUptoDate	This notification is sent when an upgrade attempt is aborted because the current version of the Wave software is later than the upgrade version.	sysCurrentVersion

Table 31-38 STD SNMP Agent, Traps

Trap #	Trap Name	Description	Pertinent MIB Data
51	stdBadCABFile	This notification is sent when an upgrade attempt is aborted because of a bad CAB file.	sysCurrentVersion
52	stdNotEnoughDiskSpace	This notification is sent when an upgrade attempt is aborted because there is not enough disk space on the machine.	sysCurrentVersion
63	stdIoNotOperational	This notification is sent under any of the following conditions: • Before attempting to start the components, FBS checks to ensure the minimum configuration is present in the Wave ISM. Currently this means that an RSC card must be present in the Wave ISM. If this check fails, FBS will not attempt to start any of the components and sends the trap. • When FBS attempts to start all components and a critical component fails to start, rendering the Wave ISM non-operational, FBS sends the trap. • After an upgrade is performed and deemed unsuccessful, FBS will attempt to restore to the previous working version of the system software. In case this process fail, FBS sends the trap.	sysCurrentVersion compName
67	stdPrerequisiteMissing	This notification is sent when an upgrade attempt is done on an Wave system that does not contain the prerequisite software version to do the upgrade.	sysCurrentVersion compName
70	stdPLDFailed	Integrated Services Card Firmware upgrade failed.	sysCurrentVersion compName

Table 31-38 STD SNMP Agent, Traps

Trap #	Trap Name	Description	Pertinent MIB Data
88	stdLowDiskSpace	This notification is sent periodically whenever there is low disk space on the machine.	sysCurrentVersion
89	stdHardDiskError	This notification is sent if there is any disk errors found during the daily disk checking.	sysCurrentVersion, compName
90	stdEventLogError	This notification is sent when there are event mining dll matching errors found in the event log.	sysCurrentVersion, compName

IOSystem

The OID for the Wave ISM is to be determined.

T-1 Private

The T-1 private agent is based on the VerticalCommunications' private extension MIB to RFC 1406, and is used to manage the T-1 physical interface, analog channels, and the Integrated Services Card trunk interface. This extension MIB defines additional variables which facilitate the management of the Vertical Wave T-1 modules.

The Private MIB (t1_private.mib) is organized into three tables:

- The Card Table contains status information about each Wave T-1 module. There is one row in the table for each module.
- The Trunk Table defines configuration and status information for each trunk on each T-1 module. There is one entry in this table for each trunk of each module.
- The Channel Table contains generic configuration, status and statistical information about each channel of each trunk.

Card Table

Each entry in the Card Table (Table 31-39) describes the read-only status of a T-1 module in the Wave system, for example, the module type (T-1 module, analog trunk module, Integrated Services Card (vdsx1CardType)), the module slot number (vdsx1CardSlotNumber), the module ISA address (vdsx1CardISAAddress).

Table 31-39 Card table, T-1 private agent

MIB Variable	Access	Definition	Syntax	Value
vdsx1cardSlotNumber	R	Physical slot in the system in which the card is installed	Integer	1-14
vdsx1cardType	R	Vertical's card type	Integer	cardTYPE-DUAL-T1 (1) cardTYPE-8-TRUNK (3) cardTYPE-RESOURCE1 (4) cardTYPE-8-CHANNEL-DID (13) cardTYPE-NOT-CONFIGURED (100)
vdsx1cardDescr	R	Vertical card identification number	Integer	0-255
vdsx1cardRevision	R	Vertical card revision level	Integer	0-255
vdsx1cardDriverVersion	R	Vertical card driver version	Integer	0-255
vdsx1cardIOPortAddress	R	The ISA bus address for this card	Integer	0-'7fffffff'h

Table 31-39 Card table, T-1 private agent **(continued)**

MIB Variable	Access	Definition	Syntax	Value
vdsx1cardErrorLED		The ERROR LED state on this card: The combined values of the ERROR LED and the READY LED are: Error Ready Definition OFF OFF Invalid state ON OFF Just after power up ON ON Software initialization OFF ON Normal operation	Integer	OFF=0, ON=1
vdsx1cardReadyLED	R	The READY LED state on this card. See above description for various combined values of READY and ERROR LEDs.	Integer	OFF=0, ON=1

Trunk Table

Each entry in the Trunk Table (Table 31-40) contains configuration information about each trunk in each module of the system, such as the type of Trunk (T-1, as well as Common Channel Signaling (CCS) vs. Channel Associated Signaling (CAS) (vdsx1TrunkType). In addition, this table describes various status information relating to this trunk, such as the channel count for this trunk (vdsx1channelCount). Each entry in the trunk table is indexed by the interface number of the T-1 device within the system.

Table 31-40 Trunk table, T-1 private agent

MIB Variable	Access	Definition	Syntax	Value
vdsx1TrunkIfIndex	R	The ifIndex (dsx1IfIndex) of this DS1 interface.	Integer	1-'7fffffff'h
vdsx1TrunkIndex	R	The index into the number of trunks associated with the card containing this trunk.	Integer	1-'7fffffff'h
vdsx1TrunkIdentifier	R	The value of the dsx1CircuitIdentifier from the Configuration Table of the T-1 standard MIB.	String	
vdsx1TrunkSlotNumber	R	The logical number of the card containing this trunk.	Integer	0-255
vdsx1TrunkDeviceNumber	R	The value for this object is the logical device number of this trunk within its slot. This number may be used to identify this device in the registry.	Integer	0-255
vdsx1TrunkInterrupt	R	Interrupt Request level for this card / trunk. NOTE: all trunks in the same card have the same IRQ.	Integer	1-2147483647
vdsx1TrunkEnabled	R	Setting this variable to Deactivated will disable the trunk.	Integer	vdsx1TrunkActivated (1) vdsx1TrunkNotConfigured(2) vdsx1TrunkDeactivated (100)
vdsx1TrunkMasterPriority	R	Designates the priority for selecting which trunk is to drive the MVIP clock, for example, which trunk drives the master timing system. The values must be different for each trunk in the system.	Integer	primary (1) secondary (2) notUsed (100)
vdsx1TrunkStream	R	The MVIP stream for this trunk.	Integer	0-7

Table 31-40 Trunk table, T-1 private agent **(continued)**

MIB Variable	Access	Definition	Syntax	Value
vdsx1TrunkStartingChannel	R	The starting MVIP channel for this trunk within its MVIP stream. If CardType is DTM or WAN1, this value is 0; if CardType is CO-POTS, this value is 16 or 24.	Integer	0, 16, 24
vdsx1TrunkType	R	The trunk type for this trunk: defines T-1 and Common Channel Signaling (CCS) vs. Channel Associated Signaling (CAS). All applicable device types are listed here.	Integer	dev-t1CAS (1) dev-t1CCS (2) dev-coPOTS (7) dev-CSU-DSU (16) dev-undef (100)
vdsx1TrunkIsdnSignaling Protocol	R	Defines the switch type for the Isdn protocol stack. • not-applicable=not a supported configuration • invalid=not in range • ess4=USA / AT&T 4ESS • ess5=USA / AT&T 5ESS • dms100=USA / Northern Telecom DMS100 • ni2=USA / National ISDN 2 (BRI, PRI) • dms100s100=NT DMS-100 switch / S-100	Integer	not-applicable (0) invalid (1) ess4 (5) ess5 (6) dms100 (7) ni2 (10) dms100s100 (263)
vdsx1TrunkLineCoding	R	Line coding for Trunk. T-1 trunk can be either B8ZS (2) or AMI (5).	Integer	B8ZS (2) AMI (5)
vdsx1TrunkFraming	R	Defines framing for trunk. T-1 trunk can be either ESF (2) or D4 (3).	Integer	other (1) ESF (2) D4 (3)
vdsx1TrunkNumberOf Channels	R	The maximum number of channels to be initiated for this trunk: 0-24 for T-1, 0-8 for CO POTS.	Integer	0-24

Table 31-40 Trunk table, T-1 private agent **(continued)**

MIB Variable	Access	Definition	Syntax	Value
vdsx1TrunkLineBuildOut	R	Defines the line build out option.	Integer	buildOut-minus7point5dB (1) buildOut-minus15dB (2) buildOut-minus22point5dB (3) buildOut-0dB (100)
vdsx1TrunkLoopback	R	This variable represents the loopback configuration of the DS1 interface.	Integer	vdsx1NoLoop (1) vdsx1PayloadLoop (2) vdsx1LineLoop (3) vdsx1OtherLoop (4)
vdsx1TrunkRedLED	R	Specifies the RED LED status of this trunk.	Integer	OFF=0, ON=1
vdsx1TrunkYellowLED	R	Specifies the YELLOW LED status of this trunk.	Integer	OFF=0, ON=1
vdsx1TrunkChangePending	R	Indicates that a change to the device values have been made to the registry. The interpretation of the values are: 1=change made to the registry, but not incorporated in the device yet. 0=the device changes the value to 0 from 1, after it incorporates the value from registry.	Integer	0-1
vdsx1TrunkLOSThreshold	R	Loss of Signal Threshold in volts. The value is indirectly defined by vdsx1TrunkLoopLength.	Integer	lOS1point36 (0) lOS1point04 (1) lOS0point84 (2) lOS0point62 (3) lOS0point43 (4) lOS0point32 (5) lOS0point22 (6) lOS-NOT-IN-USE (7)

Table 31-40 Trunk table, T-1 private agent **(continued)**

MIB Variable	Access	Definition	Syntax	Value
vdsx1TrunkTransmit PulseMask	R	Transmit Pulse Mask. Its value is indirectly defined by vdsx1TrunkLoopLength.	Integer	1-16777215
vdsx1TrunkReceive Equalizer	R	Receive Equalizer.Its value is indirectly defined by vdsx1TrunkLoopLength.	Integer	FALSE (0) TRUE (1)

Channel Table

Each entry in the channel table (Table 31-41) contains configurable parameters for each channel of each trunk, such as the type of channel (wink start, ground start, clear channel, B channel, D channel(vdsx1ChannelType)), channel enabled status (vdsx1ChannelActivated).

All configurable parameters are written to the registry on each successful SET operation (an operation to set the configuration parameters over SNMP), and the driver reconfigures the device appropriately.

Table 31-41 Channel table, T-1 private agent

MIB Variable	Access	Definition	Syntax	Value
vdsx1channelIndex	R	The logical channel number of the channel within its trunk.	Integer	1-32
vdsx1channelTrunk Index	R	The index of the trunk relative to its card.	Integer	0-255
vdsx1channelSlot Number	R	The slot number of the card to which the trunk containing this channel belongs (vdsx1cardSlotNumber).	Integer	0-255
vdsx1channelTrunk DeviceNumber	R	The value for this object is the logical device number of the trunk containing this channel within its slot, for example, vdsx1TrunkDeviceNumber.	Integer	0-255

Table 31-41 Channel table, T-1 private agent **(continued)**

MIB Variable	Access	Definition	Syntax	Value
vdsx1channelEnabled	R	Setting this variable to Deactivated will disable the channel.	Integer	vdsx1channelActivated (1) vdsx1channelDeactivated (100)
vdsx1channelType	R	The channel type: • vdsx1channelTypeUnknown: unknown type • vdsx1channelTypeWink: Ear and Mouth (E & M) start • vdsx1channelTypeGs: ground start digital trunk • vdsx1channelTypeClear: nailed up clear channel for data • vdsx1channelTypeAnalogImm: analog trunk, immediate start • vdsx1channelTypeBChan: PRI B channel on T-1 • vdsx1channelTypeDChan: PRI D channel on T-1 • vdsx1channelTypeAnalogDt: analog Trunk, dialtone start • vdsx1channelTypeAnalogGs: analog Trunk, ground start • vdsx1channelTypeDDS: DDS channel (56K or 64K) • vdsx1channelTypeAnalogDID: analog channel, DID wink	Integer	vdsx1channelTypeWink (2) vdsx1channelTypeGS (5) vdsx1channelTypeClear (6) vdsx1channelTypeAnalogImm (7) vdsx1channelTypeBChan (8) vdsx1channelTypeDChan (9) vdsx1channelTypeAnalogDt (11) vdsx1channelTypeAnalogGs (12) vdsx1channelTypeDDS (13) vdsx1channelTypeAnalogDID (14) vdsx1channelTypeUnknown (100)

Table 31-41 Channel table, T-1 private agent **(continued)**

MIB Variable	Access	Definition	Syntax	Value
vdsx1channelState	R	Indicates current state of this channel. • OOS=Out Of Service • Idle=Idle • InCall=Inbound call • OutCall=Outbound call • Offline=Off line • Other=Other state • Data=Data • Error=Error • FeRinging=Ringing far end • NeRinging=Incoming ringing • DigitSend=Sending digits • DigitRcv=Receiving digits • IncallEst=Incall established • OutcallEst=Outcall established • IncallClear=Incall clearing • OutcallClear=Outcall clearing	Integer	channelStateOOS (1) channelStateIdle (2) channelStateInCall (3) channelStateOutCall (4) channelStateOffline (5) channelStateOther (6) channelStateData (7) channelStateError (8) channelStateFeRinging (9) channelStateNeRinging (10) channelStateDigitSend (11) channelStateDigitRcv (12) channelStateIncallEst (13) channelStateOutcallEst (14) channelStateIncallClear (15) channelStateOutcallClear (16)
vdsx1channel CallerID	R	The callerID of an incoming caller, if available. If the callerID is not available, then it will have a length of zero.	String	
vdsx1channel ExternalAddress	R	The far end number of a connected call on this channel.If the number is not available, then it will have a length of zero.	String	
vdsx1channel ExternalSubAddress	R	The far end sub address of a connected call on this channel.If this is not available, then it will have a length of zero.	String	
vdsx1channelLocal Address	R	The local number of a connected call on this channel.If the number is not available, then it will have a length of zero.	String	

Table 31-41 Channel table, T-1 private agent **(continued)**

MIB Variable	Access	Definition	Syntax	Value
vdsx1channelLocal SubAddress	R	The local sub address of a connected call on this channel.If the number is not available, then it will have a length of zero	String	
vdsx1channelChange Pending	R	Indicates that a change to the channel values have been made to the registry.The interpretation of the values is: • 1=change made to the registry, but not incorporated in the device yet. • 0=the device changes the value to 0 from 1, after it incorporates the value from registry.	Integer	0-1

T-1 Private Agent Traps

The T-1 private agent also generates the traps and trap notifications to any connected manager under the line error conditions described in Table 31-42.

.

Table 31-42 T-1 private agent traps

Trap #	Trap Name	Description	Variables
1	vdsx1TrunkRedClear	This notification is sent when the specific trunk RED alarm condition clears.	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
2	vdsx1TrunkRed	This notification is sent when the specific trunk goes into the RED alarm situation. Red alarm condition signifies LOS (Loss of Signal) failure, i.e. the receiver sees no positive or negative pulses.	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex

Table 31-42 T-1 private agent traps **(continued)**

Trap #	Trap Name	Description	Variables
3	vdsx1TrunkYellowClear	This notification is sent when the specific trunk YELLOW alarm condition clears.	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
4	vdsx1TrunkYellow	This trap is generated when the specific trunk goes into a YELLOW alarm condition (for example, Loss of Frame condition).	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
5	vdsx1TrunkBlueClear	This notification is sent when the specific trunk BLUE alarm condition clears.	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
6	vdsx1TrunkBlue	This trap is generated when the specified trunk goes into a BLUE alarm condition (for example, Alarm Indication Signal, AIS, meaning the source is sending an unframed stream of one's).	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
7	vdsx1TrunkReconfigComplete	This trap is generated when the trunk has been reconfigured by the driver in response to a SET operation.	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
8	vdsx1TrunkReconfigErr	This trap is generated if the driver is unable to reconfigure the trunk (because of an illegal value or state on a SET operation).	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
43	vdsx1TrunkLoopbackPayloadOn	This notification is sent when the specific trunk enters a payload loopback state. Payload loopback means that the received signal at this interface is looped through the device. Typically the received signal is looped back for re-transmission after it has passed through the device's framing function.	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex

Table 31-42 T-1 private agent traps **(continued)**

Trap #	Trap Name	Description	Variables
44	vdsx1TrunkLoopback PayloadOff	This notification is sent when the specific trunk moves from a payload loopback state to a non-loopback state.	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
45	vdsx1TrunkLoopbackLin eOn	This notification is sent when the specific trunk enters a line loopback state. Under this state the received signal at this interface does not go through the device (minimum penetration) but is looped back out.	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
46	vdsx1TrunkLoopbackLin eOff	This notification is sent when the specific trunk goes out of a Line Looped state	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
86	vdsx1TrunkAnalogDisco nnect	This notification is sent when the specific analog trunk is disconnected.	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
87	vdsx1TrunkAnalogConn ect	This notification is sent when the specific analog trunk is connected	vdsx1TrunkIdentifier vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex
91	vdsx1EnterChannelErro rState	This notification is sent when unexpected signaling is detected on a T1 channel or analog trunk. While in this state, the T1 channel or analog trunk is out of service.	vdsx1cardSlotNumber vdsx1TrunkDeviceNumber vdsx1TrunkIndex vdsx1TrunkIdentifier

System locale settings

System locale settings

This chapter provides information about the advanced locale settings found in the General Settings applet. The Wave system locale will set the default telephone display language, the call numbering plan, and other system settings, associated with the locale you set here.

To access the System Locale settings:

1 If necessary, click the Administration tab of the Management Console.

Click

2 Click the General Settings icon, located in the General Administration section.

3 Select the System tab and click Customize next to the Locale drop-down list.

The Customize Locale dialog appears.

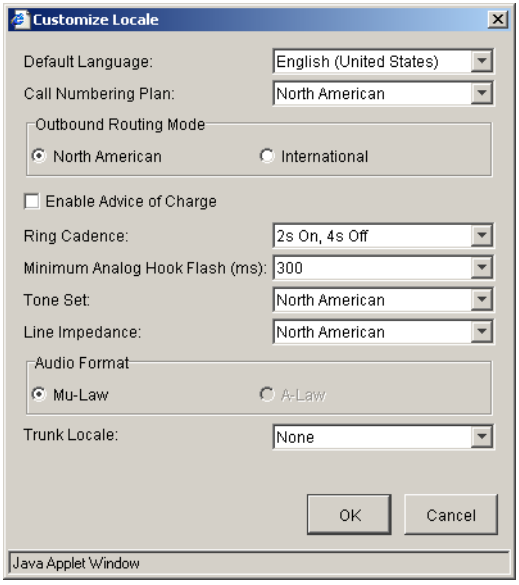


Figure 32-1 Customize Locale dialog

Caution: *You can modify the values associated with the locale you have selected in General Settings. Do not modify these settings unless you are a Wave system configuration expert.*

When you select a locale, you specify the following settings:

- Default language—Specifies the default language used on users' phones, which you may override in when you configure users on the system. If the language has not been set in the User Configuration, Mailbox Configuration, or AutoAttendant Scheduling panels, theWave system will default to the language specified in this field.
- Call numbering plan—Specifies the format of phone numbers. Depending on the locale you choose, the selected call numbering play may affect the settings in the Dialing group box on the Advanced PBX tab of the General Settings applet.
- Outbound routing mode—Determines how outbound calls are processed, using either North American or international (non-North American) numbering.
- Advice of charge—For ISDN, specifies whether the Wave system should expect information regarding the cost of calls. If enabled, call costs will appear on the Call Detail Report.
- Ring cadence—Specifies the duration of each ring and the pause between rings.
- Minimum analog hook flash—Specifies the minimum time an analog phone user must hold down the switch hook to indicate a flash.
- Tone set—Affects the tones (dial tone, busy tone, etc.) users will hear.
- Line impedance—Sets the line impedance of analog trunks to match your locale's default line impedance.
- Audio format—Specifies the audio compression scheme (Mu-Law or A-Law) for digitized voice. At this time only Mu-Law is enabled.
- Trunk locale—Affects the behavior of ISDN services.

Trunk Settings

CHAPTER CONTENTS

Line Build Out settings

Line Build Out is a means of simulating additional cable length between a T-1 trunk's transmitter and the far-end receiver. This is done in case the signal being transmitted is too strong. When the telephone company deploys T-1 lines, each cable runs for 6000 feet before going into a repeater to boost the T-1's signal strength. When the T-1 line reaches its final destination, the final span will generally not be exactly 6000 feet. Instead, the span length will be somewhere between 0 and 6000 feet and average 3000 feet. If the final span is much less than the average, the final repeater's receiver will be much too close to the customer's transmitter. The customer's transmitter signal will be too strong for the repeater to handle.

There are three FCC sanctioned signal levels that the customer can be asked to provide. They are as follows:

- **0 dB**—no artificial cable and therefore no reduction in signal strength
- **-7.5 dB**—puts the signal at 50 percent power
- **-15 dB**—puts the signal at 25 percent power

The customer provisioning letter will state what the Line Build Out (LBO) should be set at. If the provisioning letter does not give an LBO value, then use the 0 dB default.

Vertical Wave also provides a -22.5 dB LBO value (12.5 percent power). This is not sanctioned by the FCC and should never be used with the PSTN. However, for private networks where the far end is only a few feet away, this might be useful.

The default, 0 dB, is the most common signal level for connection to the carrier. If line build out is set incorrectly, the carrier may detect errors, prompting an SNMP yellow alarm and a yellow LED on the T-1 module. If you see such indicators and cannot determine another cause, try changing the Line Build Out setting.

Note: The yellow alarm will occur only in case of extreme errors, such as one in 100 bits being bad.

Customizing transmit and receive signal settings

In the event that the standard Line Build Out settings are not correct for your T-1 configuration, you can customize the following Line Build Out settings. For configuration instructions, see "Configuring digital trunk card or module settings" on page 5-10.

Caution: *Do not modify line build out settings unless you work with your T-1 provider to determine appropriate settings.*

Note: If you find a "canned" cable length that works well, these settings will be grayed out and ignored. If you specify that you are using a Custom Cable, these settings will be used.

- Enable Receive Equalizer

  This setting determines whether automatic receive equalization is enabled or not. If this is enabled, the Wave T-1 framer chip automatically and intelligently boosts the signal coming in to the optimal level for pulse detection. This is called automatic equalization. In this mode, the Wave system can accommodate an incoming signal strength range between -36 and -0 dB.

  If the Enable Receive Equalizer check box is disabled, a fixed (non-intelligent) 6 dB boost is added to the receive signal. If this box is disabled, the Receive Input Threshold list box is then enabled.

- Specify the Receive Input Threshold level

  You enable this when you disable the Enable Receive Equalizer check box. When automatic receive equalization is turned off, the framer chip recovers signals by comparing directly to a Receive Input Threshold. If the signal is lower than the threshold, the chip senses a 0. If the signal is higher than the threshold, the chip

senses a 1. If the signal is exactly the same as the threshold, the result is unpredictable.

1.36 volts is the default threshold level. T-1 signals generally range between 0 and 3 volts in amplitude. However, if a signal is extremely weak, you can set the receive threshold to as little as .22 volts.

Setting the Receive Input Threshold attempts to reduce the input threshold value to accommodate a small input signal.

Note that there are two problems with disabling the automatic equalizer. First is that the Wave system cannot adjust for dynamic changes in the signal strength of the T-1 line with the fixed boost given by the T-1 framer chip. Second, you must try to guess what the optimal input threshold level is. Generally, the automatic equalizer can determine the optimal input signal level better than you can guess the input threshold level.

- Edit the Transmit Pulse Mask

  This field allows you to input raw data to directly determine four points on the shape template of the T-1 pulse that is transmitted. Any changes to this field can easily cause the far-end to be unable to receive the T-1 signal sent by the Wave system. Do not modify this field unless specifically advised to do so by a Vertical Communications Customer Service representative.

Table 33-1 describes the configurable DSX parameters.

Table 33-1 DSX configurable parameters

Display Name	Display Value	Allowed Values	Default Value
Cable Length	0 133 266 299 512 655 3000 6000	0 133 266 299 512 655 3000 6000	655
Receive Equalizer	On Off		On

Table 33-1 DSX configurable parameters

Display Name	Display Value	Allowed Values	Default Value
Receive Input Threshold	1.36 V 1.04 V 0.84 V 0.62 V 0.43 V 0.32 V 0.22 V	1.36 V 1.04 V 0.84 V 0.62 V 0.43 V 0.32 V 0.22 V	1.36
Transmit Pulse Mask (do not modify)	Hex	0x0 to 0xFFFFFF	0x5a9301

Trunk timing values

You can find the Trunk Timers in the Trunk Configuration applet.

T-1 trunk timing values

Table 33-2 describes the different types of inbound T-1 Trunk timers for the E&M Wink Start and E&M Immediate Start signaling types.

Table 33-2 Inbound T-1 trunk timers (E&M Wink Start and E&M Immediate Start)

Display Name	Description	Default Value (msec)
Hit Counter Limit	Not an actual timer, but a counter used to determine a rare condition where a test signaling pattern is being sent by the service provider. If the counter is exceeded, the channel enters an error state.	10
Answer Delay	Minimum delay before answer	70
Inter-Digit	Maximum wait for next digit	15000
Wink Duration (applicable to E&M Wink Start only)	Duration of transmit wink	190

Table 33-2 Inbound T-1 trunk timers (E&M Wink Start and E&M Immediate Start)

Display Name	Description	Default Value (msec)
Far-End Disconnect	Time to wait to determine that far-end has disconnected	300
Call Validate	Time to wait to determine that far-end has disconnected; delay before transmit wink	90
Near-End Disconnect	Time to wait after near-end hangs up for far-end to hang up before treating the situation as an error	300

Table 33-3 describes the different types of outbound T-1 trunk timers for E&M Wink Start and E&M Immediate Start signaling types.

Table 33-3 Outbound T-1 trunk timers (E&M Wink Start and E&M Immediate Start)

Display Name	Description	Default Value (msec)
Error Duration	Length of time-out after an error before the channel is put back in service	30000
Far-End Disconnect	Time to wait to determine that far end has disconnected	250
Near-End Disconnect	Time to wait after near-end hangs up for far-end to hang up before treating the situation as an error	700
Wait Answer	Maximum wait for answer	0 (infinite)
Validate Answer	Minimum length of incoming off-hook to detect answer	600
Maximum Wink	Maximum duration of incoming wink allowed. Timeout is interpreted as GLARE	280
Validate Start Signal (applicable to E&M Wink Start only)	Minimum duration of wink	70)
Wait Start Signal (applicable to E&M Wink Start only)	Maximum wait for wink after near-end disconnects	5000

Table 33-3 Outbound T-1 trunk timers (E&M Wink Start and E&M Immediate Start)

Display Name	Description	Default Value (msec)
Wait Dial	Delay before dial after end of wink	100 (E&M Wink Start) 200 (E&M Immediate Start)
DTMF Duration (applicable to E&M Wink Start only)	Duration of DTMF tone on and off	100

Table 33-4 describes the different types of inbound trunk timers for signaling type ground start.

Table 33-4 Inbound T-1 trunk timers (ground start)

Display Name	Description	Default Value (msec)
Hit Counter Limit	Not an actual timer, but a counter used to determine a rare condition where a test signaling pattern is being sent by the service provider. If the counter is exceeded, the channel enters an error state.	5
Inter-Digit	Maximum wait for next digit	10000
Call Validate	Time to wait to determine that far-end has disconnected; delay before disconnecting	90

Table 33-5 describes the different types of outbound trunk timers for signaling type ground start.

Table 33-5 Outbound T-1 trunk timers (ground start)

Display Name	Description	Default Value (msec)
Error Duration	Length of time-out after an error before the channel is put back in service	30000
Validate Start Signal	Time to wait for dial tone before declaring a glare situation	4000
Wait Start Signal	Maximum wait for tip ground before declaring a glare situation	500

Table 33-5 Outbound T-1 trunk timers (ground start)

Display Name	Description	Default Value (msec)
Far-End Disconnect	Minimum length of incoming on-hook when far-end disconnects first	250
Wait Dial	Delay before dial after tip ground and dial tone detected	10
DTMF Duration	Duration of DTMF tone on and off	100

Table 33-6 describes the outbound trunk timers for ISDN PRI.

Table 33-6 Inbound T-1 trunk timers (ISDN PRI)

Display Name	Description	Default Value (msec)
Alert / Connect Timeout	Milliseconds after an offhook before an incoming call is processed	0
Inter-Digit	Maximum wait for next digit	8000
Maximum wait for Caller ID	Milliseconds after the first ring to wait for caller ID	2000

Analog trunk timing values

Table 33-7 describes the different types of inbound analog trunk timers for loop start and ground start signaling types.

Table 33-7 Inbound analog trunk timers (loop start, ground start)

Display Name	Description	Default Value (msec)
Ring detect trigger	Milliseconds of ringing to be detected by the microcontroller before being reported to the system software	250
CO drop (in / out)	Milliseconds of missing loop current detected by the microcontroller before a line drop event is reported to the system software	400

Table 33-7 Inbound analog trunk timers (loop start, ground start)

Display Name	Description	Default Value (msec)
Disconnect	Maximum wait for far-end disconnect after near-end disconnect of incoming call before treating the situation as an error	10000
Subsequent Ring	Maximum time between subsequent rings before deciding that far-end has given up calling	8000
Offhook Delay	The delay between sending offhook and the switch connection being made. If callers hear noise when being connected to a call on this trunk, adjust this timer for an offhook delay of 160ms. Some experimentation will reveal the best setting. Loop start only.	10
Inter-Digit	Maximum wait for the next digit before routing the call	15000
Hold off, flash (in / out)	Milliseconds after a flash before line events are actively detected	500
Call Validate	Maximum time between first and second ring	7000
Hold off, onhook (in / out)	Milliseconds after an onhook before line events are actively detected	1500
Hold off, offhook (in / out)	Milliseconds after an offhook before line events are actively detected	500

Table 33-8 describes the different types of outbound analog trunk timers for signaling types loop start and ground start.

Table 33-8 Outbound analog trunk timers (loop start, ground start)

Display name	Description	Default value (msec)
Error Duration	Length of time-out after an error before the channel is put back in service	30000
Flash Duration	Length of flash (loop start only)	500
Wait Start Signal	Maximum wait for dial tone	5000

Table 33-8 Outbound analog trunk timers (loop start, ground start)

Display name	Description	Default value (msec)
Disconnect	Maximum wait for far-end disconnect after near-end disconnect of outgoing call before treating the situation as an error	2000
Wait Dial	Delay after dial tone and before dial	500
DTMF duration	Duration of DTMF tone on and off	100

Starting the TFTP Server

Starting the TFTP Server

Vertical Wave includes a TFTP server component to support configuration of the Vertical SIP telephones and is not started by default. The TFTP server is automatically started after you enter the first IP Telephony Client license in the Software Licenses applet. If you need to manually start the TFTP server for some reason, start it using the following procedure.

To start the TFTP server on your Wave system:

1 Click the Vertical Wave Desktop icon in the Management Console.

Click

2 Click OK to clear the warning message that appears.

When you launch certain Microsoft Windows tools from the Vertical Wave Management Console, they start up in a remote control window that allows tools or applications running on the server (the Wave system in this case) to appear on the client (your workstation). Each time you use one of these tools, you will perform a remote control log on. See “Remote Access Application applets” on page 2-5 for detailed information and an example.

3 Log on to Windows.

The default user name is GlobalAdministrator and the default password is Vertical4VoIP!.

4 Click the Start, then All Programs, then ModMgr. The Vertical Communications Component Manager (ModMgr) dialog box opens.

5 Scroll down the list to locate the service called “VNI TFTP Service”.

6 Click on Start to start the service. From this point on, the service will be started and managed automatically by Wave.

7 Close all windows on the desktop.

8 Choose Start, then Log Off to return to the Management Console.

Service Confirmation Letters and Provisioning Information Forms

CHAPTER CONTENTS

The forms shown in this appendix are examples of a Provisioning Information form and a Service Confirmation Letter so you can better understand what type of information you need when configuring T-1 or analog trunks.

Note: The example forms in this appendix may vary due to service provider standards.

Sample trunk provisioning information form

Trunk Group / Provisioning Information Form

Customer Information

NSR: 165151
Customer Name: Vertical Communications
Address: 3979 Freedom Circle, Suite 400
City/State: Santa Clara, CA 95054-1203

Switch: OKLDCACNDC2
Due Date: 11/23/06
SNET DD: 11/23/06

Trunk Group Information

TGN(s): 1478
No. of Members: 24
Signaling: DTMF
No. Digits Sent: 3
IDP Feature (for PIC): 0288

Direction: 2WAY
T-1 Channels: 1-24
In Dial: Wink
Out Dial: Wink
DAS: 12

DFI Information

Ckt Switch: None
Framing: ESF
Signaling: B8ZS

V Trk Type: None
Type: None
Caller ID: Yes

Lead TN / DID Number Range Information

Lead TN: 408-585-0002
DID No. Block(s): 408-585-3400 THRU 3499

RTI: 1478
BTN: 408-585-0002

Channel	TRG#	TN	SM/DNUS/DG-STS/VT	B/D	MEM#	PRI GR#
1-24	1478	n/a	034/0/03/18	n/a	0-23	n/a

Designer Name: John Doe
Designer Phone: 408-555-9876

Issue#: 04
Issue Date: 1/23/98

Sample trunk service confirmation letter

Your trunk confirmation letter from your service provider will contain information similar to that in the sample letter that follows.

Dear Administrator:

The information that follows confirms the services to be provided by the XYZ Telecommunications Group to Vertical Communications at 3979 Freedom Circle, Suite 400, Santa Clara, CA 95054:

- (24) 2-way Digital Trunks
- Block of DIDs
  408-585-3200 through 3299
- T-1 Framing B8ZS-ESF
- Wink Start Signaling
- 3-digit delivery
- RJ-48X Jack Termination

The above service is targeted to be delivered by November 23, 2006. I will provide you with periodic updates as I receive them. Please contact me should you have any questions.

Sincerely,

Sue Simpson
Regional Account Service Coordinator

Part 5

Appendices

Protecting Your Phone System Against Toll Fraud

CHAPTER CONTENTS

About toll fraud

Businesses using any phone system, not just Wave, are vulnerable to loss of money from unauthorized people "hacking" into their phone system. Hackers make hundreds of outbound long distance or international calls that cost businesses around the world millions of dollars every year. Wave contains several features and options that can protect your system against toll fraud.

Typical toll fraud strategies

While hackers committing toll fraud try a variety of techniques to gain access to a system, it is important to note that 99% of the time access is gained through insecure (easy-to-guess) passwords. Wave's System Settings provide several options for enforcing harder-to-guess passwords.

The following are the most common methods of attempted toll fraud:

- Calling the main auto attendant, pressing #, logging in as the Administrator, pressing # for dial tone and placing outbound calls.
- Attempting to log on at every extension (101, 102, etc.) until an extension with an easy password is found. Once found, the hacker will change call forwarding to the external number they want to dial (for example, an international number or the number of another hacked PBX), and then make calls to the external number

as needed. By calling through multiple hacked PBXs, Caller ID and traces will be unable to track down the hacker's identity.

- Calling random users and telling them they are a representative from the phone company and need their voice mailbox password to track down a problem with the phone system. Users should be told to never give out their passwords, and if they have reason to believe someone else has it, to change it immediately to something secure.

Identifying toll fraud

The following methods will help you tell whether your system has been targeted by toll fraud hackers:

- Check your Administrator's call log daily for multiple logon attempts. A failed logon attempt will show as "logon - Abandoned". A successful fraudulent logon will typically show many long distance or international calls placed afterwards from that extension.

  Note: You can have Wave automatically hang up on callers and lock out accounts after multiple failed logon attempts. See “Enforcing strong password security” in Chapter 3 in Administering Wave.

- Check your phone bills carefully for international numbers or long distance numbers you do not recognize.
- Watch your Device Monitor for sudden bursts where every line is busy with people trying to log on.

Protecting your system against toll fraud

The following are a variety of ways to secure your phone system. While practicing all of these strategies will keep your phone system very secure, by far the most important strategy is to just improve the security of passwords.

Password security

Wave System Settings gives you several options for making user passwords more secure. For maximum security you should choose all of the following options:

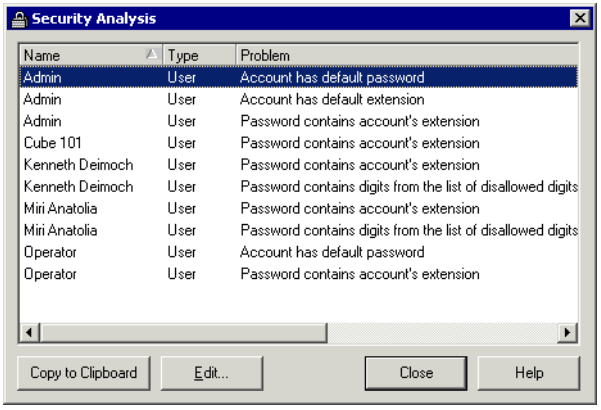
- Set a minimum password length. Passwords should be at least 5 digits long, preferably 7.
- Prevent passwords from including the user's extension.
- Prevent passwords from including easy-to-guess elements like same-digit strings (111) or consecutive-digit strings (123).
- Regularly force password change.

Changing the Admin and Operator passwords

Wave's two default users, the Admin and Operator, have easy-to-guess passwords. Immediately after installing Wave, you should change the passwords on those accounts to something more secure, by editing those users in the Users view. Reminder messages in the Administrator will warn you if you leave the extensions as is.

Identifying users with security-risk passwords

The User / Workgroup Management applet (accessed through "User / Workgroup Management" in the General Administration section of the Management Console) has a built-in Security Analysis report that analyzes your system for potential security risks. To run the Security Analysis report, choose **Tools > Analyze Security**. The report appears on-screen.



Use the report to determine which users in your system have passwords that make your system vulnerable. If you have implemented the security options described in

this section, few users should appear in the list. Those who do might have old passwords that have not yet been changed, either because they have not yet logged in and been forced to change their passwords, or because they are exempt from forced password change. Talk to those users about making their passwords more secure.

You can address your security problems directly from the dialog box by selecting an item and clicking **Edit**. The Edit dialog box for that item opens.

User permissions

Disallow security-risk permissions for all users except those individuals who really need them. You can change permissions for individual users by editing the user account.

- Security-risk permissions which should be disallowed are:
- Place external calls when logged on via a trunk (under the Standard permission group)
- Log on via trunk (Standard)
- Log on via IP trunk (Standard)
- Log on via station (Standard)
- Forward or route calls to external numbers (Standard)
- Return calls when logged on via a trunk (Standard)
- Select a specific trunk for outbound call (Administration)

Setting up dialing restrictions

A good way to prevent unauthorized outbound calling is to place restrictions on users' dialing permissions. You can change permissions for individual users by editing the user account.

Some dialing restrictions to consider:

- Disallow access to any number dialed during toll fraud. To find a list of numbers, search your call logs for frequent calls to international locations.
- Disallow dialing 011 and 00 to block all international calls (00 dials the international operator). To permit some international calls you can do the following:

- Enable 011 for those individuals who are authorized to make international calls. Those individuals can then dial any country.
- Enable country codes for those foreign countries that are appropriate for users to call. To do so, enable 011xxx where xxx is the desired country code.

The full list of country codes can be found in your phone book. The list is maintained by the ITU (International Telecommunication Union), a division of the United Nations. The ITU web site is **http://www.itu.int** and the most recently published list of country codes is available at **http://www.itu.int/itudoc/itu-t/ob-lists/icc/e212_685.html** (this list is valid as of June 2000, and some additional country codes have been assigned since then.)

- Disallow dialing sequences that call for-pay services like 1900 or 1976, 976, etc. For information on additional numbers that should be blocked, see this website:

  http://www.lincmad.com/telesleaze.html

- Disallow dialing certain international North American area codes if desired, such as those in the Caribbean. For example, disallowing 1242 blocks calls to the Bahamas.

  The full list of North American area codes can be found in your phone book or at the web site for the North American Numbering Plan Administration:

  http://www.nanpa.com

  For the numerical list of area codes, see:

  http://docs.nanpa.com/cgi-bin/npa_reports/nanpa?function=list_npa_geo_number

Making account logon more secure

There are several ways to prevent hackers from even getting to the account logon choice of your auto attendant. Some methods make it difficult for your own users to use the system, so you need to judge how far you want to go to prevent toll fraud at the expense of phone system ease of use. Please note that these options do not make your system secure by themselves, as they only slow down hackers. The only way to do that is to make sure your user passwords are secure and change often.

Auto attendant security options include the following:

- In your main auto attendant, change the default "#" for user logon to something else. Ideally, give your remote users a phone number routed to a special auto

attendant that permits remote logon, while your main auto attendant does not. For DID systems, where you can't control the specific trunk used on inbound calls, give your remote users a DID number instead that routes them to the special auto attendant.

- Do not permit logon in your main auto attendant that is assigned to every trunk. Instead, create a unique auto attendant on a different trunk each week that permits logon. Publish the trunk's phone number to your users as it changes.

Securing your phone system database

Toll fraud typically involves “hacking” over phone lines instead of data hacking. However, the Wave database runs on a Windows server on your network and contains all permission settings and can be hacked at that level. It is always wise to keep your corporate network secure from unauthorized external access. This safeguards your database against tampering by network and computer hackers. Some ways to do this include:

Use standard firewall technology to secure access to your network. If desired, allow access to specific protocols and ports, such as those for HTTP (VoIP).

For extra security, host the Wave Web Services on a separate server from the Wave Server and database.

Securing SIP stations

If your system uses SIP phones as external stations, hackers can gain entry to the system by sending a SIP message that duplicates the SIP URI of a SIP phone user, for example, vwilliams@sip:www.Vertical.com. Without protection, Wave assumes the call is coming from the external station and automatically logs it in and provides internal dial tone, permitting the caller to place outbound calls through Wave.

To protect against SIP fraud, you can do the following:

- Make sure that each SIP phone uses authentication credentials whenever it connects to Wave.
- If your system interacts with an external SIP server, such as a PSTN gateway or a SIP provider (IPSP), set up two SIP spans, one to handle SIP stations and the other to handle traffic from the external SIP server.

Checking for current scams

Most telephone carriers maintain toll fraud web pages with current information. For example:

http://www.att.com/fraud/

newscenter.verizon.com/kit/servicestandard/scams.vtml

You can monitor these web sites for up-to-date information and potential remedies.

Responding to toll fraud attempts

If your phone system has been the target of toll fraud attempts, you can do the following:

- Report Caller ID numbers and called numbers of fraudulent calls to your long distance carrier. Sometimes carriers can block certain numbers from calling you.
- Report excessive toll fraud to your local FBI office. Note, however, that the FBI does not usually get involved with toll fraud unless losses are substantial.

You can also use the information from previous toll fraud attempts to make your system even more secure. For example, you can add any numbers being called during toll fraud to the list of numbers prevented with dialing permissions. If fraudulent calls have been made to a particular few countries that are not otherwise called, disallow dialing those country codes (011xxx).

Software License Agreement

VERTICAL COMMUNICATIONS, INC.

End User Software License Agreement

NOTICE: Please carefully read this End User Software License Agreement (this "EULA") concerning your use of certain software that is owned or is provided under license by Vertical Communications, Inc., and was provided to you by Vertical Communications, Inc., or a subsidiary, affiliate or authorized dealer, distributor or other authorized sublicensor (hereafter, collectively, Vertical Communications, Inc. and any such subsidiary, affiliate or authorized third party from which you obtained such software shall be referred to as "Vertical"). The software was pre-installed with the "System" (as defined below) that you acquired or was subsequently provided by downloading from Vertical's website or by means of a disk installed by Vertical or by you. The software is provided to you under license from Vertical, and is not sold. As further described herein below, Vertical expressly retains and reserves for and unto itself, all rights of title, ownership, copyright, license and/or all other applicable rights not expressly granted hereby.

SYSTEM. You have acquired a telecommunications system ("System") from Vertical that includes software. The software may include, in whole or in part, software licensed by Vertical from an affiliate of Microsoft Corporation ("MS") and/or other sources. All installed software products ("Software"), as well as associated media, printed materials, and online or electronic documentation (hereafter, collectively, the "Documentation,"), whether of Vertical, MS or other origin, are protected by domestic and international intellectual property laws and treaties, are intended only for use in connection with the System in accordance with the terms of this EULA. Any other use of the Software or the Documentation is strictly prohibited. To the extent the Software is comprised of products of Vertical origin, Vertical and its suppliers own the title, copyright and other intellectual property rights in the Software. To the extent the Software is comprised of products of MS origin, MS and its suppliers (including Microsoft Corporation) own the title, copyright and other intellectual property rights in the Software. To the extent the Software is comprised of products of other origin, such other party and its suppliers own the title, copyright and other intellectual property rights in the Software.

By using the Software, you accept these terms. If you do not accept them, do not use the Software. Instead, contact Vertical Communications, Inc. to determine its return policy for a refund or credit.

As described below, using some features also operates as your consent to the transmission of certain standard computer information for Internet-based services.

If you comply with these license terms, you have the rights below.

1. USE RIGHTS.

- *Software.* Software provides functions or services on this System. You may access, boot from, display and run the primary operating copy of the Software only on this System. Your may use the secondary boot and/or recovery copies of the Software installed on or distributed with this System (if any) as described below in these license terms. You may reinstall the Software on this System. You may not use the Software, or its components for use on another System or server.
- *Vertical Wave System Editions.* Vertical Wave System Editions allow Users (devices and clients) access to the Software up to following edition user maximums:
    - Wave Standard Edition – allows for a maximum of 50 users.
    - Wave Professional Edition – allows for a maximum of 200 users.
    - Wave Enterprise Edition – allows for a maximum of 350 users.

  A User is defined as any physical endpoint device (hard phone, soft phone, wireless phone or fax) with an extension of DID number that accesses or uses the Software.
- *Device Software.* Device software allows a device (other than this System) to access or use the Software. A device may be a digital phone, analog phone, wireless phone, or facsimile machine. You may install and use the device software on any number of devices.
- *Client Software.* Client software allows a client (other than this System) to access or use the Software. A client may be a server, personal computer or hand held PDA. You may install and use the client software on any number of clients.
- *Processor Rights.* You may use the Software with not more than 4 processors at any one time.

End User Software License Agreement

2. ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.

a. **Specific Use.** Vertical Communications, Inc. designed this System for a specific use. You may only use the Software for that use.

You may not use the Software to support additional software programs or functions, other than utilities or similar software used solely for administration, performance enhancement and/or preventative maintenance of this System.

b. **Software Use Limits.** You are not licensed to use any of the following functions of the Software, except as described below:

- Authentication Service functions (i.e., authentication services, including use of the Software as a domain controller or any other use of DCPromo.exe)
- IntelliMirror Services (i.e., the IntelliMirror management technologies of the Software)
- Network Infrastructure Services. These are functions of the Software necessary to support a server network infrastructure. You are licensed to use these functions only for:

  (A) Dynamic Host Configuration Protocol services for IP address assignment for functionality provided by the System; and

  (B) Domain Name System (DNS) service used for name resolution for functionality provided by the System, but only for a single domain name acting in primary mode (i.e., no secondary DNS for replication) and in stand alone mode (i.e., not integrated with Active Directory domain controller). You may use Routing and Remote Access Service (RRAS), but only those functions necessary for routing and remote access for management and configuration. The VPN gateway shall not be used to access other server resources or allow remote users to gain network access. You may use Windows Internet Name Service (WINS) but only to support the functionality provided by the System.
- Printing Services. These include print spoolers, drivers, and related files in the Software that enable operation of a printer. You are licensed to use these services only to generate and print reports concerning services provided by this System.
- Terminal Services (i.e., using the terminal services feature of the Software or using other software used with the Software to provide similar services). Authorized system administrators may access and use up to 2 connections solely for the purpose of administration (including remote administration) of the Software running on this System.
- Volume Shadow Copy Service (i.e., the feature in the Licensed Product which enables point-in-time copying of files).

- **Limits on Functions Supported by the Software.** Vertical Communications, Inc. licenses you to use the Software to support only the base functions as provided and installed on this System. You are not licensed to use the Software to run or support:

  (i) directory services (such as Microsoft Active Directory),

  (ii) enterprise database software (such as Microsoft SQL Server), except non-enterprise engines used to support the specific use for which Vertical Communications, Inc. designed this server, such as Microsoft SQL Server Desktop Engine and Microsoft SQL Server 2005 Express Edition. The server software also may run or support enterprise database engines (including Microsoft SQL Server) that are integrated in, and used only to support, the Software as part of the specific use for which Vertical Communications, Inc. designed this System,

  (iii) enterprise resource planning software,

  (iv) messaging or enterprise mail (except POP3 mail and/or a platform enabling a voice messaging application),

  (v) collaboration software (such as Microsoft Exchange),

  (vi) web-based time management applications that address appointment, meeting and other calendar items,

  (vii) Microsoft Exchange, and/or

  (viii) any office automation or personal computing functions (such as word processing, spreadsheets, network browsing or personal finance), regardless of whether installed by Vertical Communications, Inc., you or another person.
- **No CALs Required.** Devices that access or use functions of Software licensed under these license terms do not require a client access license (CAL). Obtaining a CAL for any Microsoft product does not grant you rights to use functions of the Software not licensed under this EULA.

End User Software License Agreement

3. **SCOPE OF LICENSE.** The Software is licensed, not sold. This agreement only gives you some rights to use the Software. Vertical Communications, Inc. and Microsoft reserve all other rights. Unless applicable law gives you more rights despite this limitation, you may use the Software only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the Software that allow you to use it only in certain ways. For more information, see the Software documentation or contact Vertical Communications, Inc.. Except and only to the extent permitted by applicable law despite these limitations, you may not:

   - work around any technical limitations in the Software;
   - reverse engineer, decompile or disassemble the Software;
   - make more copies of the Software than specified in this agreement;
   - publish the Software for others to copy;
   - rent, lease or lend the Software; or
   - use the Software for commercial software hosting services.

   Except as expressly provided in this agreement, rights to access the Software on this System do not give you any right to implement Vertical Communications, Inc. or Microsoft patents or other Vertical Communications, Inc. or Microsoft intellectual property in software or devices that access this System.

   You may use remote access technologies in the Software such as Remote Desktop to access the Software remotely from another device. You are responsible for obtaining any licenses required for use of these protocols to access other software.

   - **COMPONENT DATA STORAGE.** The Software may contain components that use Microsoft SQL Server Desktop Engine ("MSDE"). Only those software components may use MSDE.
   - **INTERNET-BASED SERVICES.** Microsoft provides Internet-based services with the Software. Microsoft may change or cancel them at any time.

     a. **Consent for Internet-Based Services.** The Software features described below connect to Microsoft computer systems over the Internet. In some cases, you will not receive a separate notice when they connect. You may switch off these features or not use them. For more information about these features, visit

     http://www.microsoft.com/windowsxp/downloads/updates/sp2/docs/privacy.mspx.

     By using these features, you consent to the transmission of this information. Microsoft does not use the information to identify or contact you.

     b. **Computer Information.** The following features use Internet protocols, which send to the appropriate systems computer information, such as your Internet protocol address, the type of operating system, browser and name and version of the Software you are using, and the language code of the device where you installed the Software. Microsoft uses this information to make the Internet-based services available to you.

     - ***Digital Certificates.*** The Software uses digital certificates. These digital certificates confirm the identity of Internet users sending X.509 standard encrypted information. The Software retrieves certificates and updates certificate revocation lists. These security features operate only when you use the Internet.
     - ***Auto Root Update.*** The Auto Root Update feature updates the list of trusted certificate authorities. You can switch off the Auto Root Update feature.
     - ***Windows Media Digital Rights Management.*** Content owners use Windows Media digital rights management technology (WMDRM) to protect their intellectual property, including copyrights. This Software and third party software use WMDRM to play and copy WMDRM-protected content. If the Software fails to protect the content, content owners may ask Microsoft to revoke the Software's ability to use WMDRM to play or copy protected content. Revocation does not affect other content. When you download licenses for protected content, you agree that Microsoft may include a revocation list with the licenses. Content owners may require you to upgrade WMDRM to access their content. Microsoft software that includes WMDRM will ask for your consent prior to the upgrade. If you decline an upgrade, you will not be able to access content that requires the upgrade. You may switch off WMDRM features that access the Internet. When these features are off, you can still play content for which you have a valid license.

     c. **Misuse of Internet-based Services.** You may not use these services in any way that could harm them or impair anyone else's use of them. You may not use the services to try to gain unauthorized access to any service, data, account or network by any means.

End User Software License Agreement

- **BENCHMARK TESTING.** The Software may contain the Microsoft .NET Framework. You may conduct internal benchmark testing of the .NET Framework component of the Software (".NET Component"). You may disclose the results of any benchmark test of the .NET Component, if you comply with the following terms:

  (1) you must disclose all the information necessary for replication of the tests;

  (2) you must disclose the date(s) when you did the benchmark tests and version information for all Microsoft software products tested;

  (3) your benchmark testing was performed in accordance with the product documentation and/or Microsoft's support Web sites, and uses the latest updates, patches, and fixes available for the .NET Component and the relevant Microsoft operating system;

  (4) it is sufficient if you make the disclosures at a publicly available location such as a Web site, so long as a public disclosure of the results of your benchmark test expressly identifies the public site containing all required disclosures; and

  (5) nothing in this provision shall be deemed to waive any other right that you may have to conduct benchmark testing.

  The above terms shall not apply to your disclosure of any customized benchmark test of the .NET Component, if a prospective customer makes such disclosure under confidentiality in conjunction with a bid request. If you disclose such benchmark test results, Microsoft shall have the right to disclose the results of benchmark tests it conducts of your products that compete with the .NET Component, provided it complies with the same conditions above.

- **NOTICES ABOUT THE MPEG-4 VISUAL STANDARD.** The Software may include MPEG-4 visual decoding technology. This technology is a format for data compression of video information. MPEG LA, L.L.C. requires this notice:

  > USE OF THIS PRODUCT IN ANY MANNER THAT COMPLIES WITH THE MPEG-4 VISUAL STANDARD IS PROHIBITED, EXCEPT FOR USE DIRECTLY RELATED TO (A) DATA OR INFORMATION (i) GENERATED BY AND OBTAINED WITHOUT CHARGE FROM A CONSUMER NOT THEREBY ENGAGED IN A BUSINESS ENTERPRISE, AND (ii) FOR PERSONAL USE ONLY; AND (B) OTHER USES SPECIFICALLY AND SEPARATELY LICENSED BY MPEG LA, L.L.C.

  If you have questions about the MPEG-4 visual standard, please contact MPEG LA, L.L.C., 6312 S Fiddlers Green Circle, Suite 400E Greenwood Village, Colorado 80111; www.mpegla.com.

  - **SECONDARY BOOT AND RECOVERY COPIES OF THE SOFTWARE.**

    Secondary Boot Copy. If a secondary boot copy of the Software is installed on the System, you may access, boot from, display and run it solely in the event of a failure, malfunction, or corruption of the primary operating copy of the Software, and only until the primary operating copy has been repaired or reinstalled. You are not licensed to boot from and use both the primary operating copy and the secondary boot copy of the Software at the same time.

    Recovery Copy. You may use recovery copy solely to repair or reinstall the Software on the System.

  - **LEASED HARDWARE.** If you lease the System from Vertical Communications, Inc., the following additional terms shall apply: (i) you may not transfer the Software to another user as part of the transfer of the System, whether or not a permanent transfer of the Software with the System is otherwise allowed in these license terms; (ii) your rights to any Software upgrades shall be determined by the lease you signed for the System; and (iii) you may not use the Software after your lease terminates, unless you purchase the System from Vertical Communications, Inc..

  - **NO RENTAL.** You may not rent, lease, lend, or provide commercial hosting services with the Software.

4. **PRODUCT SUPPORT.** Contact Vertical Communications, Inc. for support options. Refer to the support number provided with the System.

   Vertical Communications, Inc. will provide support services only for the most current and immediately preceding release of the Software. Vertical Communications, Inc. shall have no responsibility under this EULA to fix any errors arising out of or related to the following causes: (a) modification or combination of the Software (in whole or in part), including, but not limited to, custom install scripts; (b) use of the Software in an environment other than a supported environment; (c) use of Beta Software; or (d) accident; unusual physical, electrical or electromagnetic stress; neglect; misuse; failure or fluctuation of electric power, air conditioning or humidity control; failure of media not furnished by Vertical Communications, Inc.; excessive heating; fire and smoke damage; operation of the Software with other media and hardware, software or telecommunication interfaces not meeting or not maintained in accordance with the manufacturer's specifications; or causes other than ordinary use.

5. **BACKUP COPY.** You may make one backup copy of the Software. You may use it only to reinstall the Software on the device.

End User Software License Agreement

6. **PROOF OF LICENSE.** If you acquired the Software on the System, or on a disc or other media, a genuine Certificate of Authenticity label with a genuine copy of the Software identifies licensed Software. To be valid, this label must be affixed to the System, or included on or in Vertical Communications, Inc.'s Software packaging. If you receive the label separately, it is not valid. You should keep the label on the System or packaging to prove that you are licensed to use the Software. To identify genuine Microsoft software, see http://www.howtotell.com.
7. **TRANSFER TO A THIRD PARTY.** You may transfer the Software only with the System, the Certificate of Authenticity label, and these license terms directly to a third party. Before the transfer, that party must agree that these license terms apply to the transfer and use of the Software. You may not retain any copies of the Software including the backup copy.
8. **NOT FAULT TOLERANT.** The Microsoft software is not fault tolerant. Vertical Communications, Inc. installed the Software on the System and is responsible for how it operates on the device.
9. **RESTRICTED USE.** The Software is not designed or intended for use or resale in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control or other devices or systems in which a malfunction of the Software would result in foreseeable risk of injury or death to the operator of the device or system, or to others.
10. **NO WARRANTIES FOR THE SOFTWARE.** The Software is provided "as is". You bear all risks of using it. Vertical Communications, Inc. and Microsoft give no express warranties, guarantees or conditions. Any warranties you receive regarding the System or the Software do not originate from, and are not binding on, Vertical Communications, Inc., Microsoft or its affiliates. When allowed by your local laws, Vertical Communications, Inc. and Microsoft exclude implied warranties of merchantability, fitness for a particular purpose and non-infringement.
11. **LIABILITY LIMITATIONS.** You can recover from Vertical Communications, Inc. or Microsoft and its affiliates only direct damages up to two hundred fifty U.S. Dollars (U.S. $250.00), or equivalent in local currency. You cannot recover any other damages, including consequential, lost profits, special, indirect or incidental damages.

    This limitation applies to:

    - anything related to the Software, services, content (including code) on third party internet sites, or third party programs, and
    - claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

    It also applies even if Vertical Communications, Inc. or Microsoft should have been aware of the possibility of the damages. The above limitation may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.
12. **EXPORT RESTRICTIONS.** The Software is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the Software. These laws include restrictions on destinations, end users and end use.

ACTIVATION OF SOFTWARE. The Software must be registered and activated with Vertical Communications, Inc. within thirty (30) days of installation. Failure to activate Software within the stated timeframe will result in the Software being inoperable until it is properly registered and activated with Vertical Communications, Inc.

MANIFEST AND LICENSE INFORMATION. In some cases, Vertical Communications, Inc. may require that you provide certain information, including System manifest, Software licenses and System configuration during the registration process or support activities in order to enable the Software to work properly. In all such cases, you will be advised in advance of any such requirement and will be given the opportunity to terminate the process prior to transmittal of any such information.

REMOTE ACCESS. Vertical Communications, Inc. reserves the right to remotely access the System and Software in order to provide technical support and for Software repair purposes. In all such cases, you will be advised in advance of any such requirement and will be given the opportunity to terminate the process prior to any such remote access.

SOFTWARE UPDATES. All updates to the Software will come directly from Vertical Communications, Inc. Any software updates from other sources, including Microsoft that result in the Software being inoperable will not be supported by Vertical Communications, Inc..

End User Software License Agreement

LIMITED MEDIA WARRANTY. Vertical Communications, Inc. warrants that any media on which the Software is recorded will be free from defects in materials and workmanship under normal use for a period of 90 days from the date the Software is shipped to reseller. If a defect in any such media should occur during this 90-day period, the media may be returned to Vertical and Vertical will replace the media without charge. Vertical shall have no responsibility to replace media if the failure of the media results from accident, abuse or misapplication of the media.

INDEMNIFICATION. Licensee agrees to indemnify, defend, and hold harmless Vertical Communications, Inc. from any suit, demand, cause of action or other claim of whatever nature arising out of the breach of any term of this EULA by Licensee, Licensee's agents or employees that arise or result from the use or distribution of the Software or Documentation.

GOVERNMENT LICENSEES. This provision applies to all Software and Documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and Documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights and use, and duplication or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software Restricted Rights clause of FAR 52.227-19 or subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013 or their successors, whichever is applicable.

TERM AND TERMINATION. Without prejudice to any other rights, Vertical Communications, Inc. may terminate this license if you fail to comply with the licensing terms. In such event, you must destroy all copies of the Software and all of its component parts. This License is effective until terminated; however, all of the restrictions with respect to Vertical's copyright in the Software and Documentation will cease being effective at the date of expiration of the applicable Vertical copyright; those restrictions relating to use and disclosure of Vertical's confidential information shall continue in effect. Licensee may terminate the License at any time. Upon termination for any reason, Licensee will immediately destroy or return to Vertical the Software, Documentation and all copies of each. Those provisions of this EULA that, by their nature, are intended to survive the termination of this EULA shall so survive. Without limiting the generality of the foregoing, the following sections shall survive any termination: "Restrictions on Use; Reservation of Rights", "Export Restriction", "No Warranties for the Software", "Limitation of Liability", "Trademarks", "Indemnification" and "General."

GENERAL. If any provision of this EULA shall be held by a court of competent jurisdiction to be illegal, invalid or unenforceable, that provision shall be limited or eliminated to the minimum extent necessary so that this EULA shall otherwise remain in full force and effect and enforceable. This EULA will be governed by the laws of the State of Florida without respect to any conflict of laws principles. Neither the License nor this EULA is assignable or transferable by Licensee without Vertical's prior written consent, and any attempt to do so shall be void. Vertical may assign its rights and obligations under this EULA, in whole or in part, without Licensee's consent. Any notice, report, approval or consent required or permitted hereunder shall be in writing. No failure to exercise, and no delay in exercising, on the part of either party hereto, any privilege, any power or any rights hereunder will operate as a waiver thereof, nor will any single or partial exercise of any power hereunder preclude further exercise of any other right hereunder. The parties hereto agree that a material breach of this EULA by Licensee would cause irreparable injury to Vertical for which monetary damages would not be an adequate remedy and that Vertical shall be entitled to equitable relief in addition to any remedies it may have hereunder or at law.

Should Licensee have any questions concerning this EULA, contact Vertical Communications, Inc., 106 Cattlemen Road, Sarasota, Florida 34232.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS EULA, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS EULA IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN VERTICAL AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS EULA. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST VERTICAL UNLESS VERTICAL GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS EULA.

Index

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z