555-7101-306

CallPilot

VPIM Networking Implementation and Administration Guide

Product release 2.5 Standard 1.0 October 2003

NORTEL NETWORKS™

CallPilot

VPIM Networking Implementation and Administration Guide

Publication number:	555-7101-306
Product release:	2.5
Document release:	Standard 1.0
Date:	October 2003

Publication history

October 2003

Standard 1.0 issue of the CallPilot 2.5 *VPIM Networking Implementation and Administration Guide* is released.

Contents

chapter 1

About CallPilot

This chapter introduces CallPilot, the powerful multimedia messaging system from Nortel Networks. CallPilot offers a single solution for managing many types of information, including voice mail, fax-mail, e-mail, telephone calls, conferencing, calendars, directories, and call logs.

CallPilot enables you to get all the information you need from one source, whether through display-based telephone sets, your wireless set, your Windows desktop computer, a speech recognition interface, or another personal communications device.

In this chapter

About this guide

In this section

Overview

Introduction

The *VPIM Networking Implementation and Administration Guide* provides detailed instructions for implementing Voice Profile for Internet Mail (VPIM) Networking.

Assumptions

This guide assumes that the Meridian Application Server has been correctly installed and is operational. If the application has not been installed, then install it before proceeding. For installation instructions, refer to the hardware installation guide appropriate to your server type.

If the server has been installed but is not operational, refer to the *Maintenance and Diagnostics Guide* for information on troubleshooting your system.

Skills you need

Introduction

You need certain skills and knowledge to use this guide effectively.

Nortel Networks product knowledge

Knowledge of, or experience with, the following Nortel Networks products will assist you:

- previous releases of CallPilot
- Meridian Mail

PC experience or knowledge

Knowledge of, or experience with, the following PC products will be of assistance. This guide does not document the following functionality:

- Microsoft Windows NT
- Microsoft Windows 95
- Microsoft Windows 2000

Other experience or knowledge

Other types of experience or knowledge that may be of use include the following:

- switch configuration and operation (especially trunk group access restrictions [TGARs] and network classes of service [NCOS])
- network management
- client-server systems
- flowcharting
- troubleshooting

How this guide is organized

Introduction

The *VPIM Networking Implementation and Administration Guide* is organized in the sequence of tasks required to successfully implement VPIM Networking for CallPilot. Start at the beginning of the guide and work your way through it until all required tasks are completed.

Contents

This guide contains the following chapters.

Chapter title	Description
Chapter 1, About CallPilot	This chapter describes how to work with the CallPilot interface and how to use this guide.
Chapter 2, Getting started	This chapter provides an overview of VPIM Networking. This chapter describes the features supported by VPIM Networking and how VPIM Networking works. This chapter also provides a high-level overview of the tasks that are performed during implementation.
Chapter 3, Gathering information	This chapter explains how to gather the information required to implement VPIM Networking.
Chapter 4, Configuring CallPilot for VPIM Networking	This chapter describes how to configure CallPilot for VPIM Networking. This chapter describes every box that must be completed and provides detailed procedures.

Chapter title	Description
Chapter 5, Adding sites to VPIM Networking	This chapter describes how to configure the local site. This chapter also describes how to add and configure every site in the messaging network that uses VPIM Networking to exchange messages with local site. This chapter describes every box that must be completed and provides detailed procedures.
Chapter 6, Testing and backing up VPIM Networking	This chapter describes how to test the implementation of VPIM Networking to ensure that it is properly configured. This chapter also describes how to perform a backup of the system.
Chapter 7, Maintaining VPIM Networking	This chapter explains how to perform both regularly scheduled maintenance tasks and as-required maintenance tasks.
Chapter 8, Troubleshooting VPIM Networking	This chapter provides information to identify and solve problems with VPIM Networking.
AppendixA, VPIM conformance	This appendix shows how VPIM Networking conforms to the VPIM profile.

Related information products

Introduction

The following CallPilot technical documents are stored on the CD-ROM that you receive with your system. The documents are also available from the following sources:

- CallPilot Manager
- My CallPilot
- the Nortel Networks Partner Information Center (PIC) at http://my.nortelnetworks.com

  You require a user ID and a password to access the PIC. If you do not have a PIC account, click Register to request an account. It can take up to 72 hours to process your account request.

You can print part or all of a guide, as required.

Note: To order the documents that are available in printed format, contact your Nortel Networks sales representative.

Planning and migration guides

Use these guides before you install CallPilot to help plan your system, or to plan a migration of data from Meridian Mail to CallPilot:

Document title	NTP number
Installation and Configuration Planner	—
Planning and Engineering Guide	555-7101-101
What's New Guide	555-7101-901

Installation and configuration guides

The following guides describe how to install the following:

- CallPilot server hardware and software
- desktop messaging and My CallPilot software

Document title	NTP number
Desktop Messaging and My CallPilot Installation Guide	555-7101-505
Installation and Configuration Guide for your server model This is a binder that contains the following five documents: ■ *Part 1: Installation and Maintenance Overview* ■ *Part 2: <Server model> Server Hardware Installation* ■ *Part 3: <Switch name> and CallPilot Server Configuration* ■ *Part 4: Software Installation and Maintenance* ■ *Part 5: <Server model> Server Maintenance and Diagnostics*	Refer to the *CallPilot Installation and Configuration* binder for NTP numbers.

Administration guides

The following guides provide specialized information to help you configure administer and maintain CallPilot, and use its features:

Document title	NTP number
Administrator's Guide	555-7101-301
Reporter Guide	555-7101-310
Application Builder Guide	555-7101-325

Document title	NTP number
Desktop Messaging and My CallPilot Administration Guide	555-7101-503
Meridian Mail to CallPilot Migration Utility Guide	555-7101-801

Networking guides

The following guides describe how to plan, install, set up, and troubleshoot the CallPilot networking services:

Document title	CallPilot release	NTP number
Networking Enhancements Guide	2.0	555-7101-507
Networking Planning Guide	1.0	555-7101-100
NMS Implementation and Administration Guide	1.0	555-7101-302
AMIS Networking Implementation and Administration Guide	1.0	555-7101-303
Enterprise Networking Implementation and Administration Guide	1.0	555-7101-304
Integrated AMIS Networking Implementation and Administration Guide	1.0	555-7101-305
VPIM Implementation and Administration Guide	1.0	555-7101-306

Note: For instructions on how to configure the networking services on CallPilot, refer to the CallPilot Manager online Help.

End user guides

The following guides are intended for CallPilot end users, such as telephone set users and desktop messaging users:

Document titles
Unified Messaging Quick Reference Card
Unified Messaging Wallet Card
Unified Messaging What's New Card
Command Comparison Cards
Menu Interface Quick Reference Card
Alternative Command Interface Quick Reference Card
Multimedia Messaging User Guide
Speech Activated Messaging User Guide
Desktop Messaging User Guides
My CallPilot User Guide

Troubleshooting

The *CallPilot Troubleshooting Reference* describes symptoms that can appear on all CallPilot server platforms, and describes ways to resolve them.

The *CallPilot Troubleshooting Reference* is intended for Nortel Networks distributors and technical support representatives; therefore, it is not part of the customer documentation package. Nortel Networks continually updates the *CallPilot Troubleshooting Reference*, which is available from the Nortel Networks Partner Information Center (PIC) at http://my.nortelnetworks.com.

You require a user ID and a password to access the PIC. If you do not have a PIC account, click Register to request an account. It can take up to 72 hours to process your account request.

Note: If you are not a Nortel Networks distributor, then contact your Nortel Networks technical support representative for assistance.

Using online sources

CallPilot administration online Help

The CallPilot Manager and CallPilot Reporter software contain administration online Help areas that provide access to

- technical documentation in Acrobat PDF format
- online Help topics in HTML format

To access online information, use either of the following methods:

- Click the orange Help button at the top of any page to access the Administration Help area.
- Click the grey Help button on any page to display a topic that relates to the contents of the page.

For more information about using these Help systems, access the CallPilot Manager Help, open the Getting Started book, and click “Navigating CallPilot Manager Help.”

The Application Builder software contains a Windows Help system as well as context-sensitive Help (available by clicking the ? button and then a field or label).

CallPilot end-user online Help

The My CallPilot software contains a Useful Information area that provides access to the end-user guides in PDF format.

To access online Help for the currently selected My CallPilot tab, click the Help button on the upper-right corner of the My CallPilot page.

Desktop messaging provides product-specific Windows Help for groupware clients (Microsoft Outlook, Novell GroupWise, and Lotus Notes). The stand-alone version of CallPilot Player also provides addressing and troubleshooting information for Internet mail clients.

Contacting technical support

Contact your distributor's technical support organization to get help with troubleshooting your system.

Conventions

Commands documented in procedures

As in many other Windows-based applications, in CallPilot you can execute a command in several ways. For example, to copy text you can choose any of the following methods:

- Select Copy from the Edit menu.
- Click the Copy button on the toolbar.
- Type the keyboard shortcut Control + C.

The procedures in this guide use only the first method: selecting a command from a menu.

Navigation information in procedures

A **Getting there** statement precedes each procedure in this guide. This statement summarizes the steps you must take to navigate to the window or tab where you carry out the procedure.

All **Getting there** statements start at the Nortel System Management Interface (SMI) window. This assmues that you logged on and selected the appropriate system. Eac item mentioned after the Nortel SMI window represents an icon, window or tab that makes up the path to the final destination.

Example

To define special mailboxes, such as the broadcast mailbox, you must be on the Mailboxes tab.

Getting there Nortel SMI > Meridian Application Server > CallPilot > Message Administration

After you double-click Messaging Administration, the Message Administration Properties sheet displays. Click the Mailboxes tab.

Finding your way around CallPilot

In this section

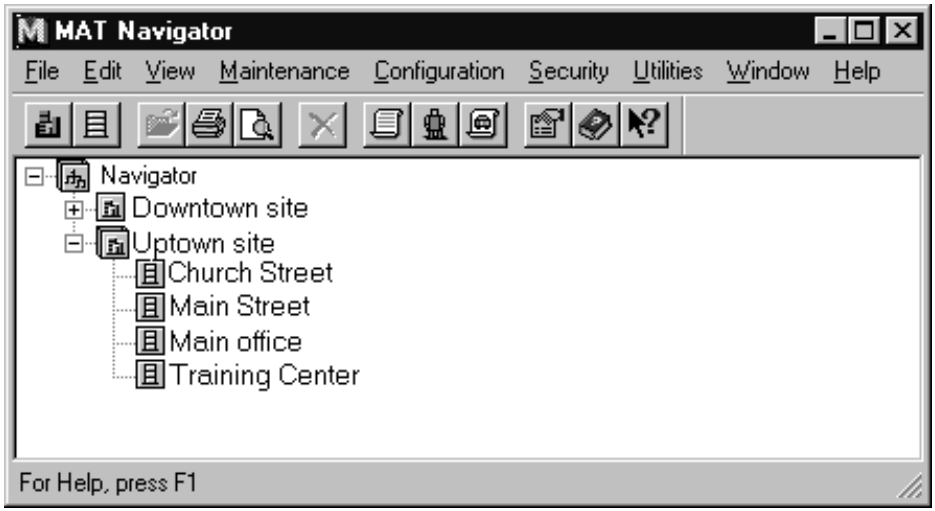
Connecting to CallPilot

Introduction

To perform administrative tasks, or to build or work with CallPilot applications, you must first connect to the Meridian Application Server (the MAS server). The MAT Navigator and the System Management Interface (SMI) work together to give you access to your system and sites.

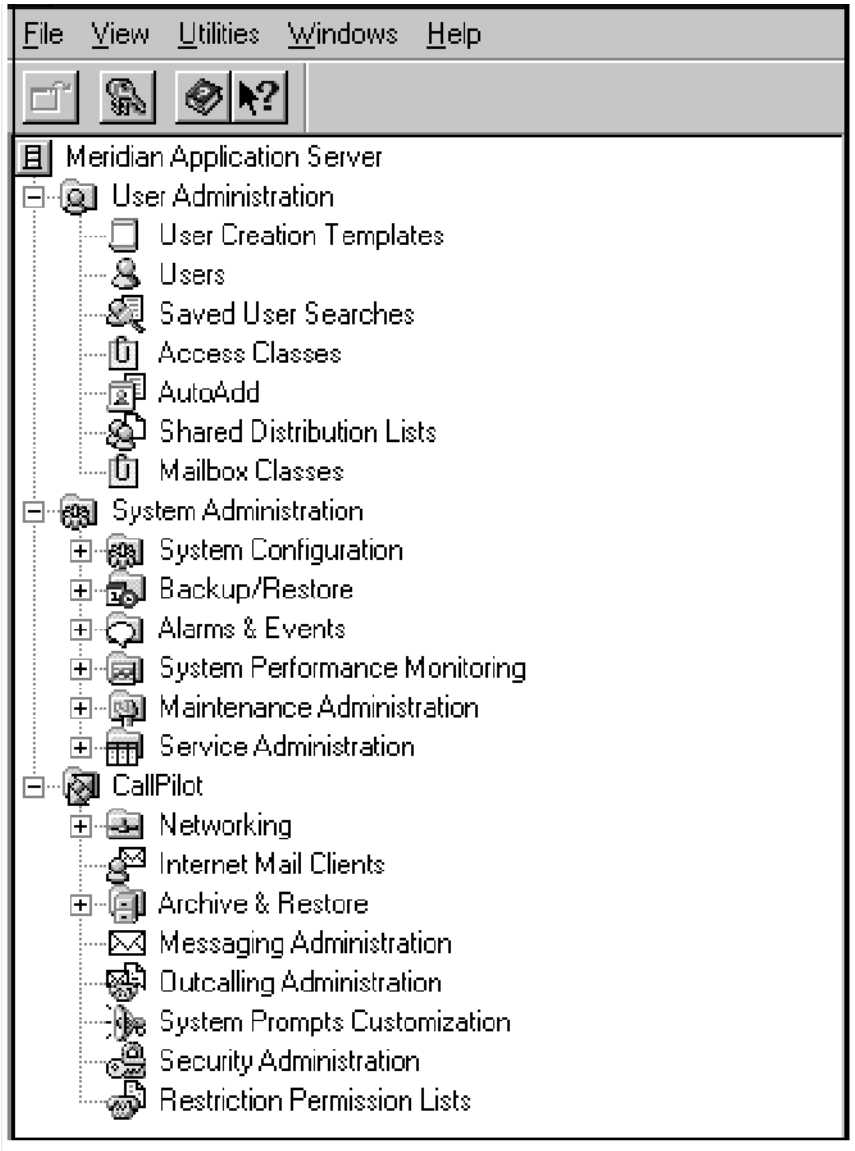
Selecting a system-the MAT Navigator

The first step in logging in is to launch the MAT Navigator, which has its own password. The MAT Navigator connects your administration client to the MAS server. It displays all your sites and systems and enables you to select one to work on.



Selecting a program—the System Management Interface (SMI)

When you select a system from the MAT Navigator, you are prompted for a second password. At this point, the SMI window for the selected system or site displays.



The SMI gives you quick and easy access to your system or sites. The SMI uses a navigation tree to display the system's hierarchy. In the tree, icons represent the folders and programs. Double-click a folder icon to view its contents. Folders can contain programs and other folders. Double-click a program icon to run the associated program.

Selecting an object-list views

When you launch certain programs, the first thing you see is a list view. The list view displays all the objects of a certain type (such as mailbox classes) that are currently defined in the system. The list view includes predefined objects as well as those defined by an administrator. From the list view window, you can select a specific object to work on.

Viewing and changing properties

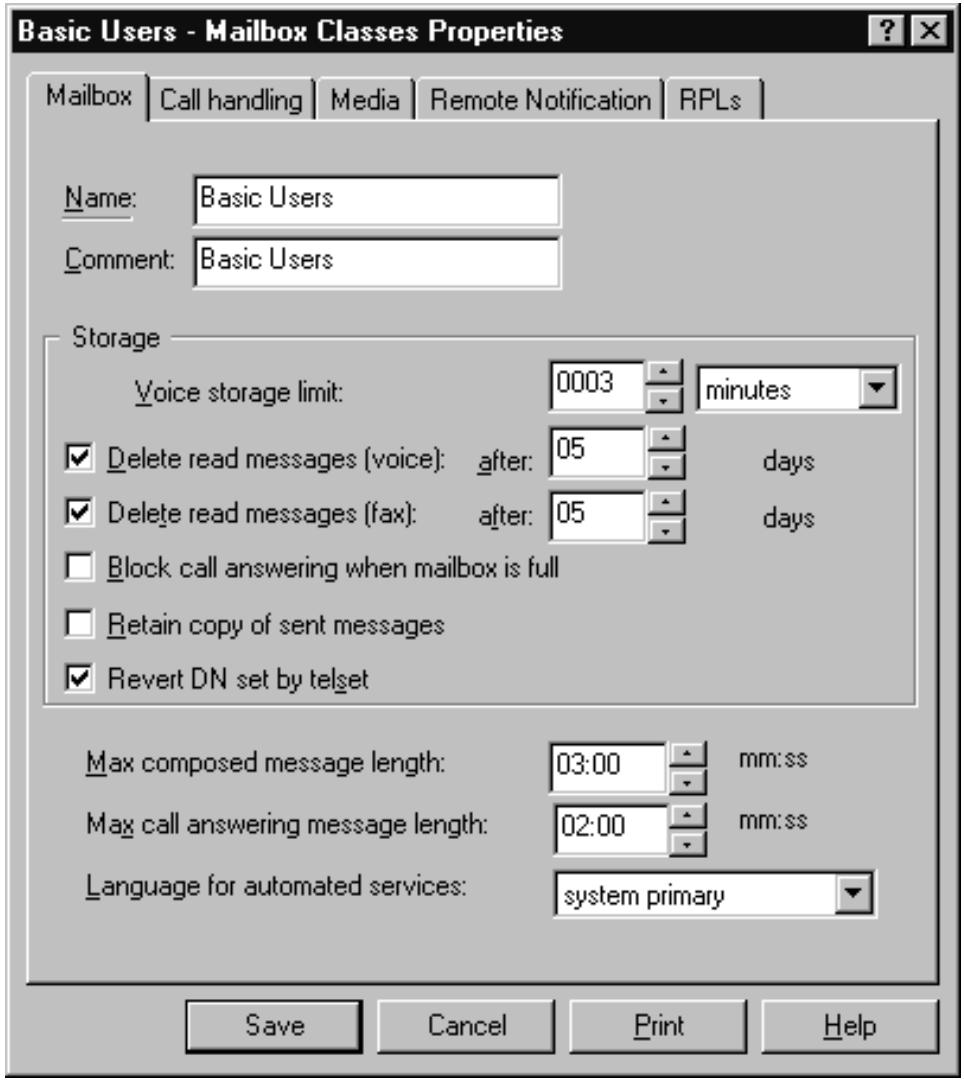
Select an object and display its properties by

- double-clicking it or
- single-clicking it and selecting Properties from the File menu
- right-clicking it and selecting Properties from the popup menu

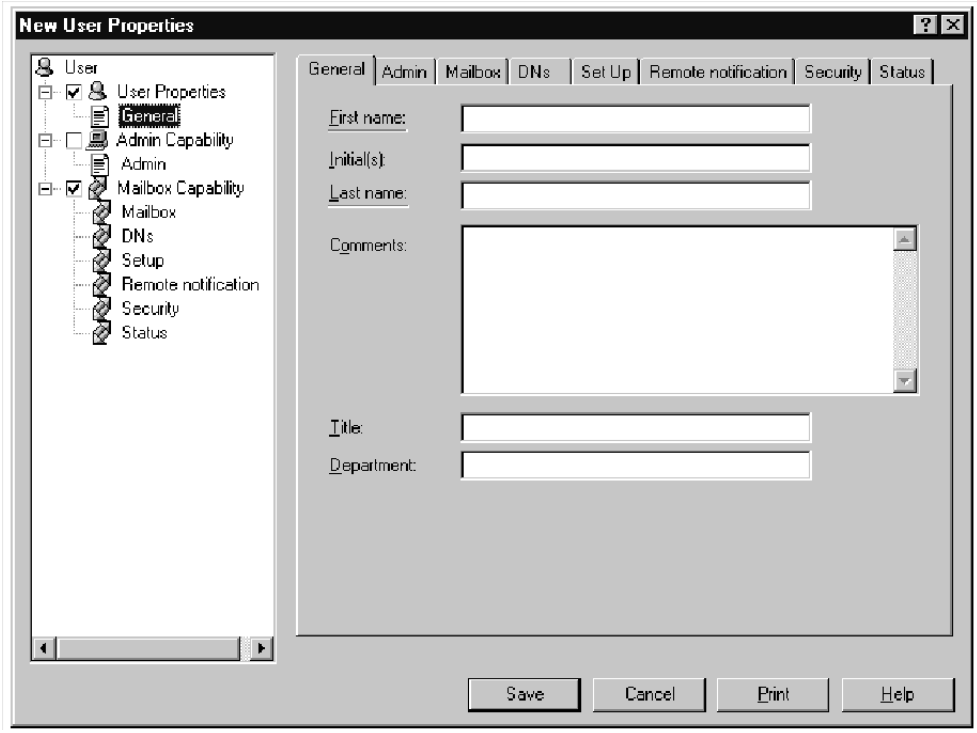
Entering data and choosing options-property sheets

A property sheet is displayed when you view an object selected from a list view. Certain programs, such as Messaging Administration, display a property sheet immediately after launching. Property sheets have one or more tabs. Each tab has fields, referred to as boxes, in which you can type data or from which you can select options.

Most CallPilot property sheets look like the following:



Some property sheets are divided into two panes. When a box is checked in the left pane, the selected capabilities are enabled and you can access the associated tabs. Select a tab by clicking its name in the left pane or by clicking the tab in the right pane. These property sheets look like this:



Mandatory boxes

If the name of a box is underlined, the box is mandatory, and you must fill it in. You cannot save if any mandatory boxes are empty.

Common buttons

The following buttons appear on most property sheets:

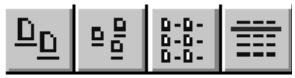
Button	Description
Save	Saves all changes made on any of the tabs in a property sheet and closes the property sheet. Therefore, save only when you have made the necessary changes on all tabs.
Cancel	Closes the property sheet without saving any changes.
Print	Prints the contents of all tabs in the property sheet.
Help	Displays Help for the current tab. From this overview Help topic, you can access other Help topics, the index, and the search function.

Using the toolbar buttons

For easier access, some of the more common tasks, such as Print and Save, are represented as buttons on the toolbar.

The following buttons are used throughout CallPilot. Buttons or icons specific to certain CallPilot functions, such as backups and archives, are documented in the relevant chapters.

Toolbar button	Description
	Saves any changes you have made and then transfers all the application's data to the server.
	Opens the Print dialog box and prints the active file or the objects you specify.
	Deletes the object you select.

Toolbar button	Description
	Displays the properties of the object you select.
	Displays the Help topics window.
 	Explains the next menu item or screen object you click. In a window, there is an arrow. On tabs or in dialog boxes, there is no arrow.
 	Opens the New dialog box, where you identify the properties of the object you are creating. The button looks different in different applications.
 	Displays the Open dialog box, where you select an object to open. The button is different in different applications.
	Reloads the current page and displays the changes you have made.
	Enables you to select how the system displays icons.

Multi-administrator access

Introduction

You can create multiple administrator accounts to make administering CallPilot easier and more efficient. Multiple accounts enable administration responsibilities to be distributed among a number of people. Therefore, certain administrators can specialize in certain tasks, such as maintaining users, performing backups, analyzing reports, or creating multimedia services.

Access classes

For security reasons, administrators should be given access only to those parts of the system that relate to their role. For example, an administrator who is responsible only for creating multimedia services should have access only to Application Builder and the Service Directory Number Table.

Each administrator account is assigned an access class. An access class is a list of the parts of the system and the level of access allowed. The access levels are as follows:

- create/delete (enables an administrator to delete objects such as users and services)
- edit
- view
- none

For example, an administrator may be able to create or delete objects in Application Builder but only view User Templates.

Simultaneous access

Multiple administrators can log in to CallPilot at the same time without overwriting other work.

If you are the first to log in to a particular resource, such as a specific mailbox class or user profile, and another administrator tries to access the same resource, a dialog box appears to inform you of the other administrator. At this point, you can do one of the following:

- Keep editing.
- Save your changes, and release the resource to the other administrator.
- Cancel your changes, and release the resource to the other administrator.

If you do not respond to this prompt within two minutes—because you are away from the terminal, for example—the system releases the resource so that others can access it. If this happens, all your unsaved changes are lost.

An administrator who accesses a resource that is currently being edited sees a read-only view of the property sheet in which all boxes are dimmed. This indicates that the resource is currently locked. The administrator is not notified when the resource is released, but must try to access the property sheet again to see whether its status has changed.

If a user tries to log on to a mailbox while an administrator is changing the profile, the user is unable to log on and receives a message that says the mailbox is in use.

Refreshing screens

Because multiple administrators can access the same database at the same time, a Refresh command is available from the View menu to ensure that the view you are seeing is the most up-to-date.

For example, if you are viewing a list of users when another administrator deletes a user, the only way to see the change is to refresh the screen. You should, therefore, refresh the screen regularly.

Error handling in property sheets

Introduction

If you make certain types of errors while entering data, you are not able to save your changes until you correct the errors. For example, if you leave a mandatory box empty, you receive a message prompting you to fix it.

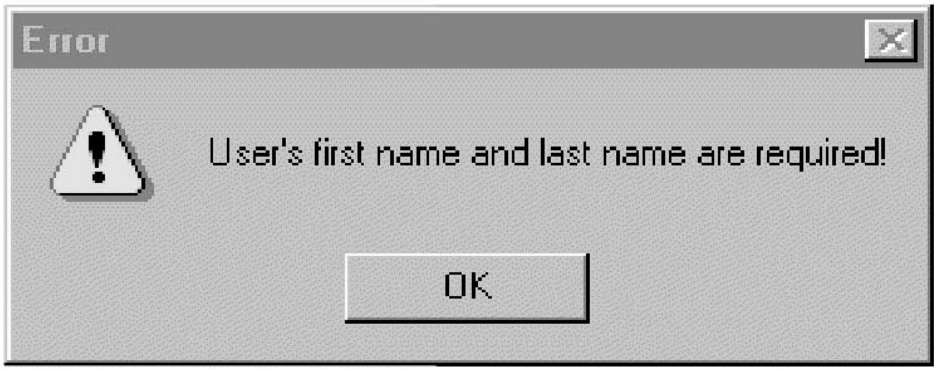
Note: These errors do not show up in the Event Browser or Alarm Monitor because the errors relate only to data entry and are not operational problems.

How error handling works

There are two types of error messages.

Type 1

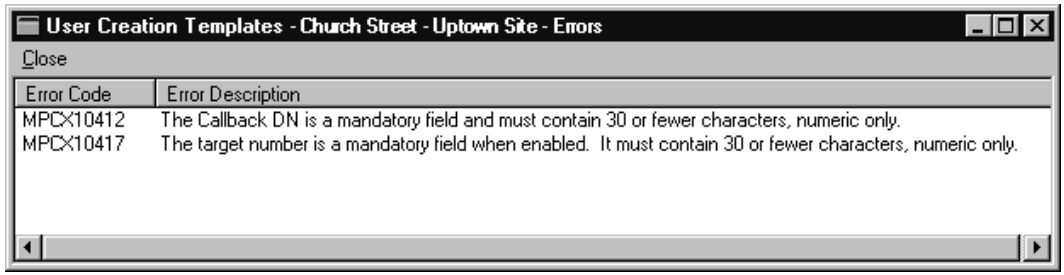
If you get this type of error message, click OK, and then fix the problem described in the message before you try to save again.



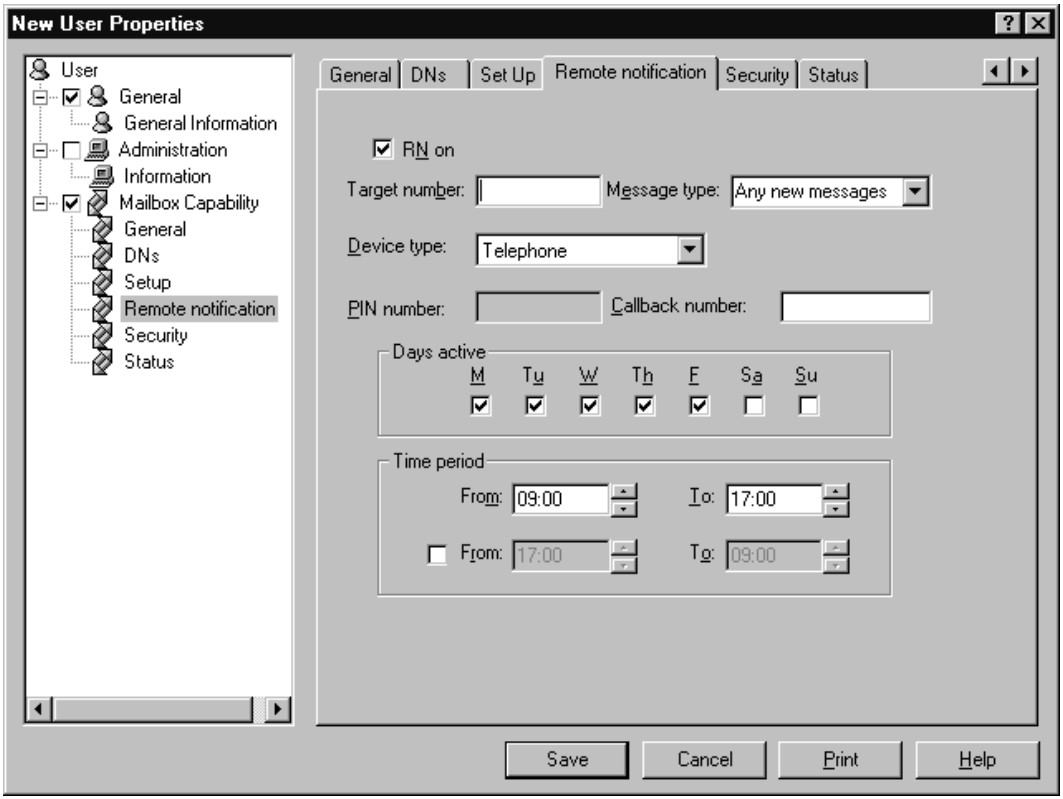
Type 2

If you get this type of error message, click OK to see a list of errors.

Double-click an error from the list. Your cursor is automatically placed in the box where the error was made so that you can correct it.



For example, if you double-click the second error, the Remote notification tab is displayed, with the cursor in the Target number box.



Using the online Help

Introduction

While administering or maintaining CallPilot, you may have questions about the purpose of certain boxes and buttons, or need more information about completing certain tasks. Online Help provides brief answers to the questions "What's this?" and "How do I...?"

Context-sensitive Help

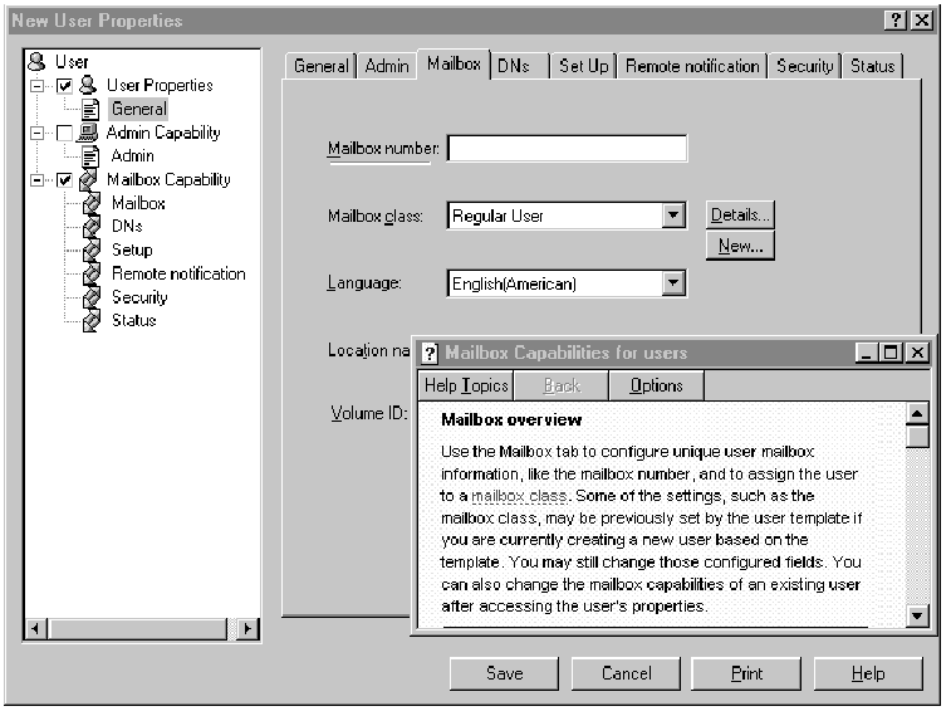
If you need to know the purpose of a particular box or button, use context-sensitive Help.

To access context-sensitive Help

1 Click the  icon in a window or the  icon on a tab or in a dialog box.

2 Point to the box or button for which you want more information, and click.

Result: A pop-up description of the selected object is displayed.



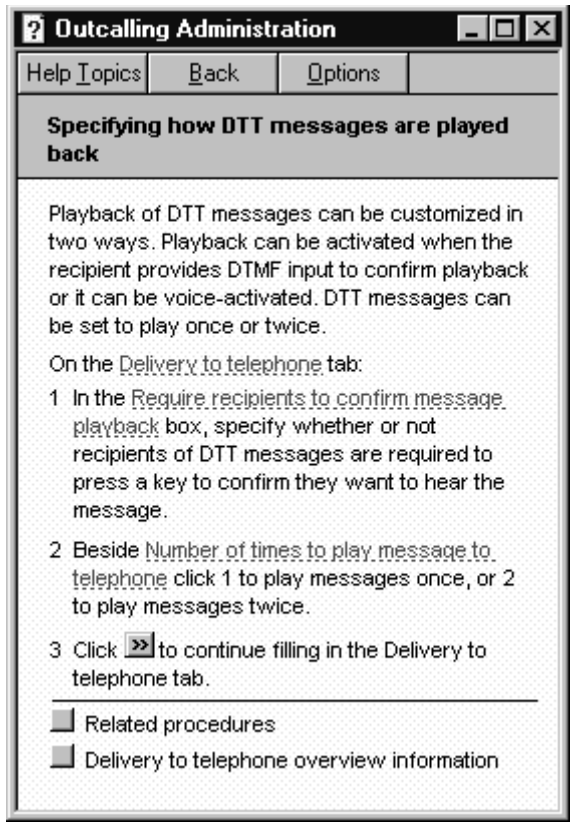
Procedures

If you need to know how to do something, you can access procedures to lead you through a task.

High-level tasks

In some cases, high-level tasks take you through longer procedures. These tasks also provide you with navigation to the step-by-step procedures they include.

For example, setting up Delivery to Telephone requires several procedures. The high-level task summarizes these procedures. You click the gray buttons within the task to open the step-by-step procedures. The high-level task remains on your screen so that you can continue to use it to move through the procedures.



Overview topics

Overview topics provide brief descriptions of tabs, features, and the tasks carried out from the tabs. However, the online guides contain more detailed feature descriptions.

To access overview topics

Click the Help button on a tab.

To find information in Help

You can look up procedures and overview topics in the following ways:

1 From the Help menu, select Help Topics.

Note: You can also press F1 on the keyboard.

2 Go to one of the following tabs:

- To see the table of contents of all the Help topics, select the Contents tab.
- To look up a subject alphabetically, select the Index tab.
- To do a full-text search to find topics that contain the words you enter, select the Find tab.

chapter 2

Getting started

VPIM Networking is one of the networking solutions offered by CallPilot. This chapter introduces VPIM Networking. It covers basic concepts and terminology that are useful for understanding VPIM Networking.

This chapter also provides a basic overview of the VPIM Networking implementation process.

In this chapter

About VPIM Networking

In this section

Overview

Introduction

VPIM Networking is one of the networking solutions offered by CallPilot.

You must be familiar with the basic concepts of messaging networks, data networks, and protocols. To review these concepts, consult the *Networking Planning Guide*.

Definition: VPIM Networking

VPIM Networking offers the ability to exchange voice, fax, and text messages with other users over a Transport Control Protocol/Internet Protocol (TCP/IP) data network.

Messages can be exchanged with users at integrated sites, which are part of your private messaging network, as well as with users who are at open, VPIM-compliant sites.

Standard

VPIM Networking uses Simple Message Transfer Protocol (SMTP) and Multipurpose Internet Mail Extensions (MIME) in compliance with the Voice Profile for Internet Mail (VPIM) standard.

Data networks

VPIM Networking uses existing data networks, not switch networks, to transport messages. The data network must support the TCP/IP protocol.

There are too many possible data network setups to be documented here. Therefore, this guide provides an overview of some of the most common setups. Working with your data network administrator, you will be able to determine how VPIM Networking is implemented on the existing data network.

Note, however, that VPIM Networking may require minor modifications to the existing configuration of the data network.

ATTENTION!

VPIM Networking is an incremental implementation on your existing data network. This guide assumes that you will work closely with the administrator of your data network to implement VPIM Networking.

Messaging to open sites

The ability to exchange messages with open sites is inherent in VPIM Networking. That is, if you have VPIM Networking implemented on your local site, local users can exchange messages not only with other sites within the private messaging network, but also with users at open sites.

Key terms

The following terms are used throughout this guide:

Term	Definition
Open	■ Not defined in the network database ■ Not part of the private messaging network, in most cases
Integrated	■ Defined in the network database ■ Part of the private messaging network
Data network administrator	■ Individual responsible for implementing and maintaining the data network at the local site

Intranets and the Internet

Introduction

An organization can exchange messages exclusively over an intranet, or the Internet, or a combination of the two. The way an organization exchanges messages determines how VPIM Networking is implemented.

Definition: Internet

The Internet is a global web of interconnected computer network—a network of networks. It provides the basis for global electronic mail (e-mail) and information exchange over the World Wide Web, as well as other services.

Definition: Intranet

An intranet is an internal, private data network. It is accessible only to authorized internal users.

Intranets are usually connected to the Internet.

The Internet consists of a number of local networks and intranets that are interconnected with gateways. These gateways sometimes have physical connections or ports that provide access to networks.

The purpose of a gateway is to accept all traffic that is intended for a specific destination and to pass along, or route, any traffic that is not intended for that destination.

How VPIM Networking works

Introduction

This basic overview provides some of the conceptual information you need for implementation. This overview also provides detailed information necessary to understand VPIM shortcuts.

VPIM address

A VPIM address is the address format used by VPIM Networking. A VPIM address is similar in form to an e-mail address.

For example, to send an e-mail message to a user over the Internet, you enter a two-part address. The left-hand side of the address contains a unique identifier for the user, often the user's name. The right-hand side of the address is the domain name of the user, the system on the data network that handles messages. For example:

- username@company.com

VPIM addresses also have two parts. However, the left-hand side usually contains the user's public switch telephone network (PSTN) number. The right-hand side is the domain name. For example:

- 14165977070@company.com

VPIM address restrictions

Some restrictions apply to VPIM addresses.

Left-hand side

- can contain numeric characters only
- maximum length of 128 characters

Right-hand side

- is case-sensitive
- maximum length of 255 characters

Note: The VPIM specification allows for different forms on the left-hand side of a VPIM address, including alphabetic characters, but numeric characters are recommended. However, VPIM Networking requires numeric characters on the left-hand side.

The VPIM specification allows for alphanumeric characters on the right-hand side. CallPilot supports alphanumeric characters on the right-hand side.

VPIM message

A VPIM message consists of two parts:

- a message header
- a message body that consists of voice, fax, and text parts
  - all message parts are MIME-encoded

Encoding parts

VPIM voice messaging parts are encoded using the ITU's G.726 32 kbps ADPCM standard.

VPIM text parts are not encoded.

VPIM fax messaging parts are encoded based on the tagged image file format-Class F (TIFF-F) specification.

Note: A fax must be in TIFF-F. When saving faxes, be aware of subtypes (there are many besides Class F). Not all subtypes are fax-compatible. All TIFF files, no matter what the subtype is, have a TIF extension.

Message header

VPIM Networking messages are addressed with the following format: left-hand_side@right-hand_side. This format is used by CallPilot for both the To: and From: entries of a message header.

For example, the To: and From: entries in a typical VPIM Networking message header might be

- To: 12046679000@anothercompany.com
- From: 15739921000@thiscompany.com

This header information is critical to VPIM Networking, because the header is used to route a message to its destination and to identify the sender.

CallPilot creates the complete To: and From: entries for users. This is convenient for telephone users, who don't have to enter the complete, long VPIM address. It is also a way of ensuring the accuracy of the address information.

Desktop and telephone users

VPIM Networking is available to both desktop users and telephone users.

Using a keyboard, a desktop user can easily enter the alphanumeric VPIM addresses, including the alphanumeric right-hand side for open VPIM sites.

However, a telephone user cannot enter the alphanumeric right-hand side of a VPIM address using the telephone keypad and is restricted to numeric addresses. Therefore, CallPilot offers alternative ways for telephone users to address VPIM Networking messages, one for messages to integrated sites and one for messages to open sites.

Telephone users are, however, still limited to a numeric left-hand side. Telephone users can hear the alphanumeric right-hand side.

Note: The distinction between desktop users and telephone users is important in this guide. When using VPIM Networking, some actions are available only to desktop users or to telephone users. Some configuration steps apply only to one type of user or the other.

Whenever specified, note the distinction between desktop user and telephone user. When the term *user* appears in this guide, there is no distinction between the desktop user and the telephone user.

Send VPIM Networking messages to other sites

Introduction

VPIM Networking supports the exchange of messages with both open sites and integrated sites.

Definition: Open site

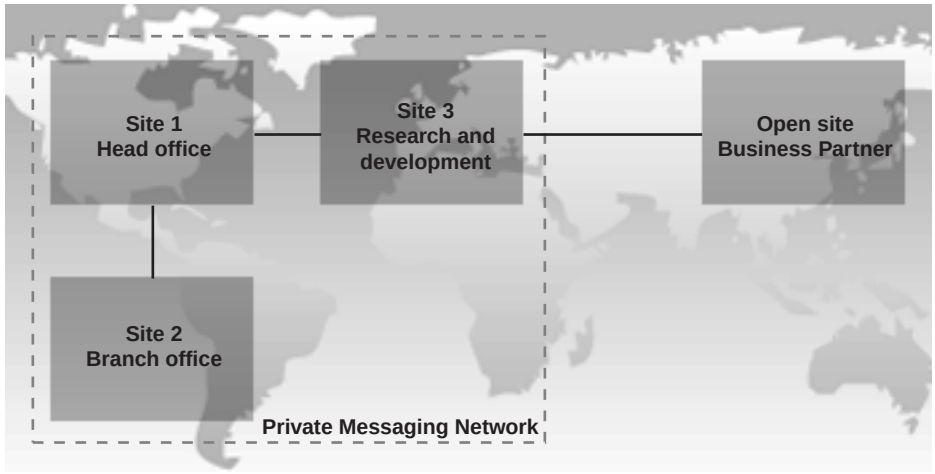
An open site is usually not part of the private messaging network. It can be any VPIM-compliant system.

Definition: Integrated site

An integrated site is part of the private messaging network and is defined in the network database.

Example

In the following diagram, the private messaging network consists of three integrated sites. All three use VPIM Networking to exchange messages with one another. Site 3 is also configured so that telephone users can exchange messages with open sites over the Internet. Desktop users at all three sites can exchange messages with open sites without any special configuration.



G101150.e

Send messages to open and integrated sites

To understand how VPIM Networking works, you must be familiar with the basic differences between messages sent to open sites and those sent to integrated sites.

Open sites

Telephone users and desktop users have different ways of addressing messages to recipients at open sites.

Telephone users

If a telephone user wants to send a message to an open site, the open site must be defined in the local network database as an open VPIM shortcut. An open VPIM shortcut identifies the PSTN number of the open site to the domain name of the open site. An open VPIM shortcut is used to form outgoing VPIM addresses only.

For example, Gwendolyn Zwnatsky wants to compose and send a message to a user at an open site. She knows the recipient's VPIM address: 12044541000@bigcompany.com

To send a message to this open site using a telephone, the list of open VPIM shortcuts should include an entry such as the following:

- 1204454 = bigcompany.com

Gwendolyn gets the PSTN telephone number and the open shortcut from the network administrator. When Gwendolyn sends a message to this open site, she must enter 15 1204454 1000, where

- 15 is the VPIM compose prefix
- 1204454 is the VPIM open shortcut
  - 1 is the country code
  - 204 is the area code
  - 454 is the area/city code
- 1000 is the mailbox number

CallPilot uses this information to identify that the message is being sent with VPIM Networking. It finds the shortcut in the network database and maps it to a domain name. CallPilot creates the following To: header from this information:

- To: 12044541000@bigcompany.com

Desktop users

To send a message to an open site, a desktop user does not require an VPIM open shortcut to be defined in the network database.

A desktop user can address a message to any open site user without restriction and can use either a VPIM open shortcut or a VPIM address.

Integrated sites

Integrated sites are part of your private messaging network. Information about all integrated sites that exchange messages with your local site is defined in your local network database.

This information includes VPIM networking shortcuts. These shortcuts are the various ways that local users can address users at the remote site.

Distinction between open and network shortcuts

VPIM open shortcuts and SMTP/VPIM network shortcuts have very different roles. The open shortcuts provide the alphanumeric domain name required on the right-hand side of a VPIM address.

The network shortcuts provide alternative ways for local users to address messages to users at remote sites. Instead of always entering the left-hand side of the VPIM address, users can enter the same numbers that they use to dial that site. The right-hand side is supplied by the fully qualified domain name (FQDN) for the site contained in the network database.

Creating the From: header

When a local user sends a VPIM Networking message to an open or integrated site, the message header contains a From: entry.

The From: entry enables the recipient to reply to the sender.

The From: entry normally consists of the PSTN address and the domain name. For example:

- 14165979999@branch.thiscompany.com

The left-hand side of the address is created from the PSTN address for the local site. The right-hand side is the fully qualified domain name of the local site's mail server. This FQDN is defined in the local network database and is added to the outbound address automatically.

Receive VPIM Networking messages

Introduction

The way your local system receives inbound VPIM Networking messages depends on how your data network is set up and whether the messages are coming from the Internet or an intranet.

CallPilot continuously monitors TCP port 25 for incoming SMTP information.

If a message is received successfully

If a message is received successfully, the message and addresses are converted to their native format and the message is delivered to the local mailboxes.

If the message is not received successfully

If there is a problem during the message transfer session, the local system logs an event. The event log indicates the address of the sending system.

If the session is successful but the message is not delivered to a local mailbox, a non-delivery notification (NDN) is generated and sent to the message sender.

There are several reasons why a message might be successfully received but undeliverable to a local mailbox. For example, the mailbox does not exist.

Receive messages over the Internet

If VPIM Networking messages are sent over the Internet, a mail relay is probably used to receive all incoming messages destined for the VPIM system on an intranet.

The mail relay receives all incoming SMTP mail and redirects VPIM messages to the appropriate CallPilot server.

There are two ways for a mail server to identify the appropriate server:

- using mail exchange (MX) records in the domain name server (DNS)
- using the right-hand side FQDN of the To: address

VPIM Networking benefits

Introduction

VPIM Networking offers many benefits, including

- a cost-effective standard for exchanging messages over TCP/IP data networks
- wide vendor support
- substantial economic benefits over analog networking
  - no long-distance toll charges for messages
  - no competition with Call Answering and Voice Mail traffic for channel capacity

Feature highlights

VPIM Networking introduces several new features to CallPilot networking. It has the ability to do the following:

- Operate over standard TCP/IP networks (Internet/intranet).
- Make better use of existing data networks.
- Save long-distance toll charges for network messages by sending them over the Internet.
- Exchange messages with other third-party VPIM-compliant systems.
- Exchange messages with fax and text, as well as voice.
- Exchange messages with other Nortel VPIM-compliant systems: Norstar Voice Mail and Meridian Mail Net Gateway.

CallPilot and VPIM Networking

VPIM Networking features

The following table lists the CallPilot features that are supported by VPIM Networking:

CallPilot feature	Supported	Notes
Call Sender	Yes	To integrated sites only. Can be used for both call answering and composed messages from network users if ■ the calling line identification (CLID) is present in the message, or ■ the mailbox numbering plan follows the dialing plan, or ■ a remote user entry is added for the network user
Names Across the Network	No	This feature is currently not supported.
Name Addressing	Yes	
Personal Distribution Lists	Yes	
Shared Distribution Lists	Yes	
Multiple Recipients	Yes	Recipients to non-VPIM sites are not included in the VPIM message.
Reply To Sender	Yes	
Reply All	Yes	
User's Actual Personal Verification	No	
Administrator-Recorded Personal Verification	Yes	

CallPilot feature	Supported	Notes
Remote Site Spoken Names	Yes	To integrated VPIM sites only.
Private Tag	Yes	Messages tagged as private are announced to the recipient. A message tagged as private may be forwarded.
Acknowledgment Tag	Yes	Acknowledgment tags result in a message to the sender indicating that the message was actually listened to.
Urgent Tag	Yes	Messages tagged as urgent trigger urgent-related features, such as Remote Notification or Message Waiting Indication. Urgent messages are given priority for transmission as determined by the scheduling parameters.
Economy Tag	Yes	Messages tagged as economy are sent with a “low” importance information tag.
Received Time Announced	Yes	A certified tagged message is acknowledged when the message is read, not received.
Sent Time Announced	Yes	Sent time is converted to the recipient’s local time zone and is expressed in local time.
120-Minute Messages	Yes	Length is restricted only by memory available on the mail server.
Sender’s Name (Text)	Yes	Only supported if American English character set (ASCII 32-126).
Recipient’s Name (Text)	Yes	Only supported if American English character set (ASCII 32-126).
Message Subject (Text)	Yes	Only supported if American English character set (ASCII 32-126).

CallPilot feature	Supported	Notes
Sender's Department	No	
Timed Delivery	Yes	

Non-delivery notifications

A non-delivery notification (NDN) is generated if an error occurs during an attempt to deliver a message. There are three types of non-delivery notifications:

- local: generated by the local sending system
- network: generated by the remote receiving system
- intermediate: generated by systems involved in routing message

Note: If VPIM Networking messages are sent over the Internet, there is no guarantee of when users receive non-delivery notifications. Internet servers may take up to several days before sending a non-delivery notification.

Free-form text non-delivery notifications

The non-delivery notifications for VPIM messages are actually generated by the delivery status notification (DSN) facility of mail relays and proxies. Most mail relays and proxies generate the correct DSN, which results in a properly formatted non-delivery notification.

However, some older mail relays and proxies generate incorrect DSNs. These result in NDNs that are free-form text messages.

Although formatted differently from the standard non-delivery notification, a free-form text non-delivery notification can be read and understood by desktop users.

If a user has a voice-only mailbox, the user never receives a free-form text non-delivery notification and receives no notification at all.

Multimedia messages and non-delivery notifications

If a multimedia message is sent to a user who does not have the mailbox capabilities to accept one or more parts of the message, the entire message is rejected.

For example, if a voice message with a text attachment is sent to a user with a voice mailbox only, the entire message is rejected and the sender receives a non-delivery notification.

Message delivery notification

A message delivery notification (MDN) is generated if a user requests one before sending a message. This request is made by tagging the message for acknowledgment. With VPIM Networking, a message delivery notification indicates that the recipient has opened at least one part of a message.

The following must also be considered:

- The receiving system may be configured to not send message delivery notifications. If so, local users cannot tell if their messages were never delivered or never read by recipients on the receiving system.
- Meridian Mail Net Gateway does not support message delivery notifications. Local users cannot tell if a recipient at a Net Gateway site read the message.

Although CallPilot supports message delivery notification, even messages exchanged between two CallPilot systems may not be entirely supported. For example, if a message is routed through any system that does not support message delivery notifications, the message delivery notifications are lost.

OM reports

Operational Measurement (OM) reports for cumulative network activity to a particular site are available for VPIM Networking.

OM reports for individual messages are not generated for VPIM Networking. Since VPIM messages do not incur long-distance toll charges, it is not necessary to track each message for the purposes of bill-back.

See also

For detailed information about CallPilot features consult the *Advanced Administration Guide*.

VPIM Networking connectivity

Connectivity

Because it uses an industry-standard protocol, VPIM Networking can connect to many other systems, including

- other CallPilot systems (Release 1 or later)
- Norstar Voice Mail (Release 3 or later)
- Meridian Mail systems (Release 11 or later) through Meridian Mail Net Gateway (Release 1 or later) (which acts as an IP-to-circuit-switched network gateway)
- VPIM-compliant systems from other vendors

Connectivity with open and integrated sites

These systems can be included in the local VPIM Networking database as integrated remote sites.

If these systems are not integrated, local users can still send messages to them as open sites.

VPIM-compliant systems from other vendors

To determine if a messaging system from another vendor is VPIM-compliant, refer to the system's documentation.

All VPIM-compliant systems can exchange messages with VPIM Networking.

Restrictions

Although VPIM Networking exchanges messages with these systems, there are some important restrictions to consider when setting up VPIM Networking.

Meridian Mail Net Gateway

Meridian Mail Net Gateway takes Meridian Mail messages sent using the Enterprise protocol, an analog protocol, and converts them into a digital protocol so that they can be sent across an IP network.

Messages exchanged between a site using VPIM Networking and a site using Net Gateway can contain only voice components, not text or fax.

Third-party systems

Although VPIM Networking uses the industry-standard VPIM protocol and can exchange messages with third-party systems from other vendors, there may be special restrictions.

Consult the documentation of the third-party system to determine if there are any special configuration considerations or any restrictions in functionality. Confirm the capabilities enabled at a third-party site.

See also

For a review of VPIM conformance specifications, consult AppendixA, “VPIM conformance”.

VPIM Networking and other networking solutions

CallPilot networking solutions

CallPilot offers several networking solutions, enabling you to create a network that is best suited to your needs.

VPIM Networking can be implemented in a network that uses a variety of messaging solutions and protocols for communication.

Multimedia support

VPIM Networking offers the fullest support for different media in the message body parts.

Networking solution	Voice only	Fax only	Voice and fax	Voice, fax, and text
Enterprise Networking	Yes	No	No	No
AMIS Networking	Yes	No	No	No
VPIM Networking	Yes	Yes	Transmits all voice and fax message body parts	Transmits all voice, fax, and text message body parts

Comparison with Enterprise Networking

Almost all CallPilot messaging features that are available with Enterprise Networking are also available with VPIM Networking.

Currently, the only feature offered by Enterprise Networking that is not available with VPIM Networking is Names Across the Network, which enables the automatic creation of temporary remote users.

Comparison with AMIS Networking

Like AMIS Networking, VPIM Networking enables you to extend your messaging network beyond your private network. Both networking solutions use industry-standard protocols. They are designed to work with all other messaging systems, regardless of vendor, as long as the systems use the same protocol.

Like AMIS Networking, VPIM Networking supports exchanging messages with integrated remote sites and open remote sites.

The following table compares VPIM Networking and AMIS Networking:

VPIM Networking	AMIS Networking
Incurs Internet/intranet toll rates	Incurs standard PSTN toll rates
Uses digital file transfer	Uses audio playback
Unaffected by line	Is susceptible to noise
Uses LAN port	Uses voice ports
Supports voice messages	Supports voice messages
Supports fax messages	Does not support fax messages
Supports text messages	Does not support text messages
Supports urgent message tags	Offers partial support for urgent message tags
Supports certified message tags	Offers partial support for certified message tags
Supports private message tags	Does not support private message tags
Sends messages to open sites	Sends messages to open sites

Data networks

In this section

Data network setup

Introduction

How VPIM Networking works and how it must be configured depends, in part, on how the data network is set up.

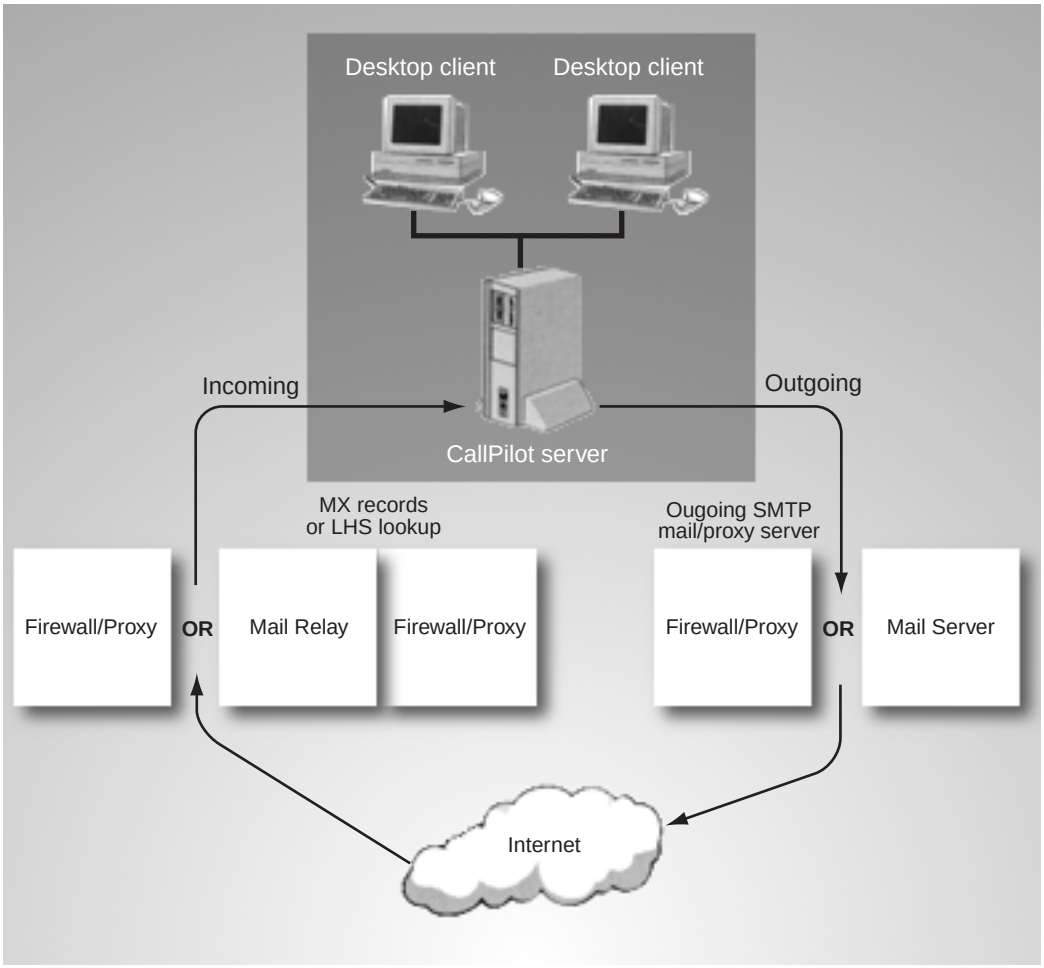
There is no single setup for data networks. Therefore, you must work with the data network administrator to understand how VPIM Networking should be implemented.

Connected to Internet

If your data network is connected to the Internet, there are many possible hardware and software setups.

In most instances, incoming VPIM Networking messages pass through a firewall, which helps to protect the security of your network. Messages that are allowed through the firewall are passed to a mail relay or a proxy server.

Outgoing VPIM Networking messages are sent either to a mail server or to a proxy server. Outgoing messages usually pass through a firewall before entering the Internet.



G101161.eps

Within an intranet

If your organization sends messages over an intranet and is not connected to the Internet, there are different configurations for the data network.

The Internet and intranets

Most data networks are configured to use a combination of the Internet and intranets. Combinations are supported by VPIM Networking.

Message treatment

Introduction

VPIM Networking treats incoming and outgoing messages in different ways.

Note: This section describes some of the inner workings of the SMTP/VPIM data network and their relationship to VPIM Networking. This section may be most relevant to the data network administrator.

Incoming messages

How CallPilot treats an incoming VPIM Networking message depends on the system configuration. The following examples explain how an incoming message is treated when it comes from an intranet and when it comes from the Internet.

Intranet

When an incoming message comes from an intranet, there is a direct SMTP/VPIM connection between two systems.

The system continuously monitors TCP port 25 for an incoming SMTP/VPIM message. When the system detects an incoming message, it uses the SMTP protocol to receive the message, including recipient information.

If the message is received successfully, the message is converted into the native CallPilot format. The address is converted to native representation and is delivered to the local mailbox of the recipient.

If an error occurs during the session, the receiving system logs an event that includes the address of the sending system. The sending system generally retries sending the message several times.

If the delivery to a local mailbox fails for any reason, such as the mailbox does not support the fax content contained in the message, a non-delivery notification is generated and sent to the sender.

Internet

When an incoming message comes from the Internet, a mail relay may be used to receive all incoming SMTP mail and to redirect the message to the appropriate CallPilot server. There are two ways to indicate the appropriate CallPilot server to the mail relay:

- **DNS MX record lookup** The CallPilot server must be configured as the least preferred MX record in the DNS server.
- **Left-hand side (LHS) resolution** Using the left-hand side of the SMTP message recipient address, the mail server redirects the message to the appropriate CallPilot system, which hosts the mailbox of the recipient.

  Example: Using the appropriate database or table lookup, the mail server maps the left-hand side, 14165551234, from the address 14165551234@acme.com to an internal host, pixie.acme.com.

Relationship of the server FQDN to VPIM shortcuts

There are two possible origins of an inbound message:

- an integrated site that is part of your messaging network
- an implicit open site, which is not part of your messaging network but is known and is listed in the open VPIM shortcuts, or an unknown open site, which is not part of your messaging network and is not included in the open VPIM shortcuts. To CallPilot, these are indistinguishable.

Message from an integrated site

The following examples are based on this message:

- From: 16135558877@chilly.org
- To: 14165551234@realcool.org

If the sender of the message is located at an integrated site in your messaging network, the sender is presented as an integrated site to the recipient.

This assumes that when VPIM Networking was implemented at the receiving site (realcool), the following were configured for the remote site (chilly):

- server location: Chilly Branch Office
- server FQDN: chilly.org
- VPIM shortcut: 1613555 (overlap: 0)

The left-hand side of the incoming message is matched against the VPIM shortcut. This identifies the message sender as a user at Chilly Branch Office.

The address is converted to an internal format designating the remote site and the sender's mailbox number (8877). For example, using a telephone to retrieve the message, the recipient hears an announcement similar to the following: "Message 1 from Mailbox 8877 at Chilly Branch Office."

Similarly, a user at realcool can compose to a chilly recipient by using the dialing plan format as configured in the messaging network configuration. For example, a user enters 63318877, where 633 is the ESN prefix for the chilly site. The message is sent to 16135558877@chilly.org using the network configuration information for the site to make up the address.

Message from an implicit open site

An implicit open site is one that is known and is included in the list of open VPIM shortcuts.

In this example, the open VPIM shortcut list includes the following entry:

- VPIM shortcut: 1613555
- FQDN: chilly.org

The address is converted to an internal format. For example, when using a telephone to retrieve the message, the recipient hears an announcement similar to the following: "Message 1, from 16135558877 at open network location chilly.org." The address is spelled out in full ("c-h-i-l-l-y dot o-r-g").

Message from an unknown open site

When an incoming message is from an unknown open site, nothing in your site configuration identifies the source.

Reply features and VPIM addresses

When a user receives a VPIM message from an open site, the Reply To and Reply All features can be used. The system handles the reply and the user does not enter an address manually. Therefore, an alphanumeric VPIM address does not affect the Reply features.

Outgoing messages

VPIM Networking handles outgoing messages according to their intended destination.

The following is an outline of the treatment of an outgoing message:

- The user composes a message using either a telephone or a desktop.
- The user enters the address of the recipient, either a VPIM open shortcut or a VPIM network address.
- CallPilot converts the message from the native CallPilot format to MIME format.
- The user's From: address in the MIME format is created using
  - a VPIM shortcut of the sender's location
  - the sender's mailbox
  - the local server FQDN
- If the message is addressed to an integrated recipient, the recipient's address is created using
  - the VPIM shortcut of the recipient's location
  - the recipient's mailbox
  - the FQDN of the server on which the recipient resides
- If the message is addressed to an open recipient, the recipient's address is stored in the native message in the correct format (for example, 124165971234@open_site.com) and is copied into the MIME format message.
- The message is sent from the local system to the destination. If the message is sent to more than one destination, the message is sent once for each remote server. The message is sent using one of the following:
  - by direct connection
  - by mail server (using an MX record)
  - by the outgoing SMTP/mail proxy server

Outgoing mail and proxy servers

The outgoing SMTP/mail proxy server only deals with outbound messages. The system first attempts to resolve the FQDN in the To: header locally. If the system locates the intended mail system locally (for example, in the DNS table), it delivers the message.

If the To: header is not resolved locally, the system assumes that the address is an Internet address and sends the message to the proxy server. The proxy server takes responsibility for routing the message to the Internet.

Outgoing mail and gateways

A message that is leaving the local site can pass through a gateway. The gateway may alter parts of the address to protect internal server names.

For example, a gateway can convert serv1.ca.company.com to company.com.

TCP/IP

Introduction

VPIM Networking uses the Transport Control Protocol/Internet Protocol (TCP/IP). Only TCP/IP data networks are supported.

The CallPilot server, on which VPIM Networking resides, is connected directly to your existing TCP/IP data network.

Definition: TCP/IP

TCP/IP is the most commonly used transport for data networks. TCP/IP is a driver that enables computers to communicate with one another regardless of their platforms. This standard is used globally.

The connections that form the basis of the Internet are based on TCP/IP.

Definition: TCP

Transport Control Protocol (TCP) is the transport layer of TCP/IP. It ensures that the information transmission is both reliable and verifiable.

TCP breaks the information into smaller portions. Each portion receives a header, which is used to route the packet to its proper destination. A portion of data and its header are know as a packet or a datagram.

TCP passes the packet, with its header, to the IP protocol, which routes the packet to the correct destination.

Definition: IP

Internet Protocol (IP) is the network layer of TCP/IP. It ensures that the information is transmitted from its source to its destination.

To transmit the packets created by TCP, IP routes them.

When IP receives packets from TCP, IP adds another header to the packets.

TCP/IP routing

Routing in a TCP/IP data network relies on IP addresses.

IP addresses

Each computer on a TCP/IP network is identified by its address. The source and destination addresses used by IP have a specific format.

An IP address is a 32-bit number represented by a four-part decimal number (n.n.n.n). Each part, known as an octet, contains 8 bits of the address. Each octet has an assigned number between 1 and 254.

Example: 45.211.100.58

Subnetting an IP address

For many organizations, one physical network is impractical, so they have two or more physical networks. Instead of getting additional IP addresses for each physical network, the networks are assigned subdivided portions of the original IP address. This is called subnetting an IP address.

Subnetting provides many advantages. One of the most important is that, to the outside world, the organization has a single IP address.

This means there is one direct connection to the Internet. All subnetted physical networks gain access to the Internet through this connection.

Fully qualified domain names

An IP address is difficult to remember and enter. While the computers on the TCP/IP network use IP addresses, end-users use fully qualified domain names (FQDNs).

A fully qualified domain name is made up of two parts:

- domain name
- host name

Domain name

A domain name is interpreted from right to left. For example, in the domain name acme.com, .com is the top-level domain for commercial sites, and acme is a domain within the .com domain.

Host name

A domain contains many computers. Each computer in a domain is a host with a name.

A fully qualified domain name (FQDN) combines the name of a host, a dot, and the domain name. For example, test.example.com.

Domain name system

The domain name system (DNS) is a naming protocol used with the TCP/IP protocol. It enables the use of names, instead of IP addresses, to route messages. The DNS provides a domain name to IP address mapping, or translation.

This mapping takes place on a name server, frequently called the domain name system (DNS) server.

A network of DNS servers works cooperatively. If one DNS server does not know how to translate a particular domain name, it passes the name on to another DNS server.

Need for DNS server

To communicate over the Internet, every physical network requires a DNS server. Many organizations own and maintain their own DNS server. Other organizations, especially smaller ones, may rely on an Internet service provider (ISP) for a DNS server.

If you do not exchange messages over the Internet, but only over an intranet, your network may or may not include a DNS server.

DNS lookup tables

A DNS server contains a lookup table that translates FQDNs into IP addresses. This table is defined and maintained by the data network administrator. The table is also automatically propagated by the DNS server.

A DNS lookup table can store different types of records, including

- mail exchange records (MX records)
- address records (A records)

DNS servers and MX records

The DNS server contains many types of records, including mail exchange (MX) records.

MX records point to the mail servers that are configured to receive mail sent to the domain name. They describe where SMTP mail for the domain should be sent.

MX records are useful because they enable you to redirect mail for any host or domain to any other host or domain. This means that, while your organization might use many mail servers, all mail can be sent to the same domain name.

For example, all mail is sent to user@company.com, even though there is no host called company.com. The MX records redirect the mail to a system that accepts mail. This separation of mail delivery and physical hosts is an efficient way of ensuring that the addresses of all users in your organization are common and easy to remember.

Many data networks have more than one mail server. You can specify the order of preference. Mail is deposited at the first server in the list. If the mail is not intended for that server, it is passed to the next server.

Every host that receives mail should have an MX record. The MX record contains a preference value that is the order that a mail server should follow when attempting to deliver messages. The preference value provides some fault tolerance in your mail setup.

MX records and mail servers

If you want to use mail exchange servers within your domain, create specific MX records for each of the mail servers in your domain. If you use MX records, assign VPIM Networking the last, or least preferred, MX resource record in the list.

Your domain can have multiple MX records, such as the following:

- acme.com mail.acme.com MX 0 mail.acme.com
- acme.com mail2.acme.com MX 10 mail2.acme.com
- acme.com mail.is.net MX 100 mail3.acme.com

In this case, mail delivery is attempted to mail.acme.com first, because it has the lowest preference value. If delivery fails, mail delivery is attempted to mail2.acme.com.

MX records and user accounts

MX records provide routing for destination systems. They do not provide routing for individual user accounts. End-user routing may be provided by a mail server, for example.

DNS server setup

The DNS server should be properly set up and the database should be properly filled before you implement VPIM Networking. However, you will have to add one or more records to the database.

One record is for the server, which is entered as part of the CallPilot installation and is not specific to VPIM Networking.

As an option, you can add MX records if they are being used.

TCP/IP protocols

Introduction

VPIM Networking uses the TCP/IP protocol to exchange messages over data networks.

TCP/IP is actually a family of protocols that are often called application protocols. These application protocols are based on TCP/IP, but are specialized for particular purposes.

Industry-standard protocols

VPIM Networking uses the following TCP/IP application protocols:

- Simple Message Transfer Protocol (SMTP)
- Extended Simple Mail Transfer Protocol (ESMTP)
- Multipurpose Internet Mail Extensions (MIME)

SMTP, ESMTP, and MIME are industry-standard application protocols. A standard describes an interface between components of different vendors, which is fundamental to the concept of networking.

By using only industry-standard protocols for VPIM Networking, CallPilot offers universal compatibility and state-of-the-art technology.

SMTP and ESMTP

SMTP is a way to move e-mail from server to server on a TCP/IP network. Most e-mail systems that send mail over the Internet use SMTP to send messages. The messages are retrieved with an e-mail client using either Post Office Protocol (POP) or Internet Mail Access Protocol, version 4 (IMAP4).

In general, SMTP is also used to send messages from a mail client to a mail server. For this reason, when you configure an e-mail application, both the POP or IMAP server and the SMTP server must be specified.

ESMTP offers several enhancements to SMTP, including machine-readable non-delivery notifications.

MIME

Although TCP/IP is capable of 8-bit binary data transfer, SMTP allows for only 7-bit data transfer.

This means that, to be exchanged over a data network, voice, fax, and simple text messages must be encoded into a 7-bit representation and encapsulated into a format that can be broken into packets consisting of message headers and data.

This encoding and encapsulation is done by another application protocol, MIME.

Definition

The Multipurpose Internet Mail Extension (MIME) is a specification for formatting non-ASCII messages so that they can be transmitted over the Internet. MIME enables multimedia e-mail messages containing graphics, audio, video, and text to be sent. MIME also supports messages written in other character sets besides ASCII.

VPIM

VPIM is a profile that conforms to specifications.

VPIM Messaging uses the ESMTP/MIME application protocols in compliance with industry-standard specifications. These specifications are known collectively as VPIM.

Definition

VPIM is a new standard that provides detailed conformance rules for the use of Internet mail for voice mail messaging systems.

With the development of voice messaging, a class of special-purpose computers has evolved to provide voice messaging services. These computers generally interface to a telephone switch and provide call answering and voice messaging services.

Traditionally, messages sent to a computer at a remote site were transported using analog protocols based on dual-tone multifrequency (DTMF) signaling and analog voice playback. As the demand for networking increased, there was a need for a standard high-quality protocol to connect analog protocols. To

address this need, the VPIM Work Group of the Electronic Messaging Association (EMA) has developed the VPIM profile of the Internet standard MIME and ESMTP protocols for use as a digital voice messaging networking protocol.

Implications

Because VPIM is an industry standard, VPIM Networking can exchange messages with all VPIM-compliant systems from other vendors.

Nortel Networks and VPIM

Nortel Networks is playing a leading role in the development of VPIM. Nortel Networks chaired the VPIM Work Group of the Electronic Messaging Association (EMA), an inter-industry forum dedicated to developing secure messaging technologies.

RFCs

VPIM was turned over to the Internet Engineering Task Force (IETF) of the Network Information Center (NIC), which continues to produce a series of documents that contain protocol and model descriptions. All Internet-standard protocols are written up in these documents, known as Requests for Comments (RFCs).

VPIM Networking is designed to fulfil the requirements specified in RFC 2421 on VPIM Version 2 (September 1998).

VPIM compliance

RFC 2421 describes, in detail, how messages are formatted.

To be considered VPIM-compliant, a messaging system must implement all mandatory features of VPIM in two areas: content and transport. In addition, systems that are VPIM-compliant must not send messages with features beyond the standard unless explicit per-destination configuration of these enhanced features is provided.

VPIM Networking is VPIM-compliant and can exchange messages with all other VPIM-compliant messaging systems, regardless of vendor.

For a point-by-point review of how VPIM Networking complies with the standard, consult AppendixA, “VPIM conformance”.

See also

For additional information on VPIM, visit the official VPIM website:

- http://www.ema.org

Security

In this section

VPIM Networking security

Introduction

Security and message integrity are major concerns for users sending messages over the Internet.

When a private data network is connected to the Internet, the Internet becomes almost an extension of the private network. This poses several security concerns, especially keeping unauthorized users from accessing your network and ensuring that messages are not tampered with during transport.

ATTENTION!

The following information is intended as an overview only. For detailed information on how to secure your system, consult your data network administrator or a security specialist.

Existing security

VPIM Networking makes use of the existing security features of your data network. If it is connected to the Internet, your network probably uses some or all of the following:

- firewall
- packet filters
- proxy servers and application gateways

These are standard security features for a TCP/IP network.

Discuss security concerns

Many configurations provide the correct security for a particular system. Discuss all security issues with the data network administrator.

Firewalls

Introduction

If your messaging network sends messages over the Internet, your data network should be protected by a firewall.

This guide assumes that if your local data network is connected to the Internet, a firewall is already in place.

The following discussion is an overview of how a firewall works with CallPilot. For information on how to configure the firewall to secure your network, consult your data network administrator.

Definition: Firewall

A firewall is a mechanism—consisting of hardware, software, or both—that protects your network from other users on the Internet. Many firewalls are independent devices, while others reside on existing machines.

A firewall controls who can access information behind it and how they can access it. The firewall determines the relationship between users within the firewall and those outside of it.

All traffic into a private data network must go through the firewall. All traffic from the private data network into the public data network must also go through the firewall. Each message is examined, and those that do not meet specified security criteria are blocked.

Other security features

Introduction

In addition to a firewall, your data network may use other standard security features, such as packet filters, proxy servers, and application gateways.

Packet filter

A packet filter, also known as a screening router, limits TCP packet traffic to and from hosts on your network. Packet filters usually consist of both hardware and software components. You set the limits that a packet filter uses.

In most instances, a packet filter is a stand-alone router. All messages traveling to and from hosts on your network go through the router. Software that contains the limits you have established restricts traffic flow.

A packet filter uses the information in the TCP packet header. The packet filter checks the source and destination addresses and compares them to your limits.

You can limit all traffic to only packets that you want. For example, if you want your network to exchange messages only with your branch office, you can set your packet filter to accept only these messages.

Proxy server and application gateway

Proxy servers and application gateways provide another level of security for your network.

Definition: Proxy server

The proxy server performs duties for other computers on the network.

A proxy server separates an intranet behind a firewall. A proxy server often sits on the firewall. At its simplest, the proxy server allows users Internet access from a secured LAN.

A proxy server intercepts all messages entering and leaving a network.

A proxy server also effectively hides true network addresses. Remote users send messages to the proxy server, which then passes the messages to their intended recipients.

Definition: Application gateway

An application gateway is the host computer that runs the proxy server. Application gateways offer the following services:

- authenticating and logging usage
- hiding the internal system names—only the name of the application gateway is visible to the outside world
- simplifying the programming of the packet filter—less complicated filtering rules are required, and only traffic destined for the application gateway is filtered and all other traffic is rejected

Message encryption

Introduction

Message encryption is a special type of security feature.

Definition

Message encryption provides a way to send encoded messages from one site to another in a form that only the two sites can understand.

VPIM Networking and encryption

VPIM Networking on CallPilot does not support any encryption applications.

Connecting to Net Gateway sites

Meridian Mail Net Gateway optionally supports Entrust encryption between Net Gateway sites. Although CallPilot can exchange messages with Net Gateway sites, it does not support encrypted messages.

Messages originating from other sites that are encrypted with Entrust will be rejected by a CallPilot VPIM Networking site. A non-delivery notification is returned to the sender of the message.

CallPilot appears to Net Gateway as a generic VPIM-compliant site. Net Gateway will not send encrypted messages to CallPilot systems.

Implementing VPIM Networking

In this section

Overview

Introduction

Successful implementation of VPIM Networking requires planning and preparation. A plan that specifies the objectives and functionality of the implementation is important.

Before you begin to implement VPIM Networking, you should understand the basic implementation process and what you are expected to do.

ATTENTION!

This section is intended as an overview only. It is assumed that you will work with your data network administrator to set up VPIM Networking.

Implementation scenarios

There are many ways to implement VPIM Networking. The implementation depends on the connections established among the CallPilot system, other sites in the messaging network, and other sites to which you want to send messages.

Whether or not your site uses mail relays, proxy servers, and firewalls, as well as how they are configured, affects the implementation of VPIM Networking.

Therefore, there is no one standard procedure for implementing VPIM. This overview presents several typical implementations that vary in complexity. Your system is probably similar to one of them.

Before you begin

Implementing VPIM Networking is an incremental activity. The following assumptions are made:

- A private, server-based data network, including all necessary security devices, is already in place. This network must support the TCP/IP protocol.
- The Meridian Application Server, on which CallPilot runs, is installed, tested, and connected to the data network.

- CallPilot is installed and tested (except for VPIM Networking), and mailboxes are configured.
- The switch is installed and configured.
- If implemented on the local site, Network Message Service (NMS) is fully implemented.
- If local desktop users use Internet Mail Access Protocol (IMAP) clients, IMAP is fully configured and tested.
- Contact has been made with the network administrators of the remote sites.

Data network is set up

VPIM Networking uses your private data network.

Your Simple Message Transport Protocol (SMTP) message network is configured for your unique needs and may vary in complexity from other networks.

VPIM Networking interacts with one or more of the following systems:

- Domain Name System (DNS) server
- SMTP e-mail proxy server (or gateway, or relay)

Configuration and management of these systems is at your discretion. The following overview is intended as a basic guideline only.

DNS server

The names of VPIM Networking remote sites are entered into the network database during VPIM Networking implementation. These names must be resolvable to IP addresses by VPIM Networking's SMTP delivery agent using the Windows NT system network sockets facilities on the MAS server.

The MAS server may be configured to use a local host name table or, more likely, to use an external DNS. This server must be able to resolve, in cooperation with other DNS servers, all of the network site names entered in the database.

In the event that an intervening firewall or e-mail gateway separates CallPilot from the Internet or intranet, then CallPilot must resolve only the IP address of the relay server, which is also entered during implementation. However, a DNS server must, in turn, be available to the relay server to resolve the final destination address of the site's name in outbound VPIM Networking messages.

DNS and MX records

Where a gateway, proxy, relay server, or firewall intervenes between CallPilot and the Internet or intranet, the DNS can be configured with mail exchange (MX) records. This allows SMTP traffic from remote VPIM Networking sites to be redirected through the gateway and then delivered to the local VPIM Networking system. The DNS does not have to be configured with MX records, because there is an alternate mechanism for the left-hand side to be looked up.

A number of MX records may be specified, with the order in which they are to be used. The preference number in an MX record indicates the preference; a low number indicates a high preference.

For example, if messages addressed to 14165551234@acme.com are to be delivered to the host machine mail.acme.com, then the DNS must be configured with an MX record, such as

- acme.com IN MX 10 mail.acme.com

In this example, 10 is the preference number.

However, if you use another company or ISP to handle your SMTP mail services, the DNS must be configured with an MX record that indicates this relationship, such as

- acme.com IN MX 10 mail.ourISP.net

MX record preference number

If your system directs incoming messages through a mail relay, you may set up MX records. The mail relay can use MX records in the DNS database to locate the CallPilot server. If MX records are not used, the left-hand side of the VPIM address is used.

The mail relay tries each of the hosts listed in the MX records, in order of preference. The host that handles the VPIM Networking messages must be last because CallPilot does not relay messages that cannot be delivered locally.

Firewall

If the Internet is being used to transport VPIM Networking messages, a firewall must be in place and must support transmission of SMTP/MIME.

E-mail gateway server

VPIM Networking may be configured to forward all outbound SMTP message traffic to a machine that serves as an SMTP relay.

If a proxy is to be used for this site, the proxy software must be configured to recognize and handle messages for any other site. For example, the proxy with a domain name of example.com must have an entry that maps, for example, 14165551234 at example.com to 14165551234 at test.example.com.

Incoming VPIM Networking messages are always received as SMTP proxies on port 25. How the message was routed to the site is irrelevant to CallPilot. For example, CallPilot does not care if the incoming messages were routed through mail relays.

For outgoing messages, however, CallPilot is interested in the routing path of the message. The outgoing message can be routed directly to the destination system, or it can be routed through a mail server or a proxy server.

When you configure VPIM Networking, you specify the server that is used for outgoing messages. If you use any other port but port 25 for outgoing messages, you also specify the port number.

Internet Mail Access Protocol (IMAP)

If local users use desktop clients that support IMAP, configure the Internet Mail Client on CallPilot before implementing VPIM Networking.

Because IMAP also uses SMTP, some of the configuration of IMAP is completed on the same dialog boxes where VPIM Networking is configured.

Complete the Incoming SMTP/VPIM messages box on the Message Delivery Configuration dialog box—SMTP/VPIM tab. Complete the SMTP/VPIM Server FQDN box on the Local Messaging Server Properties dialog box—General tab. Add one SMTP/VPIM Networking Shortcut to the Local Prime Switch Location Properties—SMTP/VPIM tab.

When you are implementing VPIM Networking, you may find these boxes already completed. Do not change their configuration or desktop users may be affected.

Windows NT configuration

Configure Windows NT for VPIM Networking. Configure

- TCP/IP setup
- server FQDN
- DNS
- time zone environment variable

See also

For a general overview of the implementation process, consult the *Networking Planning Guide*.

The *Networking Planning Guide* also provides a more detailed discussion about the preliminary requirements, the creation of network diagrams, and the maintenance of a network history.

Planning and engineering considerations

Introduction

When implementing VPIM Networking, the following planning and engineering issues must be considered:

- impact of VPIM Networking load on your local area network (LAN), proxies, firewalls, and mail relays
- message handling abilities (throughput)
- message queuing capacities
- message delivery times
- VPIM Networking limitations

LAN load

It is predicted that the sustained maximum load imposed by VPIM Networking on its connected LAN is 180 kbyte/s. This is less than 1 percent of the 10BaseT bandwidth and is equal to the estimated pump rate for the SMTP delivery process.

This load is independent of the aggregate number of SMTP connections on allocated IP ports.

The average data rate imposed on the LAN by VPIM Networking in order to keep four voice channels active is 21 kbyte/s. This is less than 1 percent of 10BaseT bandwidth.

For example, a 94-minute message creates a 33 Mbyte file that takes three minutes to go from one VPIM Networking system to another.

Message handling abilities (throughput)

Message throughput by VPIM Networking to and from the SMTP network accessed by a LAN depends on the traffic conditions present on that LAN.

The time required to deliver a message also varies with the wide area network (WAN) facilities used to reach, and within, the Internet or intranet.

Message queuing capacities

In its role as a gateway device, VPIM Networking must queue all received messages.

Message delivery times

The total time to deliver a message from one VPIM Networking site to another consists of the following time factors:

- message handling time of VPIM Networking—messages are prepared for ESMTP/MIME transmission
- transfer time on digital network to a receiving or intervening mail relay server
- store and relay time for each mail server or proxy that handles the message between sending and receiving sites

VPIM Networking limitations

Operational performance depends on the characteristics of the Internet or intranet IP network accessed by the LAN. Factors that influence the reliability and throughput of messages transferred to the Internet or intranet may include the following:

- LAN traffic from other sources
- wide area network (WAN) characteristics and traffic
- router capabilities
- electronic mail gateways, proxies, relays, and routers

See also

For detailed planning and engineering information, consult the *Planning and Engineering Guide*.

chapter 3

Gathering information

This chapter describes how to gather the information required to implement VPIM Networking.

Information is required about the data network, the dialing plan configured on the local switch location, and the other sites in the messaging network.

This chapter also describes how to gather information about the other sites in the messaging network, and how to convert this information into a messaging network representation.

In this chapter

Information required

In this section

Overview

Introduction

Before you begin to implement VPIM Networking, gather the information that you need. Having this information before you begin speeds the implementation process. When you analyze the information for inconsistencies and incompleteness, you ensure that potential problems are resolved ahead of time.

Required information

You must gather three types of information:

- local data network information
- local site information, especially about the switch configuration and dialing plan
- messaging network information that is provided by all remote sites

Why gather information?

The gathered information is used to

- Identify the sites in the messaging network.
- Identify the networking protocols used among sites.
- Identify the dialing plan used by each site.
- Determine if the dialing plan needs any modification.
- Create a messaging network representation.
- Prepare for CallPilot configuration.

Data network information

Introduction

VPIM Networking is implemented on top of the existing data network.

To configure VPIM Networking, you must know something about your local data network and the remote data networks.

Data network

The following items were required when CallPilot was installed in your data network:

- FQDN of the outgoing SMTP mail server
- IP address of the DNS
- host name of the local CallPilot system
- subnet mask used by the local CallPilot system

To implement VPIM Networking on CallPilot, the following additional information is needed:

- FQDN of the local server

You must also know the FQDN of each remote server that is expected to exchange VPIM messages with the local CallPilot server.

Gathering this information requires collaboration with the messaging network administrators at other sites.

Remote data network information

For each remote site with which the local site exchanges VPIM Networking information, you must have the FQDN of the SMTP server.

Determining the server FQDN

Introduction

The server FQDN is required to configure VPIM Networking.

The server FQDN is based on the Windows NT setup configured on your system when the Meridian Application Server was implemented.

Getting there Windows NT > Start > Settings > Control Panel

To determine the server FQDN

1. On the Control Panel, select Network.

   Result: The Network dialog box appears.

2. Select the Protocol tab.

3. Select TCP/IP Protocol in the Network Protocols list, and click Properties.

   Result: The Microsoft TCP/IP Properties page appears.

4. Click the DNS tab.

5. Write down the host name and the domain name.

   Note: When combined, these become the server FQDN. A dot is inserted between the host name and the domain name to form the server FQDN.

   Example: hostname and domainname.com are combined to create the server FQDN, hostname.domainname.com.

6. Click Close until the Control Panel closes.

Determining the SMTP/mail proxy server FQDN

Introduction

When configuring VPIM Networking, you may need to provide the outgoing SMTP or the mail proxy server FQDN, depending on your physical network setup.

To determine the FQDN

The server that handles the outgoing messages for your local site already has a FQDN. Ask the data network administrator to provide the required FQDN.

The FQDN has a form similar to the following:

- mail.company.com

Switch information

Introduction

Even though VPIM Networking transmits messages over the data network, not a switch network, dialing plan information is still required if messages are exchanged with integrated sites.

When you begin to implement VPIM Networking, the switch is already installed and configured and is operational for CallPilot.

This means that the switch is set up for dialing among the sites in the messaging network. The dialing plans that are configured on the switch for making telephone calls between sites are also used to address messages among sites.

If messages are exchanged with open sites only, dialing plan information is not required.

Gather dialing plan information

You need the dialing plan information that is configured on the switch. You must know the dialing plan used in the messaging network and how all sites dial one another.

The easiest way to gather this information is to ask the switch technician or system administrator.

Gathering information directly from the switch

Gathering information directly from the switch is not recommended. The information that you require is found on several switch configuration files called overlays. Finding the information can be difficult and time-consuming.

If you must gather the information from the switch, consult your switch documentation for the proper procedures and detailed information on each overlay.

How dialing plans are used by VPIM Networking

The dialing plan that is configured on the switch is used by VPIM Networking. VPIM Networking is designed to be virtually transparent.

Users can address a VPIM Networking message to an integrated site by using the same numbers that they would use to call that integrated site.

Example

To call the site in Dallas, Samantha Singh dials an ESN prefix, 7888, and the extension number of the individual she is calling, 1234.

To send a message to the same user, she enters 75 to begin composing a message, and enters the ESN prefix and the extension number as an address. VPIM Networking translates this information into a complete VPIM address that forms the To: entry:

- 12145551234@company.com

The 1214555 is a VPIM Network shortcut for the Dallas site configured in the local database. The Dallas site must have corresponding information configured for its local site.

Information required from switch

Introduction

Switch configuration information is required to implement VPIM Networking.

Information checklist

The following switch configuration information is required:

- name or physical location of switch (useful to name the switch location on CallPilot)
- dialing plan used
  - Electronic Switched Network (ESN)
  - Coordinated Dialing Plan (CDP)
  - hybrid dialing plan, combining ESN and CDP
  - another dialing plan, such as public switched telephone network (PSTN)
- if ESN or hybrid dialing plan is used:
  - ESN access code
  - ESN location codes
    - local switch location
    - remote switch location
  - overlap of location codes with extension numbers
- if CDP or hybrid dialing plan is used:
  - CDP steering codes
    - local switch location
    - remote switch location
  - overlap of steering codes with extension numbers
- range of extension numbers used at the local site (for example, 7000–7999)
- confirmation that all extension numbers at this switch location can be dialed *directly* from the local switch
- confirmation that all extension numbers at this switch can be dialed in the *same* way

Information from other sites

Introduction

Implementation of a networking solution requires a coordinated effort. Many decisions must be made before implementation begins.

Gather the following information from the other sites in the messaging network that exchange messages with the local site using VPIM Networking:

- site names
- Enterprise site IDs, if Enterprise Networking is implemented in the messaging network
- fully qualified domain names (FQDNs) of the servers
- dialing plan used between the local site and remote messaging servers
- if any remote sites are NMS sites, the following information for each satellite switch location:
  - switch location name
  - switch type
  - location ID

Messaging network representation

Introduction

A messaging network representation provides a complete summary of your messaging network. It contains information about each of the sites and indicates the relationship between each pair of sites.

If sufficiently detailed, a messaging network representation is the primary source of information for implementing a messaging network.

The more detail you can supply, the easier you will find the process of implementation.

A diagram is the most suitable form of representing most messaging networks. A spreadsheet is more appropriate for large messaging networks.

Definition: Messaging network diagram

A messaging network diagram is a graphical representation of your network. It includes the following types of information:

- all sites in the network
- the protocols implemented at each site
- how sites are connected
- the protocol used among sites
- site names and codes
- dialing plan information

Definition: Messaging network spreadsheet

A spreadsheet is more appropriate for representing a large messaging network. It provides the same information as the diagram.

Benefits

There are many benefits to creating a representation of your messaging network. A representation

- offers a clear view of how your network is connected

- gathers all the required information in one source
- offers a way to assess the design and determine if there are any conflicts to resolve before implementation
- provides a useful means of planning future modifications
- helps during the analysis of traffic issues
- reveals areas for improvement
- provides support personnel with a concise, clear view of your messaging and data networks

Coordinating efforts

Much of the information for your network representation must be provided by the administrators of other sites. For example, you need to know the name, server FQDN, and other information from every site with which you exchange VPIM Networking messages.

Although each site administrator creates a representation, ideally one administrator should create a final version that is provided to all sites. This ensures that the representation is comprehensive and that each site uses the same information for implementation.

Protecting the representation

Your network representation contains sensitive information. Keep it properly stored and protected as part of standard security procedures.

See also

For detailed instructions on how to create a network representation, as well as several examples, consult the *Networking Planning Guide*.

chapter 4

Configuring CallPilot for VPIM Networking

This chapter describes how to configure CallPilot during the VPIM Networking implementation process.

The chapter introduces the concepts that are necessary to understand the configuration process and provides detailed configuration procedures.

In this chapter

Configuring CallPilot

In this section

Overview

Configuring CallPilot

The implementation of VPIM Networking requires additional configuration of CallPilot. The information that is entered determines how VPIM Networking exchanges messages.

The configuration process depends on whether you plan to use VPIM Networking to exchange messages with open sites only, with integrated sites only, or with both integrated and open sites.

ATTENTION!

It is strongly recommended that you perform each step in the configuration process in the order presented.

Before you begin

The CallPilot server and your network should be configured and tested.

If your VPIM Networking site is an NMS network, NMS should be configured and tested.

You should know the addresses of several VPIM-compliant systems so that you can test the configuration.

DNS server

Introduction

If VPIM Networking sends messages over the Internet, your site requires a domain name system (DNS) server.

Your local site can maintain its own DNS server or use an Internet service provider (ISP). In both instances, however, additional configuration must be done to the DNS server to make it work with VPIM Networking.

ISP coordination

Many smaller corporations have an external supplier, known as an Internet service provider (ISP), supply DNS services.

If your data network uses an ISP, most of the setup is complete. The ISP fulfills the following requirements:

- registers a domain name on your behalf
- gives the numeric IP addresses of the primary and secondary DNS servers
  - These addresses are used to configure the TCP/IP stacks of the Meridian Application Server.

Work with the ISP

Even if an ISP is supplying your DNS services, you must ensure that the configuration of the DNS server is complete. You must

- Tell the ISP which DNS records you want to publish. These published records allow outside users to send SMTP messages to your network.
- Have the ISP add another mail exchange (MX) record for the computer that accepts e-mail connections for your domain into the DNS database of the ISP. This allows you to receive VPIM Networking messages over the Internet.

- Have the ISP add an A record, corresponding to the MX record, to the DNS database of the ISP.

ATTENTION!

An ISP is not behind a firewall. Check with your ISP to resolve security issues before deciding to use an ISP for mail services.

If you are using your own DNS servers

Many organizations set up and maintain their own DNS servers.

If your organization uses its own DNS servers, this guide assumes that they are already properly set up and configured.

However, VPIM Networking has specific requirements in the lookup table of a DNS server.

Maintain one DNS server

InterNIC does not grant a domain name to an organization unless there are at least two DNS servers. While most small organizations use an ISP to provide both, and most large organizations maintain their own, some organizations use an ISP for one server and maintain another one themselves.

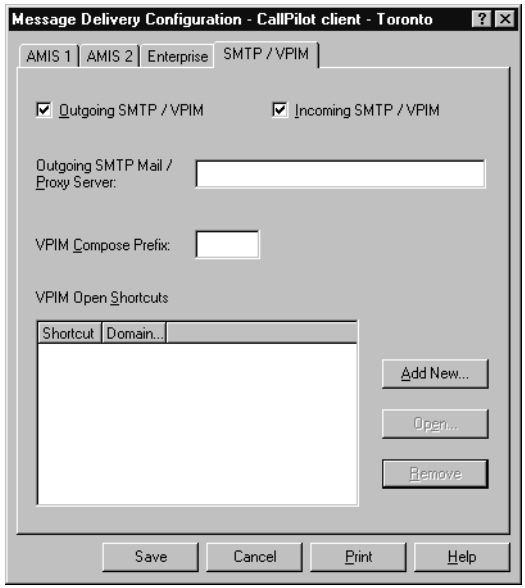
If this is the case for your organization, ensure that the DNS records of both the ISP and the local lookup tables are configured as described.

Message delivery parameters—SMTP/ VPIM tab

Introduction

To implement VPIM Networking, you must set the message delivery parameters that establish how your local messaging server handles VPIM messages.

These parameters are set on the Message Delivery Configuration—SMTP/VPIM tab.



Outgoing and incoming SMTP/VPIM

If VPIM Networking is installed on your system, the following parameters are enabled by default:

- Outgoing SMTP/VPIM
- Incoming SMTP/VPIM

Clear these options to restrict the use of VPIM Networking.

If you do not want local users to send VPIM Networking messages to any other site, open or integrated, clear the Outgoing check box.

If you do not want local users to receive messages from any other site, open or integrated, clear the Incoming check box.

To completely disable VPIM Networking, clear both options.

ATTENTION!

Clearing the Outgoing SMTP/VPIM check box also affects all Internet mail clients. If your system uses IMAP, messages are not exchanged. For a discussion of IMAP security issues and how this check box is used, consult the *Advanced Administration Guide*.

VPIM Compose Prefix

The VPIM compose prefix alerts CallPilot that the rest of the number that is about to be entered is a VPIM address. You must define the VPIM compose prefix.

The VPIM compose prefix is used by telephone users addressing open sites with a VPIM network shortcut. The shortcut must not be unique among the prefixes that are defined in the local network database. The VPIM compose prefix might conflict with other numbers because, while the entire shortcut is unique, the first portion of it might conflict with another number in the network database.

The VPIM compose prefix must not conflict with any other prefixes used in the system, such as the name dialing prefix or the AMIS compose prefix.

If users at your site do not use VPIM network shortcuts to address a message, the VPIM compose prefix is optional.

Example

A VPIM open shortcut is defined as 1416597 = Nortel.ca. A VPIM compose prefix, 22, is defined. Users can address to mailbox 1234 by entering 22 1416597 1234.

The VPIM compose prefix does not conflict with the left-most digits of the VPIM shortcut.

When a VPIM compose prefix is not required

Telephone users

If a telephone user addresses a message to an integrated site using the ESN or CDP dialing plan, the VPIM compose prefix is not required. In this case, the dialing plan code is the unique identifier within the messaging network. When the system locates the dialing plan code within the local network database, both the intended receiving site and the network protocol to be used are identified.

Example

A user addresses a message to a user at a remote site with an ESN compose prefix and a mailbox number: ESN prefix 6333, mailbox 8080. CallPilot checks the network database for the ESN prefix. When it locates the prefix, it also knows the protocol that is used to send a message to that remote site. In this case, the protocol is VPIM Networking.

Desktop users

Desktop users can enter a VPIM compose prefix to address to users at open VPIM sites. However, normally desktop users simply enter the full VPIM address.

Outgoing SMTP Mail/Proxy Server

An outgoing VPIM Networking message may go directly to the destination system, or it may be routed through a mail server or a proxy server. If the message is routed through a mail server or a proxy server, you must enter its FQDN.

When you specify the mail server FQDN, you are telling your system which server is ultimately responsible for handling the outgoing VPIM Networking messages on behalf of the local site.

The specified outgoing server is not the first server contacted. An attempt is made to find the destination host in the local DNS before using the configured server. If the destination host is located in the DNS, this host is used. This arrangement allows corporate mail to be sent directly to servers on an intranet. Mail to external sites is directed through the Internet and passes through mail servers or proxy servers.

Enter the server name in the SMTP mail/proxy server box.

FQDN

While gathering the information to implement VPIM Networking, the data network administrator should have given you the outgoing SMTP mail or proxy server FQDN.

VPIM Open Shortcuts

Desktop users have no difficulty sending messages to users at open sites. A typical open address consists of both numeric and alphabetic characters (for example, 14165971234@nortel.com). These are easy to enter with a computer keyboard.

However, entering the alphanumeric, right-hand side, of an open address is not supported for telephone users. VPIM open shortcuts enable telephone users to address messages.

A VPIM open shortcut maps, or translates, the alphabetic domain name on the right-hand side to a numeric format (for example, 1416597 maps to nortel.com).

A benefit of VPIM open shortcuts is that users have to remember only one way of contacting a recipient.

Example

A desktop user addresses a user at Corporation Inc., an open site, as follows:

- 12045971234@corporation.com

A VPIM open shortcut is defined for this address as follows:

- 1204597 = corporation.com

A telephone user is therefore able to address the user as follows:

- VPIM compose prefix (15) + VPIM open shortcut (1204597) + mailbox number (1234)
- 1512045971234

Restriction

The maximum number of VPIM open shortcuts is 500.

Note: The shortcuts entered here are for open VPIM addressing. They are used for sites that are not part of the private messaging network, or for sites that use only VPIM Networking to open sites.

When sites are added to the VPIM open shortcuts

You might know of several open sites with which users at your local site will exchange VPIM Networking messages. You add these sites during the initial configuration of VPIM Networking.

However, as local users use VPIM Networking and become comfortable with it, they will request the addition of more open sites to the list of shortcuts. Maintaining the VPIM open shortcuts is an ongoing task. The list should reflect the current needs of your local site.

For example, Betty is conducting extensive business with the Polar Ice Company in Anchorage. She wants to be able to send and compose messages to the marketing director at Polar Ice. She requests that Polar Ice be added to the list of VPIM open shortcuts so she can send messages from both her telephone and her desktop.

See also

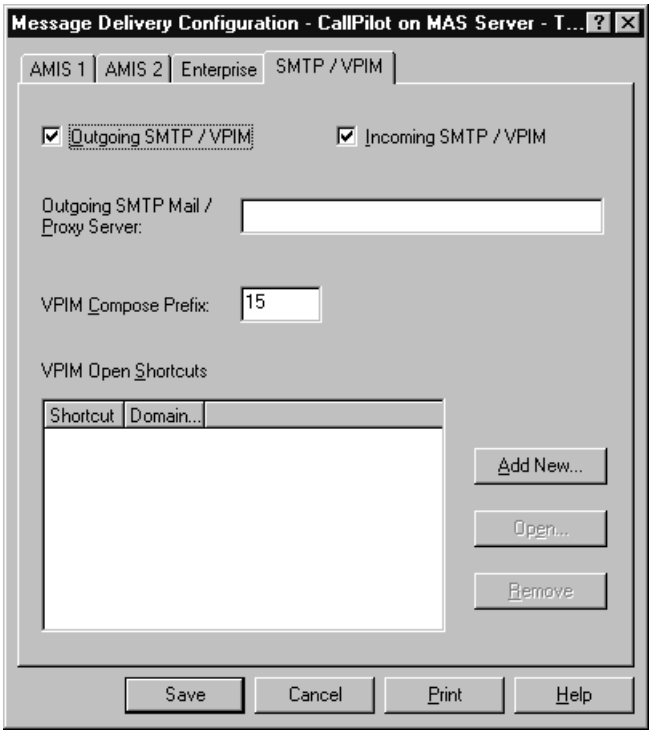
For detailed procedures on maintaining the VPIM open shortcuts, consult “Adding, modifying, and deleting VPIM open shortcuts” on page 231.

Configuring the message delivery parameters

Introduction

You must configure the parameters that determine how your system handles messages.

These parameters are configured on the Message Delivery Configuration—SMTP/VPIM tab.



Getting there Nortel SMI > Meridian Application Server > CallPilot > Networking > Message Delivery Configuration > SMTP/VPIM tab

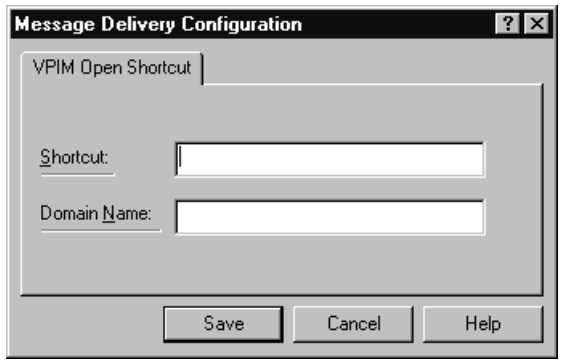
To configure VPIM Networking parameters

1. To enable your site to send outgoing VPIM Networking messages, ensure the Outgoing SMTP/VPIM check box is selected.
2. To enable your site to receive incoming VPIM Networking messages, ensure the Incoming SMTP/VPIM check box is selected.
3. Enter a VPIM compose prefix.

   Note: The VPIM compose prefix must be unique among the prefixes used by the site and cannot conflict with CDP steering codes or ESN prefixes.
4. Enter the address of the mail server or proxy server used by outgoing messages in the Outgoing SMTP Mail/Proxy Server box, if applicable.

   Note: The address was collected during the information-gathering process.
5. Click Add New to add an VPIM open shortcut.

   Result: The VPIM Open Shortcut tab appears.



6. Enter the numeric shortcut for the open site in the Shortcut box.
7. Enter the FQDN for the open site in the Domain Name box.
8. Repeat steps 5–7 for every required VPIM open shortcut.
9. Click Save.

chapter 5

Adding sites to VPIM Networking

This chapter describes how to define the sites in the messaging network that exchange messages with the local site using VPIM Networking.

This chapter describes how to configure the local messaging server and prime switch location. It also explains how to add and configure the remote messaging servers and switch locations if the option to add networking sites is enabled on the system.

In this chapter

About the messaging network

In this section

Overview

Introduction

A CallPilot messaging network consists of a local site and one or more remote sites.

All sites in your private messaging network with which your local site exchanges messages must appear in the Messaging Network Configuration tree view. If a remote site is part of the messaging network, but the local site does not exchange messages with that remote site using VPIM Networking, you do not add that remote site to the tree view during the implementation of VPIM Networking.

To implement VPIM Networking, configure the local site and add and configure all remote sites that will exchange messages with the local site using VPIM Networking.

ATTENTION!

It is strongly recommended that you complete each step in the configuration process in the order presented.

See also

Sites are configured in the Messaging Network Configuration tree view. For an overview of how to work with the tree view, consult the relevant section in the *Networking Planning Guide*.

Before you begin

You need the following before you begin:

- Your messaging network representation is complete, and the required information is available:
  - remote site name
  - remote site switch location type
  - remote site dialing plan information
  - remote site VPIM Network shortcuts
  - remote site loopback mailbox number

- if remote site is a Network Message Service (NMS) site, all satellite switch location information

- If your local site is an NMS site, NMS is configured and tested.
- If local desktop users use IMAP clients, the Internet Mail Client is configured and tested.
- The VPIM message delivery parameters are configured.

Configuration and other networking solutions

Introduction

If another CallPilot networking solution is installed on your local system, most of the local messaging server and local switch location configuration is complete.

Confirm the settings, and enter the information that is specifically required to implement of VPIM Networking.

NMS local site

If your local site is an NMS site, NMS should be implemented and tested before you begin to implement VPIM Networking.

If NMS is implemented, the NMS satellite switch locations for the local site appear in the Messaging Network Configuration tree view.

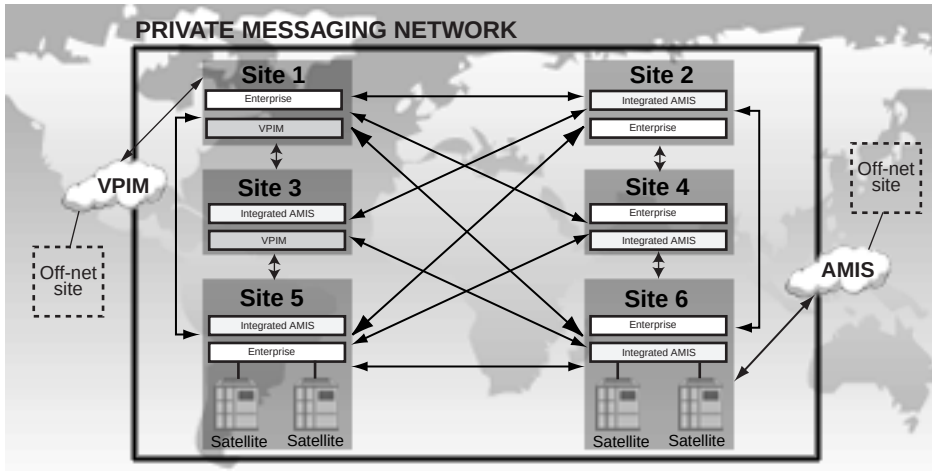
Remote sites

If another CallPilot networking solution is implemented on your system, remote sites have been added and configured. These sites appear in the Messaging Network Configuration tree view. These sites communicate with the local site using the other networking solution.

When you implement VPIM Networking, you add and configure the remote sites that communicate with your local site using VPIM Networking. These sites appear in the tree view only as you add them.

Example: Implementing VPIM Networking

In this example, you are the network administrator of Site 1. Working with the network administrators of other sites, you have created a messaging network representation. Note that many details are removed from this diagram for clarity.



G101139.e

Your local site has the following networking solutions: Enterprise Networking and VPIM Networking.

Since you are following the recommended order of implementation, you have implemented and tested Enterprise Networking. During this implementation, you configured the local site and added Sites 2, 4, 5, and 6 to your network database, because these sites use Enterprise Networking to exchange messages with your site.

To implement VPIM Networking, you complete additional details required for the local site configuration. You add VPIM open shortcuts to your network database, because local users will exchange messages with open sites. You add and configure Site 3 as a remote site.

Configuring the local site

In this section

Overview

Introduction

When CallPilot is initially installed on your system, a local messaging server and a prime switch location are automatically added to the Messaging Network Configuration tree view.

Local messaging server name

By default, both the local messaging server and the prime switch location are assigned the name “Untitled.” Assign new names to the local messaging server and the prime switch location during configuration.

The local site receives its name from the name assigned to the local messaging server.

Configuration

Both the local messaging server and the prime switch location must be configured.

Configuration of the messaging server consists of saving general information about the messaging server, such as name and description, to the network database.

Configuration of the prime switch location consists of saving general information about the switch location as well as detailed dialing plan information.

Configuring the local server if another messaging solution is implemented

If you have implemented another CallPilot networking solution on your local system, you have already completed much of the local messaging server configuration.

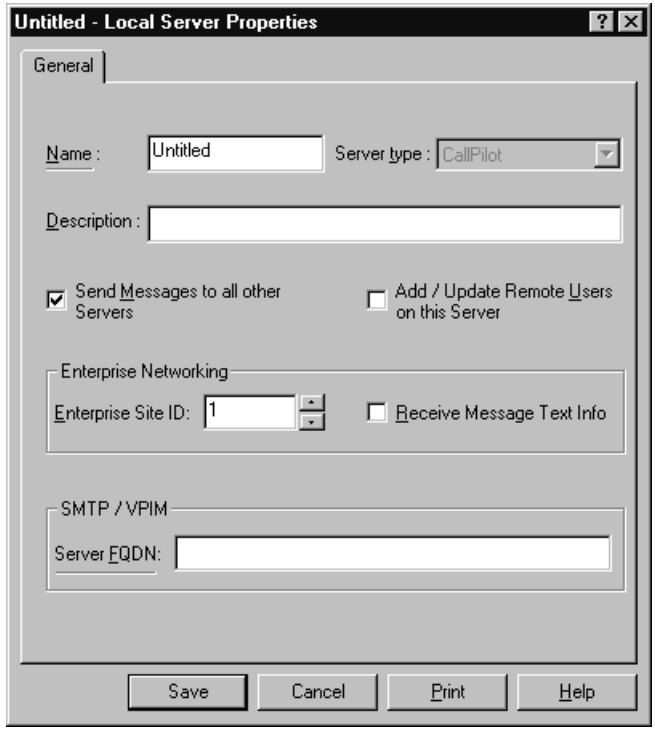
Complete the additional configuration required for VPIM Networking.

Configuring the local messaging server

Introduction

You must configure the local messaging server to implement VPIM Networking.

The local messaging server is configured on the Local Messaging Server Properties—General tab.



Name

By default, both the local messaging server and the prime switch location are assigned the name “Untitled.” Assign new names during configuration.

The messaging server is usually given a name that corresponds to its geographic location.

Local site name

The name given to the local messaging server becomes the name of the local site.

Server type

The local messaging server is always CallPilot.

Description

Provide a brief description of the messaging server, or implementation notes, such as when the server was configured or who completed the configuration, in the Description box.

Send Messages to all other Servers

The Send Messages to all other Servers check box determines if the local site can send messages to integrated remote sites in the messaging network.

This check box is selected by default and is cleared only under exceptional circumstances.

When cleared, the local messaging server does not send messages to any integrated remote site using any protocol. Messages can still be sent to open remote sites.

When to clear this option

This option lets you quickly disable messaging from your local site. Clear this check box in emergency situations.

Restricting messages to individual sites

Clearing the Send Messages to all Other Servers check box is a quick way to disable the system. It is not used to restrict the sending of messages to individual sites.

To prohibit the local messaging server from sending messages to a particular integrated remote site, clear the Send messages to this Server check box on the Messaging Network Configuration—Remote Messaging Server Properties—General tab.

For example, your messaging network has six sites. You want to send messages to five of them. You select the Send Messages to all other Servers check box while configuring the local messaging server. You clear the Send Messages to this Server check box when configuring the remote server to which you do not want to send messages.

Restricting messages to open remote sites

There is no way to prohibit the local messaging server from sending messages to specific open remote sites or to all open remote sites.

To restrict local users from sending messages to open sites, you must clear the Send Outgoing VPIM Messages checkbox on the Message Delivery Configuration—SMTP/VPIM Networking tab. However, this also restricts the sending of messages to integrated remote sites.

Add/Update Remote Users on this Server

The Names Across the Network feature is available with Enterprise Networking only.

The Add/Update Remote Users on this Server check box enables the Names Across the Network feature to work with Enterprise Networking.

The Names Across the Network feature is not supported by VPIM Networking.

If enabled, this check box should have been configured during the implementation of Enterprise Networking.

Enterprise Site ID

The Enterprise Site ID box is enabled only if Enterprise Networking is implemented on your local messaging server.

If enabled, this box should have been configured during the implementation of Enterprise Networking.

Receive Message Text Info

The Receive Message Text Info check box is enabled only if Enterprise Networking is implemented on your local messaging server.

If enabled, this check box was configured during the implementation of Enterprise Networking.

Server FQDN

The fully qualified domain name (FQDN) of the VPIM Networking server is required.

The FQDN of the local messaging server is automatically added to the From: entry in an outbound message. It forms the right side of a VPIM address.

The FQDN is taken from the Windows NT TCP/IP configuration page. You determined the FQDN while gathering the required information for implementing VPIM Networking. For a review of how to determine the FQDN, see “Determining the server FQDN” on page 104.

Note: If Internet Mail Client is implemented locally, and local desktop users use IMAP clients, the Server FQDN box is already completed.

Getting there Nortel SMI > Meridian Application Server > CallPilot > Networking > Messaging Network Configuration

To configure the local messaging server

1. In the Messaging Network Configuration tree view, select the local messaging server.
2. On the File menu, click Open.

   Result: The Local Prime Server Properties dialog box appears.
3. To change the name of the local messaging server, enter a new name in the Name box.

   Tip: The name given to the local messaging server is also the name of the local site.

   Note: The server type is always CallPilot and cannot be changed.
4. In the Description box, enter details about the local messaging server.
5. To send messages to all other sites in the messaging network, ensure the Send messages to all other Servers check box is selected.

   Note: The Add/Update Remote Users on this Server, Enterprise Site ID, and Receive Message Text Info boxes are enabled only if Enterprise Networking is installed. They are configured during the implementation of Enterprise Networking.

6 In the Server FQDN box, enter the fully qualified domain name of the local messaging server.

Tip: The FQDN is taken from the Windows NT TCP/IP Properties page.

Note: If another networking solution is already implemented on the local site, the FQDN box already contains either the correct FQDN or a placeholder. Confirm or replace the information as required. If Internet Mail Client is implemented, the FQDN box is already completed correctly.

7 Click Save.

Result: The information is validated and saved to the network database.

What's next?

After configuring the local messaging server, you must configure the local prime switch location.

Configuring the local prime switch location

Introduction

You must configure the local prime switch location to implement VPIM Networking.

The final step in configuring the local site for VPIM Networking is to configure the local prime switch location.

If any other networking solution is implemented

If another networking solution is implemented on the local site, the local switch location configuration is already configured.

You must check the current configuration information. Make any necessary modifications.

If NMS is implemented

If NMS is implemented on the local site, the information required for the local switch location configuration is already complete.

All satellite switch locations attached to the local prime switch location are also already installed.

If no other networking solution is implemented

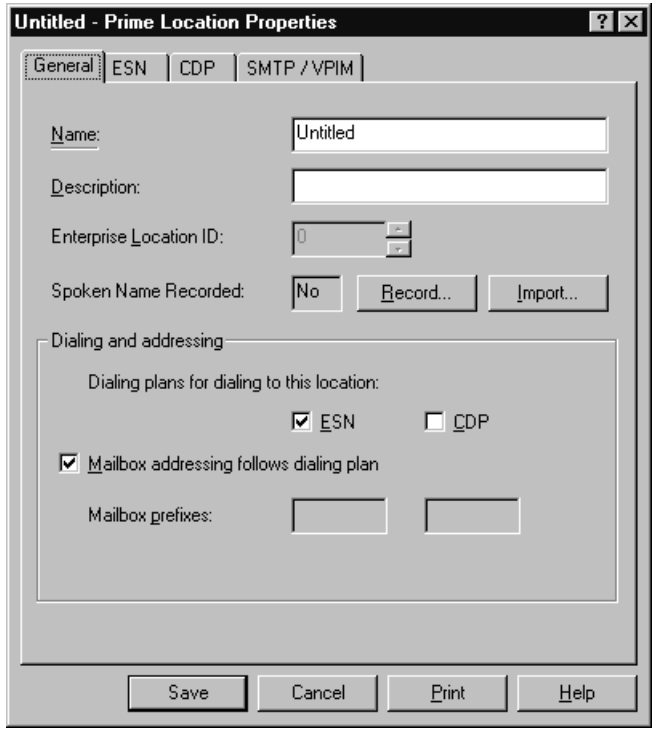
If no other networking solution is implemented on the local site, you must complete the General tab. You may have to complete the ESN tab or the CDP tab, or both, depending on the dialing plan used on your local switch location. You must also complete the SMTP/VPIM tab.

Where the prime switch location is configured

The Prime Switch Location Properties dialog box consists of four tabs:

- General
- ESN
- CDP

- SMTP/VPIM



General tab

Complete the General tab no matter what dialing plan your site uses.

ESN tab

Complete the ESN tab if the local site uses the ESN or a hybrid dialing plan.

CDP tab

Complete the CDP tab if the local site uses the CDP or a hybrid dialing plan.

SMTP/VPIM tab

Complete the SMTP/VPIM tab to implement VPIM Networking.

Open VPIM Networking

If you are implementing VPIM Networking to work with open remote sites only, complete the following tabs:

- General—set the dialing plan to none by clearing both dialing plan boxes
- SMTP/VPIM

Name

Every switch location needs a name that is unique within the messaging network. Usually, this name is the same as the name of the messaging server. This ensures that the identity of the switch location within the network is immediately apparent. A geographic name is common.

For example, if a messaging server is named “Moscow,” the prime switch location is usually also named “Moscow.”

By default, the local prime switch location is given the name “Untitled.” This name must be changed.

Description

The Description box is useful for short notes, reminders, or comments about the switch location.

You might find it useful to specify your switch model, the date of the switch configuration, or contact information for the switch technician.

Enterprise Location ID

The Enterprise Location ID box is not enabled for the prime switch location.

Note: The Enterprise Location ID for the prime switch location is always 0 and cannot be changed.

Spoken Name Recorded

If your local site is not an NMS site, the Spoken Name Recorded check box is not enabled.

If your site is an NMS site, the Spoken Name Recorded check box was configured during the NMS implementation.

Dialing plan information

You need detailed information about the dialing plan used by the local site when you configure the local prime switch location.

Dialing plans for dialing to this location

You must specify which of the following dialing plans is used to dial to the local switch location:

- ESN
- CDP
- hybrid that combines ESN and CDP
- another dialing plan (such as PSTN)

When you configure the local prime switch location, you specify the dialing plan that is used to dial to the local site.

Note: If you use ESN anywhere in the messaging network, you must select ESN because you need an ESN access code.

Mailbox specifications

The following boxes are dynamically enabled and disabled depending on the dialing plan you have specified for the local prime switch location:

- Mailbox addressing follows dialing plan
- Mailbox prefixes

Mailbox addressing follows dialing plan

A mailbox number is often the same as the number used to dial a user. While common, this arrangement is not a requirement. You must specify whether at your local site the mailbox number is the same as the number dialed.

For example, Li Chen’s mailbox number is 7575, but her extension number is 8888.

The Mailbox addressing follows dialing plan check box is enabled only if NMS is installed on the local messaging server.

If enabled, this check box was configured during the implementation of NMS.

Mailbox prefixes

A mailbox prefix is a leading string of digits that uniquely identifies a mailbox number as belonging to a particular site.

If the local site does not have NMS installed, the mailbox prefixes are never required for the local prime switch location.

If the local site does have NMS installed, the mailbox prefix or prefixes are already properly configured.

Getting there Nortel SMI > Meridian Application Server > CallPilot > Networking > Messaging Network Configuration

To configure the Prime Switch Location Properties dialog box

1. In the Messaging Network Configuration tree view, select the local prime switch location.
2. On the File menu, click Open.

   Result: The Prime Switch Location Properties—General tab appears.
3. To change the name of the local prime switch location, enter a name in the Name box.
4. In the Description box, enter details about the local prime switch location.

   Note: The Enterprise location ID is always 0 and cannot be changed.
5. Confirm the status of the Spoken Name Recorded box.

   Note: This box is enabled only if NMS is installed and was completed during NMS implementation.
6. Specify the dialing plan used to dial the local prime switch location. Select the

   - ESN check box if ESN is used
   - CDP check box if CDP is used
   - ESN and CDP check boxes if a hybrid dialing plan is used

   Note: Leave both check boxes clear if another dialing plan, such as PSTN, is used.
7. If the local site is an NMS site, check the configuration of the Mailbox addressing follows dialing plan check box and the Mailbox prefixes boxes.

8 Determine whether you must complete another tab. If not, click Save to close the dialog box.

9 Select another tab to continue the configuration.

What's next?

If the local site uses an ESN, CDP, or hybrid dialing plan

After you complete the General tab, you must complete the ESN tab, or the CDP tab, or both tabs, depending on the dialing plan used.

If the local site uses another dialing plan

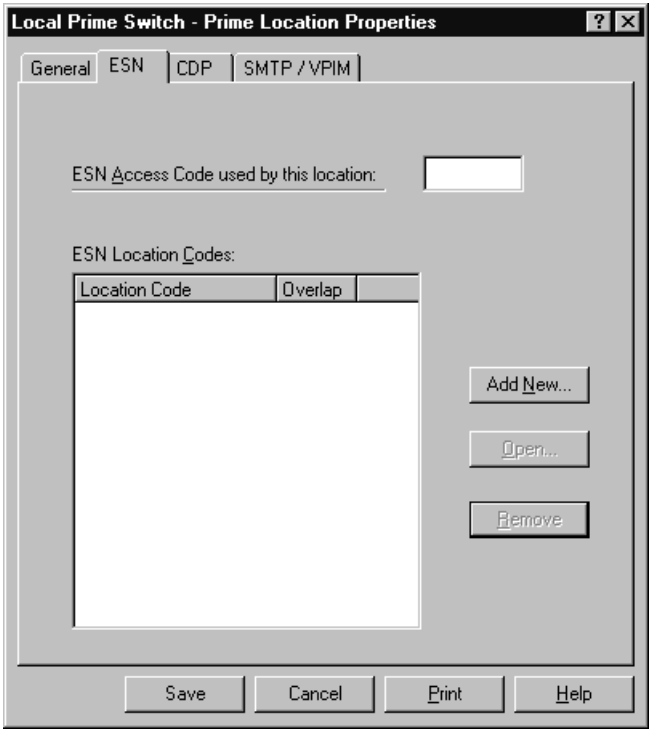
If your local site uses another dialing plan, such as PSTN, complete the VPIM tab.

Configuring ESN information

Introduction

If the local prime switch location uses either an ESN dialing plan or a hybrid dialing plan, you must complete the ESN tab.

You must provide the ESN access codes and ESN location codes. These are combined to create the ESN prefix.



See also

For a description of the ESN dialing plan and how it works, consult the *Networking Planning Guide*.

ESN Access Code used by this location

The ESN access code is used to access ESN routing in the same way that an access code, such as 9, is used to dial out to the public network from a private network.

Typically, all switches in a messaging network use the same ESN access code.

ESN Location Codes

An ESN location code is a routing prefix that identifies a location within a network. It is usually three digits long, but can be up to ten digits long.

You must also indicate the number of digits in the ESN location code that overlap the mailbox number.

The ESN Location Codes list contains all ESN location codes currently assigned and indicates the overlap between the ESN location code and the mailbox directory numbers.

ESN location codes can be added, modified, or deleted at any time. The ESN location codes must always match the dialing plan configuration on the switch.

ESN location code capacity

The maximum number of ESN location codes for a switch location is 30.

ESN location code overlap

When you are entering the dialing plan information for the local site, you must calculate the number of digits in the ESN prefix that overlap the digits in the local extension.

If there is overlap between the rightmost digit or digits of the location code and leftmost digit or digits of the extension number, enter the amount of overlap.

The following table provides examples of ESN location code overlap.

Access code	Location code	Extension number	Number dialed by users at other sites	Overlap
6	33**8**	**8**300	633**88**300	0
6	33**8**	**8**300	633**8**300	1

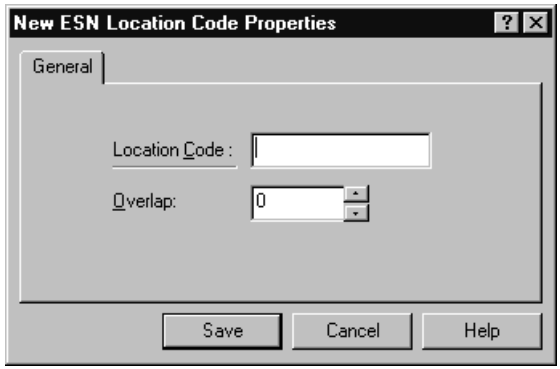
Access code	Location code	Extension number	Number dialed by users at other sites	Overlap
6	300	**8**000-**8**999	6300**8**300-6300**8**999	0
6	30**2**	**2**5000-**2**6999	630**2**5000-630**2**6999	1

Getting there Nortel SMI > Meridian Application Server > CallPilot > Networking > Messaging Network Configuration > Prime Switch Location Properties > ESN tab

To configure the ESN information

1. Enter the ESN access code.
2. To add a new location code, click the Add New button.

   Result: The New ESN Location Code Properties dialog box appears.



3. In the Location Code box, enter the location code.
4. In the Overlap box, enter the number of digits in the extension number that overlap the location code.
5. Click Save.

   Result: The location code and overlap are validated and appear in the ESN Location Codes list box on the ESN tab.
6. Repeat steps 3–5 for each ESN location code required.

7 When you have finished configuring the ESN information, determine if you must configure CDP information.

- If yes, click the CDP tab.
- If no, click Save to validate the ESN configuration information and save it to the database.

What's next?

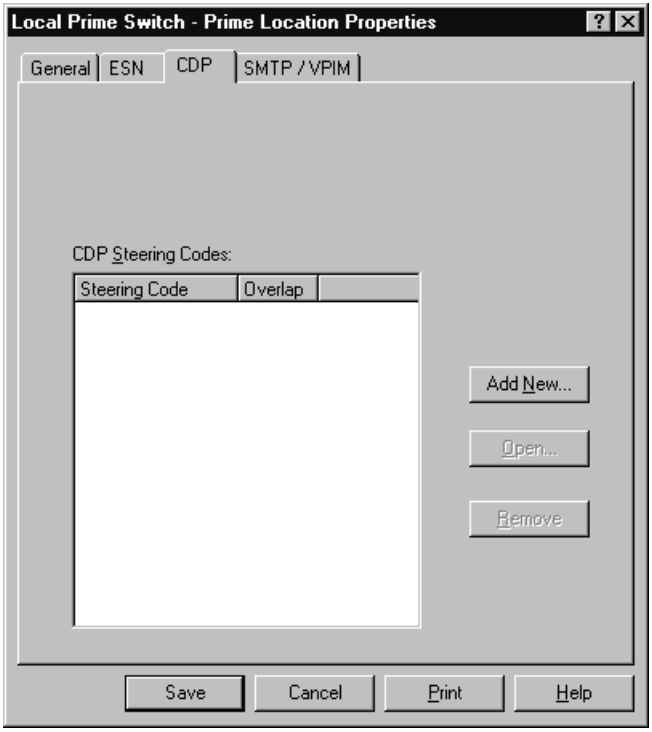
If your local prime switch location uses the hybrid dialing plan, click the CDP tab to continue configuring the local prime switch location.

Configuring CDP information

Introduction

If the local switch location uses either a CDP dialing plan or a hybrid dialing plan, complete the CDP tab.

You must provide the CDP steering codes.



See also

For a general description of the CDP dialing plan and how it works, consult the *Networking Planning Guide*.

CDP Steering Codes

A CDP steering code is a site prefix that identifies the local site within the network. Therefore, a CDP prefix must be unique for all switches in the messaging network.

CDP steering codes are determined by the switch technician.

The CDP steering codes defined on the switch are entered on CallPilot because the system must be able to identify the steering code in the mailbox number to determine the site.

The CDP Steering Codes list box contains all CDP steering codes currently assigned to the switch location. The list box also indicates the overlap between the CDP steering codes and the mailbox directory numbers.

CDP steering codes can be added, modified, or deleted.

CDP steering code capacity

The maximum number of CDP steering codes for a switch location is 500.

CDP steering code overlap

When entering the dialing plan information, you must calculate the number of digits in the CDP steering code that overlap the digits of the local extension.

If there is overlap between the last digit or digits of the steering code and the first digit or digits of the extension number, enter the amount of overlap.

Normally, the steering code overlaps with the first few digits of a local extension number.

The following table provides three examples of CDP steering code overlap:

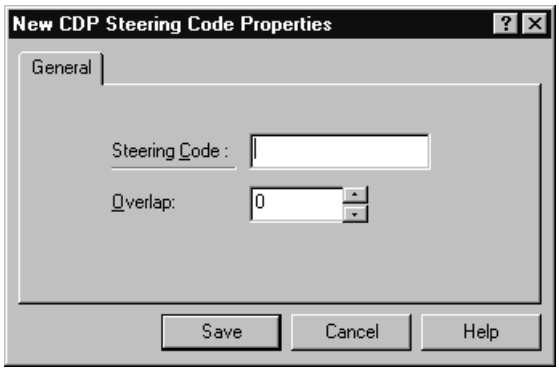
Steering code	Extension number	Number dialed by users at other sites	Overlap
22	**22**345	**2222**345	0
22	**22**345	**222**345	1
22	**22**345	**22**345	2

Getting there Nortel SMI > Meridian Application Server > CallPilot > Networking > Messaging Network Configuration > Prime Switch Location Properties > CDP tab

To configure the CDP information

1 To add a new steering code, click the Add New button.

Result: The New CDP Steering Code Properties dialog box appears.



2 In the Steering Code box, enter the steering code.

3 In the Overlap box, enter the number of digits in the extension number that overlap the steering code.

4 Click Save.

Result: The steering code and overlap are validated and appear in the CDP Steering Codes list box on the CDP tab.

5 Repeat steps 1–4 for each CDP steering code required.

6 When you have added all the necessary CDP steering codes, click Save.

Result: The information is validated and saved to the network database.

What's next?

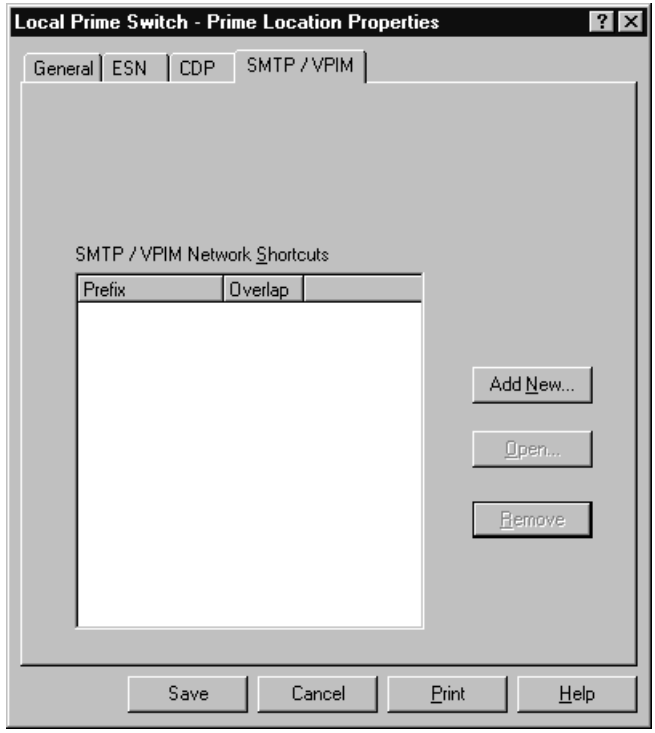
Complete the SMTP/VPIM tab, and configure the VPIM Networking shortcuts.

Configuring VPIM information

Introduction

You must configure SMTP/VPIM network shortcuts if telephone users are going to address messages to remote sites in your messaging network. These are attached to all outgoing messages.

The SMTP/VPIM networking shortcuts are configured on the SMTP/VPIM tab.



SMTP/VPIM Network Shortcuts

Although you can define up to 30 SMTP/VPIM network shortcuts, most messaging networks need only one or two.

The SMTP/VPIM network shortcuts defined for the local prime switch locations provide a way to create the left side of the From: entry in a message header. They are not shortcuts in the sense that they are only a few digits long.

SMTP/VPIM network shortcuts are also used to identify local addresses of incoming messages.

Note: SMTP/VPIM network shortcuts are defined on the New SMTP/VPIM Prefix Properties dialog box. The VPIM prefix is the SMTP/VPIM network shortcut.

Example

With the following SMTP/VPIM network shortcut defined:

- 1416777

the From: entry sent with an outbound message from mailbox xxxx is

- From: 1416777xxxx@serverFQDN

where xxxx is the extension number.

Relationship to PSTN

Usually, the SMTP/VPIM network shortcut corresponds to the PSTN number for the local site.

If the telephones are not directly dialable from the PSTN and calls are routed to a switchboard, enter the switchboard number with an overlap of 0. For example, 14165557000, overlap 0.

Note: It is strongly recommended that you use PSTN numbers as the SMTP/VPIM network shortcuts.

Length of shortcuts

Although it might be tempting to define short SMTP/VPIM networking shortcuts, such as 4588, avoid doing so.

ATTENTION!

The shorter a SMTP/VPIM network shortcut is, the more likely it will conflict with the left-hand side of another open VPIM address.

For example, if your organization owns the telephone numbers 14165977000-7999 and the mailboxes are 7000-7999, then define 14165977, overlap 1—not 1416597, overlap 0. This avoids a mismatch with an open VPIM address, such as 16165972134@neighbor.com.

SMTP/VPIM Network Shortcuts Overlap

When entering the dialing plan information, you must calculate the number of digits in the VPIM network shortcut that overlap the digits of the local extension.

If there is overlap between the last digit or digits of the shortcut and the first digit or digits of the extension number, enter the amount of overlap.

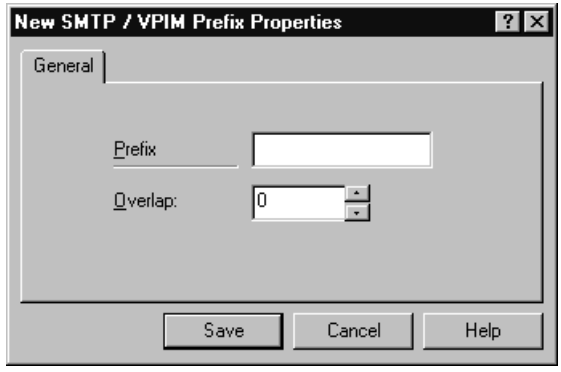
Note: If Internet Mail Client is implemented locally, and local desktop users use IMAP clients, one network shortcut is already configured.

Getting there Nortel SMI > Meridian Application Server > CallPilot > Networking > Messaging Network Configuration > Prime Switch Location Properties > SMTP/VPIM tab

To configure the VPIM information

1 To add a new SMTP/VPIM network shortcut, click the Add New button.

Result: The New SMTP/VPIM Prefix Properties dialog box appears.



2 In the Prefix box, enter the SMTP/VPIM network shortcut in dialable format.

Note: A PSTN format is recommended. Only one SMTP/VPIM network shortcut is required.

3 In the Overlap box, enter the number of digits in the mailbox number that overlap the shortcut.

4 Click Save.

Result: The shortcut and overlap are validated and appear in the SMTP/VPIM Network Shortcuts list box on the SMTP/VPIM tab.

5 Repeat steps 1–4 for each network shortcut required.

6 When you have added all the necessary network shortcuts, click Save.

Result: The information is validated and saved to the network database.

What's next?

If the local site is not an NMS site, you have completed the configuration of the local site and are ready to begin adding and configuring remote sites.

If the local site is an NMS site, complete the configuration of the local site. See "Configuring an NMS local site" on page 159.

Configuring an NMS local site

Introduction

If your local site is an NMS site, you configured the local prime switch location and the local satellite switch locations during the implementation of NMS.

You must complete two steps to implement VPIM Networking:

- Check the current configuration.
- Configure the SMTP/VPIM tab for all switch locations.

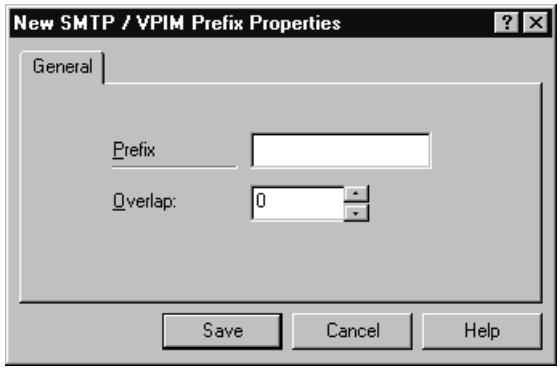
Getting there Nortel SMI > Meridian Application Server > CallPilot > Networking > Messaging Network Configuration

To configure a local satellite switch location for VPIM Networking

1. Select the local satellite switch location.
2. On the File menu, select Properties.

   Result: The Properties dialog box for the selected switch location appears.
3. Check the current configuration, and make changes if necessary.
4. Click the SMTP/VPIM tab.
5. To add a new SMTP/VPIM network shortcut, click the Add New button.

   Result: The New SMTP/VPIM Prefix Properties dialog box appears.



6 Enter the SMTP/VPIM networking shortcut in the Prefix box and the overlap with the local mailbox numbers.

7 Click Save.

Result: The SMTP/VPIM network shortcut appears in the SMTP/VPIM Network Shortcuts list box on the SMTP/VPIM tab.

8 Repeat steps 5–7 for each SMTP/VPIM network shortcut required.

9 When you have added all required SMTP/VPIM networking shortcuts, click Save.

Result: The information is validated and saved to the network database.

10 Repeat steps 1–9 for all switch locations in the local site.

What's next?

You are ready to begin adding and configuring the remote sites that use VPIM Networking to exchange messages with your local site. See the section "Adding and configuring a remote site" on page 161.

Adding and configuring a remote site

In this section

Overview

Introduction

When you implement VPIM Networking, you add to the Messaging Network Configuration tree view all the remote sites that use VPIM Networking to exchange messages with the local site.

Every remote site added to the tree view must be configured.

Information required

The information that you enter when configuring a remote site reflects the information that is configured for that site in its own local network database. For example, you enter the name of that site and its FQDN. You must get this information from the remote network administrator.

But configuring a remote site is not simply copying the information provided by the remote site. You also enter information that reflects how your local site will communicate with that remote site. For example, for each remote site you decide whether your local site sends messages to this particular remote server.

Main steps

There are three main steps to adding a remote site to your local network database. For each remote site, you must add and configure

- the remote messaging server
- the remote prime switch location
- the remote satellite switch locations, if the remote site is an NMS site

Network representation

Much of the information that you must provide while configuring a remote messaging server is contained in the network diagram or spreadsheet.

Configuring a remote messaging server

Introduction

When CallPilot is initially installed on your system, your local site, consisting of a local messaging server and a local prime switch location, is automatically added to the Messaging Network Configuration tree view.

However, you must manually add each remote site that exchanges messages with the local site using VPIM Networking to the Messaging Network Configuration tree view. Both the remote messaging server and the remote prime switch location must be configured.

The following tabs must be completed for each remote messaging server:

- Remote Messaging Server Properties—General tab
- Remote Messaging Server Properties—Connections tab

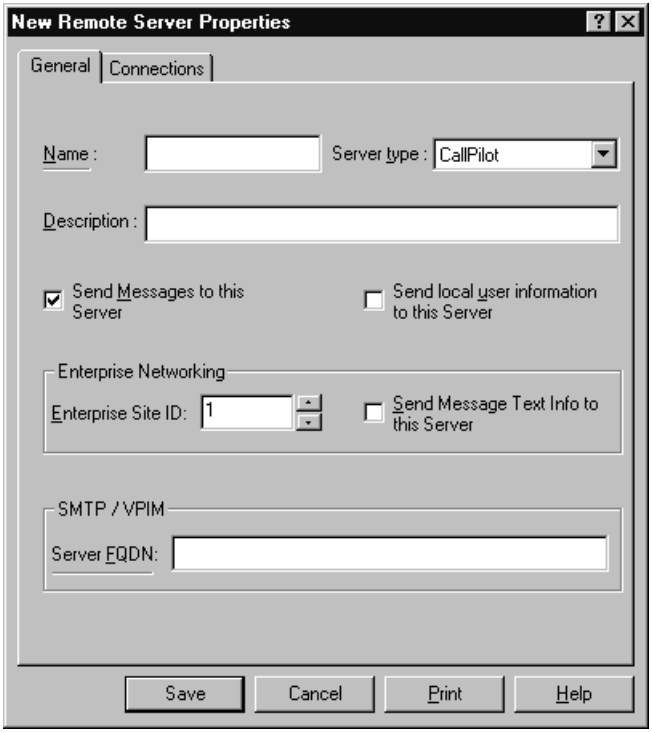
Remote servers and other networking solutions

If you have implemented another CallPilot networking solution on your system, you have already added remote sites to the Messaging Network Configuration tree view.

The process of adding a remote site is essentially the same regardless of the networking solution being implemented. However, when you add remote sites during the implementation of VPIM Networking there are important differences to consider.

Remote Messaging Server Properties—General tab

The Remote Messaging Server Properties—General tab contains detailed information about the remote messaging server and defines how the local site and the remote site exchange messages.



Name

You should assign the remote messaging server the same name that was assigned by its local network administrator. This makes the network easier to administer and maintain, because all network administrators use the same names for the same sites.

For example, if a remote site calls itself Connecticut, you should name it Connecticut when you add it to the Messaging Network Configuration tree view.

Server type

The remote messaging server can be any of the following types:

- CallPilot (CallPilot)
- Meridian Mail Net Gateway (MMNG)
- Norstar Voice Mail (Norstar)
- Meridian Mail
- Other

Description

Provide a brief description of the remote messaging server or useful notes, such as when the messaging server was configured or who completed the configuration.

Send Messages to this Server

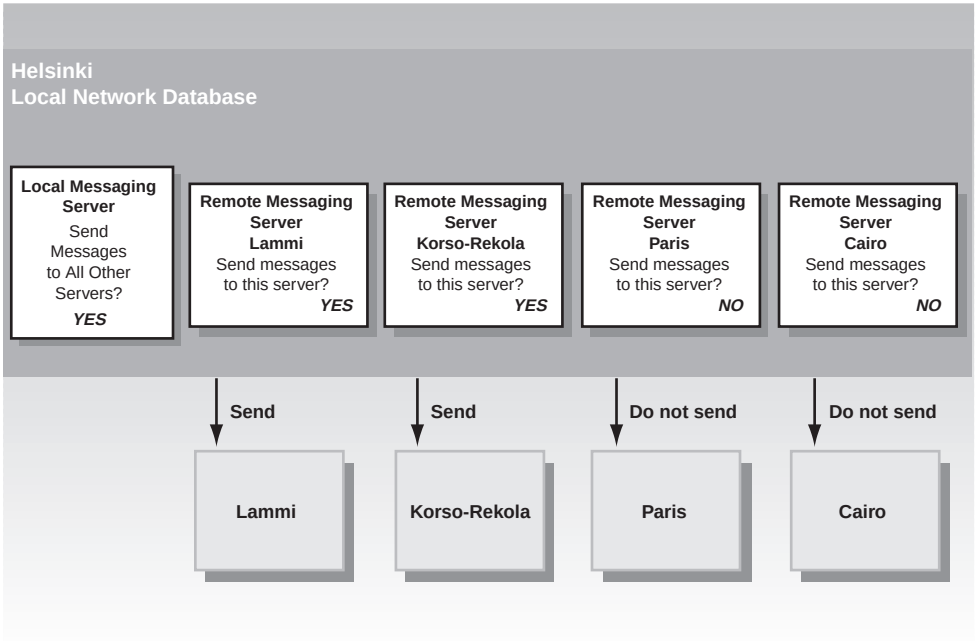
The Send Messages to this Server check box interacts with the Send Messages to all Other Servers check box on the Local Messaging Server Properties—General tab.

When you configured the local messaging server, you decided if you wanted the local messaging server to send messages to all remote messaging servers. This option is selected by default and is cleared under exceptional circumstances only.

However, you can still stop the delivery of messages to specific remote messaging servers. The Send Messages to this Server check box enables you to block the delivery of messages from your local messaging server to a particular remote site.

Example

In the following diagram, Helsinki is configured to deliver messages to all other sites. However, the network database records for Paris and Cairo specify that messages are not sent to these messaging servers. Messages are sent to Lammi and Korso-Rekola. Therefore, while the potential exists for sending messages to all remote sites, only two sites receive messages from Helsinki.



G100995.eps

Send local user information to this Server

The Send local user information to this Server check box determines if the Names Across the Network feature is used with this remote site. If enabled, this feature was configured during the implementation of Enterprise Networking.

Enterprise Site ID

The Enterprise Site ID box is enabled only if Enterprise Networking is installed on the local site.

All remote sites connected to a site that has Enterprise Networking installed must have an Enterprise site ID, regardless of the actual protocol used with the site.

Therefore, if Enterprise Networking is installed locally, when implementing VPIM Networking you must enter the site ID for all remote sites, even those that exchange messages with the local site using the VPIM protocol.

Consult the network representation for the correct Enterprise site IDs.

Send Message Text Info to this Server

This check box applies only to remote sites that use Enterprise Networking to exchange messages with the local site. For remote sites that use VPIM Networking, this box is not applicable.

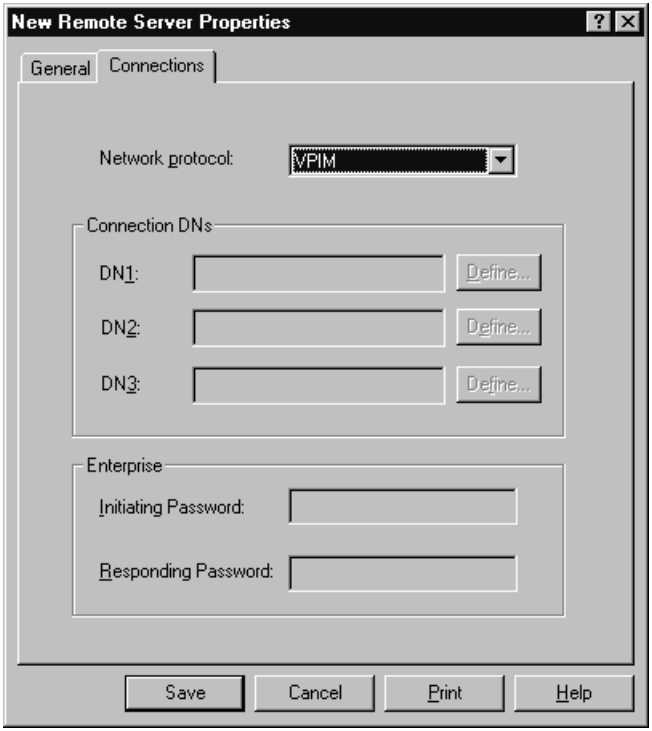
Server FQDN

You must provide the FQDN of the server at the remote site.

This FQDN forms the right side of the To: entry in a message header for a message sent to this site. The right side is formed from a VPIM networking shortcut for this remote site.

Remote Messaging Server Properties—Connections tab

The configuration of a remote messaging server continues on the Connections tab.



Network protocol

When implementing VPIM Networking, the only box that you must complete on this tab is Network protocol. Select VPIM, because your local site uses VPIM Networking to exchange messages with this remote site.

To use a particular protocol, both sites must have the same networking solution installed and implemented.

If a remote site does not use the same protocol as the local site, the following occurs when the local site attempts to send a message:

- The message is not delivered.
- An error message is generated.

- The remote site is put into error status.

Other boxes

When you implement VPIM Networking, you do not complete the Connection DNs or the Enterprise Passwords boxes.

Getting there Nortel SMI > Meridian Application Server > CallPilot > Messaging Network Configuration

To configure a remote messaging server

1. In the Messaging Network Configuration tree view, select Remote Server Maintenance.
2. On the File menu, click New > Messaging Server.

   Result: The Remote Messaging Server Properties dialog box appears.
3. On the General tab, in the Name box, enter the name of the remote messaging server.
4. Select the server type from the Server type box.
5. In the Description box, enter details about the remote messaging server.
6. To enable the local messaging server to send messages to this remote messaging server, ensure that the Send Messages to this Server box is selected.
7. If an Enterprise site ID is required, enter the unique site ID number of the remote messaging server or a valid placeholder.
8. In the Server FQDN box, enter the FQDN of the remote site.

   Note: The FQDN is supplied by the remote network administrator.
9. To continue configuring the remote messaging server, click the Connections tab.
10. From the Network protocol list, select VPIM.
11. Click Save.

    Result: The information is validated and entered into the local network database.

What's next?

After you add information about the remote messaging server into your local network database, you must also add information about the remote prime switch location.

Configuring a remote prime switch location

Introduction

When you added a remote messaging server to the Message Network Configuration tree view, a corresponding prime switch location was added.

A remote prime switch location must be configured. This process is almost identical to configuring the local prime switch location.

Remote Prime Switch Location Properties dialog box

The remote prime switch location is configured on the Remote Prime Switch Location Properties dialog box, which has four tabs:

- General
- ESN
- CDP
- SMTP/VPIM

General tab

Completing the General tab is mandatory.

ESN tab

Complete the ESN tab if an ESN or hybrid dialing plan is used with this remote site.

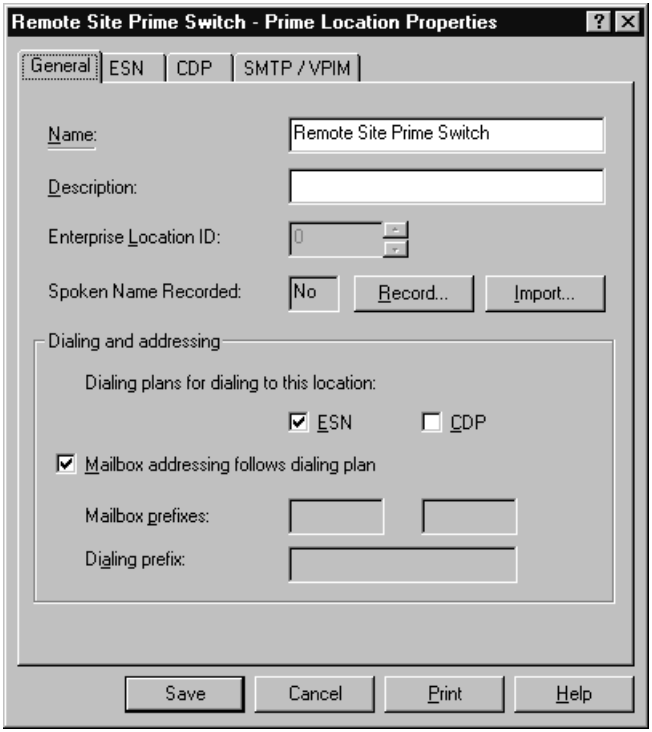
CDP tab

Complete the CDP tab if a CDP or hybrid dialing plan is used with this remote site.

SMTP/VPIM tab

Because your local site is using VPIM Networking to transfer messages with this remote site, must complete the SMTP/VPIM tab.

Remote Prime Switch Location Properties—General tab



Name

Assign a unique name to each switch location. The name should correspond to the switch location to make the location easy to identify. A street name or city name is a good choice.

The remote prime switch location is automatically given the name of the remote server that was added to the Messaging Network Configuration tree view. This name can be changed.

Description

Enter short notes or comments about the remote prime switch location in this box.

Enterprise Location ID

The Enterprise Location ID box is enabled only if Enterprise Networking is implemented on the local site.

A location ID is required for all remote sites if Enterprise Networking is installed locally, even if another protocol is used to exchange messages with this site.

The location ID of the remote prime switch location is set to 0 by default and cannot be changed.

Spoken Name Recorded

When local users compose a message to this remote site or use the playback feature to determine the sender of a message, they hear a message that identifies the sender. The content of the message depends on whether a spoken name for that remote site is recorded.

If a spoken name is recorded, voice mail users hear the location name followed by the local mailbox directory number.

Example: “Dallas, Mailbox 2346.”

Spoken name not recorded

If a spoken name is not recorded, local users hear a general message that does not identify the sender’s site by name.

For example, for an ESN switch location, users hear the ESN location prefix followed by the local mailbox directory number.

Example: “Mailbox 6444 2346.”

When a spoken name is not desirable

You may decide that you do not want local users to hear a spoken name for a particular remote site. For example, if CDP is used for messaging with this remote site and the mailbox numbers follow the dialing plan, you may decide that a recorded spoken name is unnecessary. In this case, do not record or import a spoken name.

Ways to add a spoken name recording

There are two ways to add a spoken name recording: record a spoken name directly by clicking the Record button, or import a prerecorded message.

Dialing plan information

Provide general information on the dialing plan used by the switch.

The dialing plan boxes have complex interactions. They are dynamically enabled or disabled depending on the choices made. Complete all enabled boxes.

Dialing plans for dialing to this location

You must specify which dialing plan is used to dial this remote switch location from the local switch location. There are four possible dialing plans:

- ESN
- CDP
- hybrid, combining ESN and CDP
- other (such as PSTN)

Mailbox addressing follows dialing plan

When a mailbox follows the dialing plan, a user dials and addresses a message to a recipient in the same way. There are two ways to achieve this correspondence:

- A user's mailbox number and extension number are the same.
- The addressing plan and the dialing plan are the same.

If either situation is true, select the Mailbox addressing follows dialing plan check box.

Clear this option if users at the site do not dial and address recipients in the same way.

Example: If the local ESN prefix is 6222 and the local mailbox is 1234, remote users can dial the local user with the numbers 62221234, which is the ESN prefix and the mailbox number combined.

Example: If the CDP steering code is 22 and the local mailbox is 1234, remote users can dial the local user with the number 221234, which is the steering code and the mailbox number combined.

Mailbox prefixes

Mailbox prefixes are used by users on other switches to address a message to users on the local switch.

A mailbox prefix must be provided if the mailbox does not follow the dialing plan or if another dialing plan, such as PSTN, is used.

A mailbox prefix does not have to overlap with local mailbox numbers. Two mailbox prefixes can be entered. Either prefix can be used to address any mailbox at the local site. Normally, however, only one prefix is required.

Usually, the mailbox prefix is a shortcut. A mailbox prefix can be any number as long as it does not conflict with other network data.

A mailbox prefix can also be the entire telephone number of the site, including country code, city/area code, and exchange.

Example: If the mailbox prefix is 22 and the mailbox number of a local user is 6565, users at other switches address the local user by dialing 226565.

Dialing prefix

A dialing prefix is needed if the local site uses another dialing plan, such as PSTN, and users at your local site use a dialing prefix to reach users at this remote location.

Usually, if the Dialing prefix box is enabled, you enter the prefix.

In a few cases, a dialing prefix is not needed. For example, if the mailbox number, with the mailbox prefix, can be dialed directly, a dialing prefix is not needed. This situation is rare because most systems use at least some sort of access code.

Dialing plan information required

The dialing plan boxes have complex interactions and are dynamically enabled and disabled depending upon choices made. Complete all enabled boxes.

Getting there Nortel SMI > Meridian Application Server > CallPilot > Networking > Messaging Network Configuration

To configure the remote prime switch location

1. In the Messaging Network Configuration tree view, select the remote prime switch location.
2. On the File menu, select Properties.

   Result: The Remote Prime Switch Location Properties dialog box appears.
3. On the General tab, in the Name box, enter the name of the remote prime switch location.
4. In the Description box, enter details about the switch location.

   Note: The Enterprise Location ID is always set to 0 for remote prime switch locations and cannot be changed.
5. If needed, click Record to record a spoken name for the site, or click Import to import a prerecorded spoken name.

   Note: For instructions on how to record a spoken name, see “Recording a spoken name” on page 189.

   For instructions on how to import a spoken name, see “Importing a spoken name” on page 192.
6. Specify the dialing plan used to dial this remote switch location. Select the

   - ESN check box if ESN is used
   - CDP check box if CDP is used
   - ESN and CDP check boxes if a hybrid dialing plan is used

   Note: Leave both check boxes clear if another dialing plan, such as PSTN, is used.
7. If the mailbox addressing follows dialing plan, select the Mailbox addressing follows dialing plan check box.
8. Complete the Mailbox prefixes boxes and Dialing prefix box if necessary.
9. Determine whether you must complete another tab. If not, click Save to close the dialog box.

ESN information

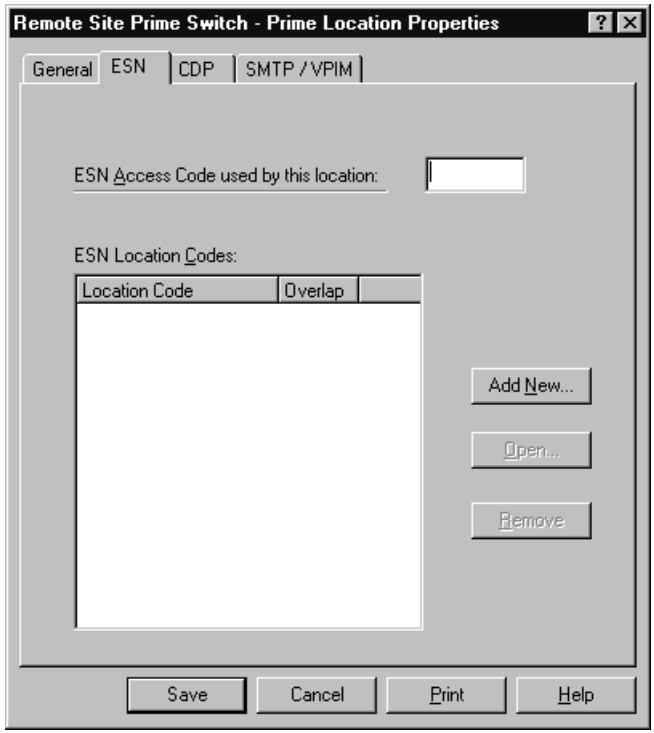
If the remote prime switch location uses an ESN or hybrid dialing plan, complete the ESN tab.

The procedure for configuring the ESN information for a remote prime switch location is identical to the procedure used for the local prime switch location.

For a review of the ESN access codes, ESN location codes, and overlap, consult “Configuring ESN information” on page 148.

To configure the ESN information

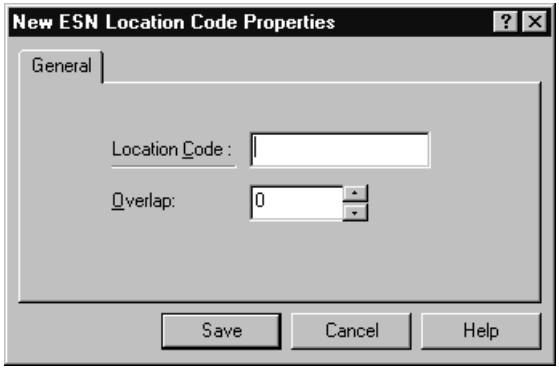
1 Open the Messaging Network Configuration—Remote Prime Switch Location Properties—ESN tab.



2 Enter the ESN access code.

3 To add a new location code, click the Add New button.

Result: The New ESN Location Code Properties dialog box appears.



4 In the Location Code box, enter the location code.

5 In the Overlap box, enter the number of digits in the mailbox number that overlap the location code.

6 Click Save.

Result: The location code and overlap are validated and appear in the ESN Location Codes box on the ESN tab.

7 Repeat steps 3–6 for each ESN location code required.

8 When you have finished configuring the ESN information, determine if you must configure CDP information. If yes, click the CDP tab. If no, click Save.

What's next?

If your remote prime switch location uses the hybrid dialing plan, click the CDP tab to continue configuring the local prime switch location.

If the local prime switch location uses only the ESN dialing plan, click Save to validate the configuration information and save it to the network database.

CDP information

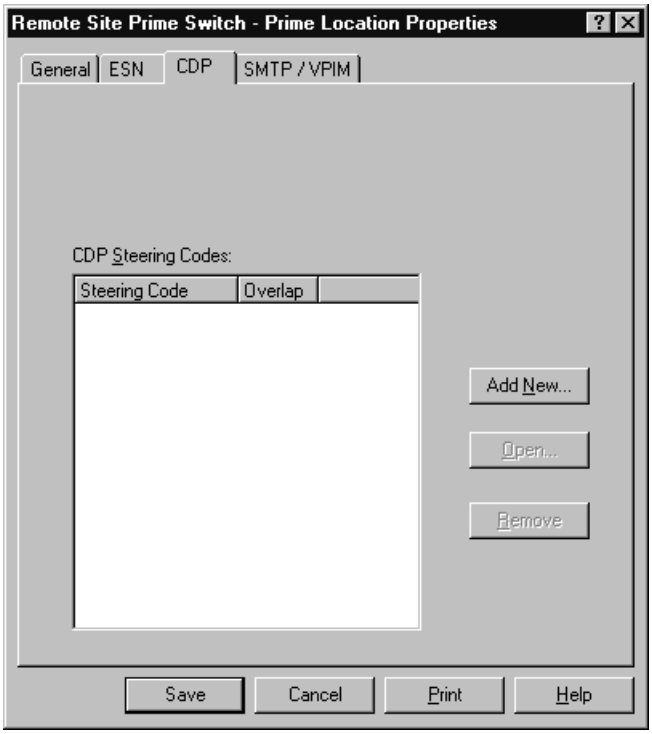
If a CDP dialing plan or a hybrid dialing plan is used to connect the local site to the remote site, complete the CDP tab.

Configuring the CDP information for a remote prime switch location is identical to configuring the local prime switch location.

For a review of the CDP steering codes and overlap, consult “Configuring CDP information” on page 152.

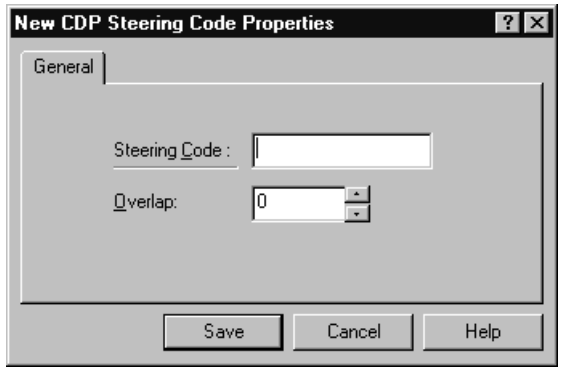
To configure the CDP information

1 Open the Messaging Network Configuration—Remote Prime Switch Location Properties—CDP tab.



2 Click the Add New button.

Result: The New CDP Steering Code Properties dialog box appears.



3 In the Steering Code box, enter the steering code.

4 In the Overlap box, enter the number of digits in the mailbox number that overlap the steering code.

5 Click Save.

Result: The steering code and overlap are validated and appear in the CDP Steering Codes box on the CDP tab.

6 Repeat steps 2–5 for each CDP steering code required.

7 When you have added all necessary CDP steering codes, click Save.

Result: The information is validated and saved to the network database.

What's next?

Click the VPIM tab to finish configuring the remote prime switch location.

VPIM information

To use VPIM Networking to exchange messages with the remote site, complete the VPIM tab.

Configuring the VPIM information for a remote prime switch location is identical to configuring the local prime switch location. See "Configuring VPIM information" on page 155.

For a review of SMTP/VPIM network shortcuts consult "How VPIM Networking works" on page 49.

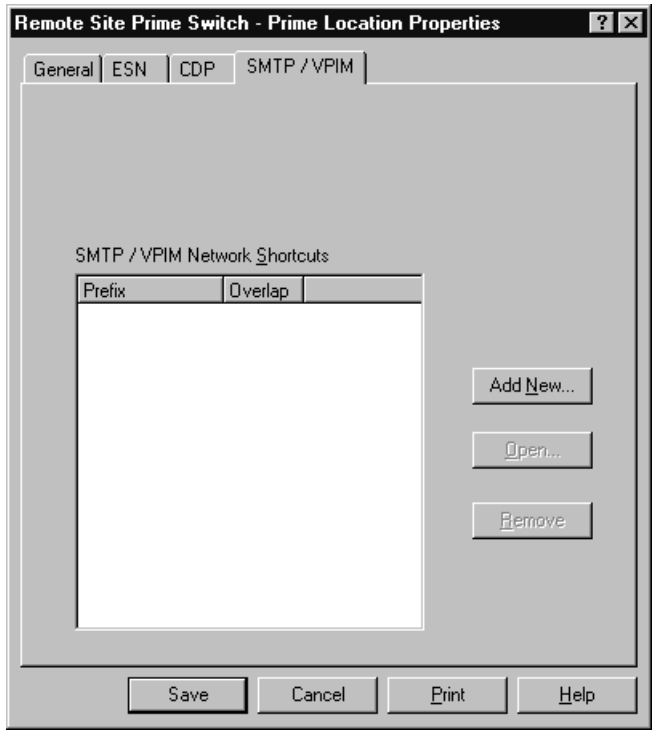
Relationship of SMTP/VPIM network shortcuts

The SMTP/VPIM network shortcuts that you enter for a remote site in your network database must correspond to the SMTP/VPIM network shortcuts that the remote site defines for itself in its network database.

There must be a correspondence because, when a message is received from a remote site, the message contains a From: entry in the message header that contains a SMTP/VPIM network shortcut for that site.

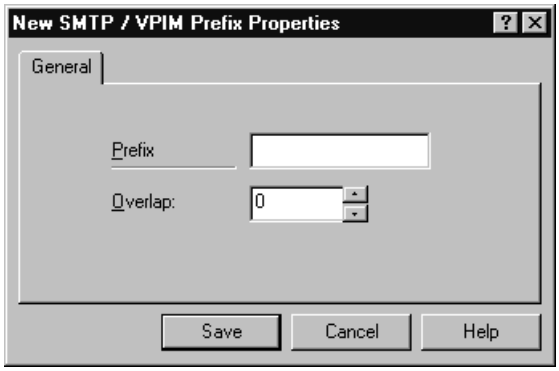
To configure the VPIM information

1 Open the Messaging Network Configuration—Remote Prime Switch Location Properties—SMTP/VPIM tab.



2 Click the Add New button.

Result: The New SMTP/VPIM Prefix Properties dialog box appears.



3 In the Prefix box, enter the SMTP/VPIM network shortcut in dialable, PSTN format.

Note: Only one SMTP/VPIM network shortcut is required.

4 In the Overlap box, enter the number of digits in the mailbox number that overlap the shortcut.

5 Click Save.

Result: The shortcut and overlap are validated and appear in the SMTP/ VPIM Network Shortcuts list box on the VPIM tab.

6 Repeat steps 2–5 for each network shortcut required.

7 When you have added all necessary SMTP/VPIM network shortcuts, click Save.

Result: The information is validated and saved to the network database.

Configuring a remote satellite switch location

Introduction

If a remote site is an NMS site, you must add and configure each of its satellite switch locations. This information is saved to the local network database.

Although a prime switch location is added automatically when a remote site is added to the Messaging Network Configuration tree view, you must manually add each satellite switch location of a remote NMS site.

Capacity

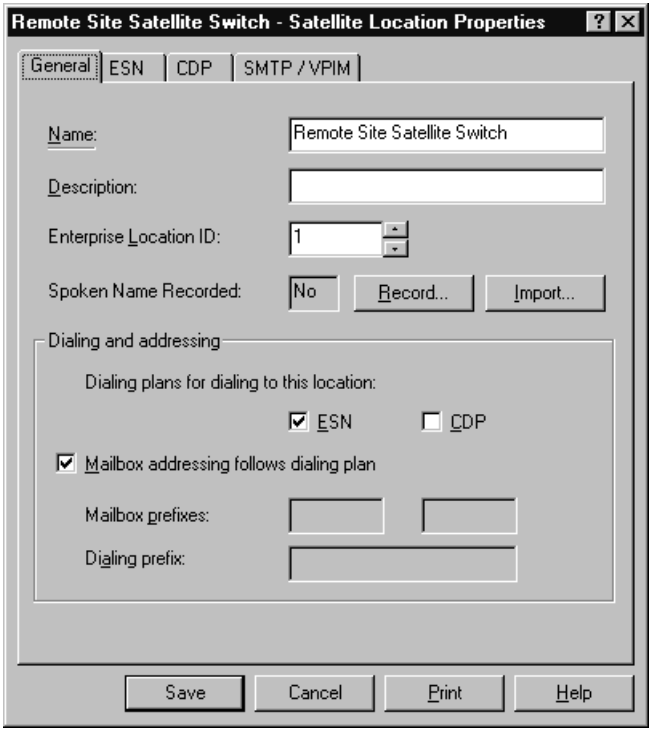
An NMS site can have up to 59 satellite switch locations.

Organization

When you add a satellite switch location, this location appears in the Messaging Network Configuration tree view. Satellite switch locations are listed alphabetically below the prime switch location.

Where to configure a satellite switch location

To configure a satellite switch location, complete the General tab of the Satellite Switch Location Properties dialog box.



You must also complete the tabs that correspond to the dialing plan used by the local site.

ESN tab

Complete the ESN tab if an ESN or hybrid dialing plan is used.

CDP tab

Complete the CDP tab if a CDP or hybrid dialing plan is used.

SMTP/VPIM tab

Because your local site is using VPIM Networking to transfer messages with this remote site, complete the SMTP/VPIM tab.

Spoken Name Recorded

When local users compose a message to a remote satellite switch location or use the playback feature to hear who sent a message, the name of the switch location is played.

If a spoken name is not recorded, local users hear the full DN, such as “Mailbox 64441234.” If a recording of the spoken name is available, local users hear the switch location name followed by the mailbox number, such as “Milan 1234.” You can either record a message using the telephone or import a prerecorded WAV file.

When a recording of the spoken name is available, Yes appears in the Spoken Name Recorded box.

If you do not want your local users to hear the name of this satellite switch location when composing messages or using playback, do not record a message. For example, if you are using CDP to transfer messages to the site and mailbox numbers follow the dialing plan, you may feel that a spoken name is unnecessary.

Dialing plan interaction

The dialing plan boxes are dynamically enabled or disabled depending on the choices made. Complete all enabled fields.

SMTP/VPIM network shortcuts

Specify SMTP/VPIM network shortcuts for the satellite switch location on the SMTP/VPIM tab.

Every satellite switch location must have unique SMTP/VPIM network shortcuts, because the shortcuts are used to identify the locations.

Every satellite switch location must have at least one SMTP/VPIM network shortcut. Every VPIM network shortcut must be unique within the messaging network.

See also

Configuring a satellite switch location for a remote site is identical to configuring a remote prime switch location for a remote site.

For a review, consult “Configuring a remote prime switch location” on page 171.

Getting there Nortel SMI > Meridian Application Server > CallPilot > Networking > Messaging Network Configuration

To configure a remote satellite switch location

1. On the Messaging Network Configuration tree view, highlight the remote messaging server.
2. On the File menu, select New > Switch location.

   Result: The Satellite Switch Location Properties dialog box appears.
3. Complete the General tab.

   Note: For detailed instructions on how to record a spoken name, see “Recording a spoken name” on page 189. For detailed instructions on how to import a spoken name, see “Importing a spoken name” on page 192.
4. Complete the ESN tab, the CDP tab, and the SMTP/VPIM tab as required.
5. Click Save.

   Result: The information is validated and the satellite switch location is added to the remote site.
6. Repeat steps 1–5 for each satellite switch location required.
7. When all satellite switch locations are added, click Save to save them to the Messaging Network Configuration tree view.

Recording a spoken name

Introduction

You can create a recording of the name of a switch location. A recorded name is heard by a local user whenever an address is played back. A recorded name for a site is played if a user does not have a personal recorded name.

Local switch location

If your local site is not an NMS site, a spoken name is not required for the local site.

If your local site is an NMS site, you can decide if you want to record a spoken name. For example, if the NMS site uses CDP, you may decide a spoke name is not necessary.

Remote switch location

A spoken name should be available for every remote site in your Message Delivery Configuration tree view.

The recording is played when local users compose messages to the remote site.

Importing a spoken name

If you do not want to record your own voice using the telephone, you can import a prerecorded WAV file. See “Importing a spoken name” on page 192.

Before you begin

You need a telephone to serve as a microphone.

Getting there Nortel SMI > Meridian Application Server > CallPilot > Networking > Messaging Network Configuration

To record a spoken name

1. In the Messaging Network Configuration tree view, select the switch location of the site for which you want to record a spoken name.
2. On the File menu, select Open.

   Result: The Switch Location Properties dialog box appears.
3. On the General tab, click Record.

   Result: The Specify Phoneset dialog box appears.

4. Enter the telephone number of the telephone to be used as a microphone and click Dial.

   Result: The telephone rings and the Voice Recorder dialog box appears.
5. Answer the telephone.
6. In the Voice Recorder dialog box, click Record.
7. Speak the name of the site into the telephone.
8. Click Stop.

9 To review the recording, click Play.

10 If you are satisfied with the recording, click Done.

Importing a spoken name

Introduction

You can import a prerecorded file of the name of a switch location. The recording is heard by a local user whenever an address is played back. A recording for a site is played if a user does not have a personal spoken name.

Local switch location

If your local site is not an NMS site, a spoken name is not required for the local site.

If your local site is an NMS site, you can decide if you want to import a spoken name. For example, if the NMS site uses CDP, you may decide a spoken name is not necessary.

Remote switch location

A spoken name should be available for every remote site in your Message Delivery Configuration tree view.

The recording is played when local users compose messages to the remote site.

Recording a spoken name

If you do not want to import a prerecorded spoken name, you can record your own voice message using the telephone. See “Recording a spoken name” on page 189.

Before you begin

A prerecorded WAV file must be available. Check the quality of the recording before importing the file.

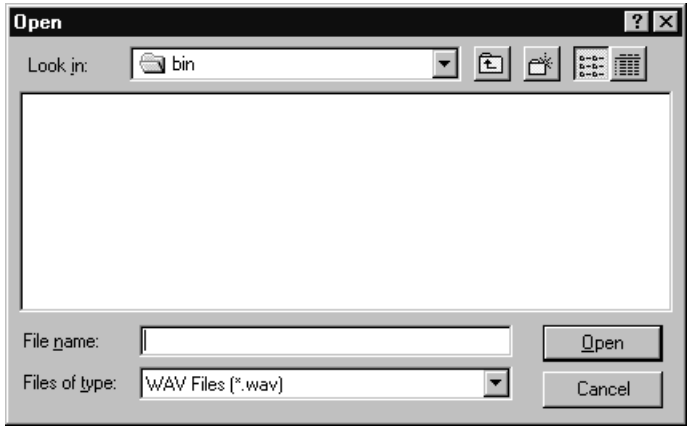
Getting there Nortel SMI > Meridian Application Server > CallPilot > Networking > Messaging Network Configuration

To import a prerecorded file

1. In the Messaging Network Configuration tree view, select the switch location of the site for which you want to import a prerecorded file.
2. On the File menu, select Open.

   Result: The Switch Location Properties dialog box appears.
3. On the General tab, click Import.

   Result: The Open dialog box appears.



4. Select the WAV file, and click Open.

   Result: The file is imported.
5. Close the Open dialog box.

Non-CallPilot remote sites

Introduction

VPIM Networking can exchange messages between a CallPilot system and the following non-CallPilot remote systems:

- a Meridian Mail (Release 11 or later) system through a Meridian Mail Net Gateway (Release 1 or later) system
- a Norstar Voice Mail (Release 3 and later) system
- VPIM-compliant systems from other vendors

Coordination

If a remote site is a non-CallPilot system, you must coordinate with the network administrator of that remote site to ensure that the systems are properly configured. You must share the standard information that is required between any sites in a messaging network.

Example

The two sites must coordinate dialing plans and ensure that there are no conflicts in the configuration information.

Adding and configuring the remote site

Adding a non-CallPilot remote site to the local network database is exactly the same as adding a CallPilot remote site.

To configure the non-CallPilot remote site, you require no special information. You must only specify the server type on the Remote Messaging Server dialog box. The rest of the configuration is the same as the configuration of a CallPilot remote site.

Server type

Specify the server type of a non-CallPilot system on the Messaging Network Configuration—Remote Server Properties—General tab.

Instructions for the remote administrator

For both Meridian Mail and Norstar Voice Mail systems, no special instructions must be communicated to the remote network administrator.

The remote administrator adds the CallPilot site to the remote network database like any other remote site. No special configuration is required.

Meridian Mail remote sites

Introduction

CallPilot can use VPIM Networking to exchange voice messages with a Meridian Mail system through a Meridian Mail Net Gateway system. Fax and text messages are not supported.

If a remote site is a Net Gateway system, you must coordinate with the network administrator of that site to ensure that the systems are properly configured.

Most of the coordination involves standard information that is required between any sites in a messaging network. For example, you need to coordinate your dialing plans and Enterprise site IDs.

Net Gateway sites that support VPIM messages use the internal dialing plan for VPIM shortcuts. For example, a Net Gateway site that uses the ESN location code 338 has a shortcut, 6338.

Special coordination

Some coordination is not typical, and you may need to work with the remote administrator of the Net Gateway site to ensure that configuration is correct.

Net Gateway supports the Meridian Mail Remote Voice User Propagation feature. This feature is equivalent to the CallPilot Names Across the Network feature.

VPIM Networking does not support Names Across the Network. Therefore, when the remote administrator of the Net Gateway site adds your site to that network database.

- The Remote Voice User Propagation option must be turned off.

- The Entrust encryption option for your site must be turned off.
- The remote administrator must describe your site as “Another” system.

Norstar Voice Mail remote sites

Introduction

CallPilot can use VPIM Networking to exchange messages with Norstar Voice Mail systems.

If a remote site is a Norstar system, you must coordinate with the network administrator of that site to ensure that the systems are properly configured.

The coordination involves standard information that is required between any sites in a messaging network, for example, site names and dialing plan information.

Instructions for the remote Norstar administrator

There are no special instructions for the remote Norstar administrator.

The CallPilot site is added to the network database like any other site.

Norstar does not support ESN or CDP dialing plans. Typically, a Norstar site is configured to use another dialing plan and has a mailbox prefix defined.

Norstar supports voice, fax, and text messages.

VPIM-compliant third-party systems

Introduction

VPIM Networking uses industry standards and can exchange messages with VPIM-compliant third-party systems.

However, there may be special restrictions or considerations.

Confirm compliance and compatibility

Consult the documentation of the third-party system to determine if there are any special configuration considerations or restrictions in functionality.

Determine how the third-party system must be configured to exchange messages with your site.

Confirm the capabilities enabled on the third-party system to ensure that features are available.

See also

For a review of VPIM conformance specifications, consult AppendixA, “VPIM conformance”.

chapter 6

Testing and backing up VPIM Networking

This chapter describes how to test the configuration of VPIM Networking. The test suite ensures that VPIM Networking is working properly both locally and with remote sites.

This chapter also describes how to create a backup of your system to ensure that the configuration is not lost due to system failure.

In this chapter

Tests and backups

In this section

VPIM Networking test suite

Introduction

After implementing VPIM Networking, test the system to ensure that it is working properly.

The VPIM Networking test suite determines if the local site is correctly configured and if the local site can exchange messages with remote sites.

Perform the tests in sequence. If any test in the suite fails, resolve the problem before continuing with the tests.

Note: These tests are not intended to validate the VPIM compliance of a third-party system. It is assumed that any system you communicate with is compliant.

Test suite

The VPIM Networking test suite consists of three tests.

This test	Determines if
connectivity test	there is connectivity between sites.
loopback test	messages can be exchanged with other sites in the messaging network.
telnet test	the outgoing mail server is operational.

Before you begin

You must work with the remote network administrators at each remote site.

Review each test before beginning. Ensure that the preliminary requirements for each test are met.

Connectivity test

Introduction

Packet Internet Groper (ping) is a utility that is used to test TCP/IP networks and the Internet. The ping test, or pinging, determines if there is connectivity between sites.

Pinging

At its simplest, pinging consists of sending a message and waiting for its echo to be bounced back.

You ping another computer on a data network to ensure that it can be reached from your computer.

Pinging has several functions, including troubleshooting and testing a data network.

A series of ping tests should be performed when you set up VPIM Networking.

Getting there Windows NT > Start > Program > Command Prompt

To perform the ping test

1. In the MS-DOS window, at the prompt, enter the following command:

   ping <destinationFQDN>

2. Check the results of the ping test.

Evaluating results

The ping test is successful if you receive a reply to the message.

The test is not successful if you receive a request timed out message. This message indicates that there is no connection or a bad connection between sites.

The test is not successful if you receive an invalid FQDN message. This message indicates that an invalid IP address was entered.

If the test is not successful

If you do not receive a response, check the destination FQDN and perform the test again. If you receive no response a second time, ping another server FQDN. If you receive a response from this site, it is possible that there is a problem with the host that you originally tried to contact.

Loopback test

Introduction

The loopback test verifies that messages can be sent from a local site to a remote site, and returned to the local site.

The loopback test is performed with every remote site with which the local site exchanges VPIM messages.

The loopback test consists of composing and sending a message to the loopback mailbox on a remote site. The loopback mailbox automatically returns the message to the originator.

Before you begin

Before performing a loopback test, ensure a loopback mailbox exists on every remote site to be tested.

Ask each remote network administrator for the loopback mailbox number. If a loopback mailbox is not available, any mailbox on the remote system can be used. In this case, the message must be replied to manually from the remote system. Ask for help from the remote administrator to complete this test.

To perform the VPIM Loopback test

1. Log in to CallPilot.
2. Press **75** to compose a message.
3. Enter the network address of the remote site.
4. Record the message.

   Note: Tag the message as urgent.
5. Press **79** to send the message.
6. Wait for your Message Waiting Indicator (MWI) to activate.

   Note: The MWI indicates that the message was successfully returned. This may take several minutes.
7. Log in and listen to the message.
8. Log out of the system.

Evaluating results

The test is successful if you hear the message that you recorded.

The message is not successful if you receive a non-delivery notification.

If the test is not successful

If the VPIM loopback test fails or produces unexpected results, do the following:

- Confirm the loopback mailbox number with the remote administrator.
- Perform the test again.
- If still unsuccessful, consult the Operational Measurement reports to determine the following:
  - Is the remote site operational?
  - Are both sites configured to use VPIM Networking to exchange messages?

Telnet test

Introduction

The telnet test determines if an outgoing server is operational. If the local site uses an outgoing server for VPIM Networking, you must be able to telnet to this server. If the local site does not use an outgoing server, you must be able to telnet the server for each remote site.

Getting there Windows NT > Start > Programs > MS-DOS

To perform the telnet test

1 At the prompt, enter the following:

telnet <server FQDN> <port number>

Note: In most instances, the port number is 25. Change the port number if necessary.

2 Press Enter.

Result: The Telnet window opens.

3 Check the results.

- `220 <message>` indicates a successful test
- `421 <message>` indicates the server is currently busy. Try the test again.
- A warning box with a connection failure message indicates there may be problems with the server.

4 After completing the test, close the MS-DOS window.

Backing up VPIM Networking

Introduction

When all tests of the system are successfully completed and VPIM Networking is working properly, perform a backup.

The backup ensures that the configuration is not lost due to a system failure.

Backup schedule

Perform backups as part of the implementation process and as part of regular maintenance activities.

Implementation backup

Perform a manual backup as the final step in the VPIM Networking implementation process. This backup is needed even if the system is configured to perform an automatic backup.

In the unlikely event that the system experiences a disk failure before the automatic backup takes place, the network configuration could be lost.

Maintenance backup

Perform a backup whenever VPIM Networking configuration information is modified.

System backup components

A system backup consists of two parts:

- a switch backup
- a CallPilot backup

Switch backup

For detailed instructions on how to perform a switch backup, consult your switch documentation.

CallPilot backup

You can perform a full or partial backup of your CallPilot server.

For detailed instructions on performing a CallPilot backup, consult the relevant section in the *Advanced Administration Guide*.

chapter 7

Maintaining VPIM Networking

After you complete the VPIM Networking implementation, you only need to perform regular maintenance.

This chapter describes the maintenance procedures that must be performed regularly. The chapter also describes maintenance procedures that are performed on an as-required basis, such as when there are changes at sites in the messaging network.

In this chapter

About maintaining VPIM Networking

In this section

Overview

Introduction

After VPIM Networking is successfully implemented and tested, it requires maintenance.

There are two types of maintenance tasks:

- regularly scheduled tasks
- as-required tasks

Regularly scheduled tasks

Regularly scheduled tasks include

- checking the network status
- reviewing Operational Measurement (OM) reports

Although you can perform regularly scheduled tasks at any time, they should be performed at least once a week. Because these tasks do not interfere with the normal operation of VPIM Networking, you can schedule them for a convenient time.

If you monitor the performance of your messaging network, you avoid future problems. Careful monitoring shows bottlenecks in the system and indicates how the system can be improved.

Monitoring can also help in planning and forecasting future requirements.

As-required tasks

Perform as-required tasks as needs arise. These tasks include

- adding additional shortcuts
- disabling and enabling VPIM Networking
- modifying settings

- adding or deleting remote sites from the network database

ATTENTION! Because as-required tasks may affect the performance of the entire system, they must be carefully scheduled for off-peak hours.

Perform a backup following maintenance

If an as-required task involves a change in the network configuration, perform a backup of the system.

Network history

Introduction

Keep detailed records of your network's history. These records can

- Indicate significant performance or equipment issues that real-time monitoring cannot detect.
- Provide a background for comparing with the current information.
- Help future system administrators who need information about growth, equipment, maintenance, and system configuration changes.
- Provide information needed during support calls.

Information to record

A network history typically includes the following types of information:

- installation dates and descriptions
- contact information for all key personnel involved in system installation and configuration
- details of software installed on the messaging server, including versions
- installation progress and results, including tests
- diagrams of the initial and subsequent messaging networking configurations
- any problems encountered and their solutions
- hardware and software changes
- current configuration information
- changes to the messaging network configuration

Records should be easy to access and read. Graphics, including hand-drawn sketches, can be very useful.

Where to keep the records

Records for each site in a network should be kept in one location. They can be kept in a log or online. Note, however, that online records cannot be accessed if the system fails.

The information contained in your network is valuable and should be safely stored. In the wrong hands, this information might result in the loss of system integrity.

See also

For a detailed description of messaging network histories, consult the *Networking Planning Guide*.

Printing configuration information

Introduction

Printouts of the system configuration are often included in a network history. You can print all configuration information contained in your local network database.

Note: The tree view of the messaging network contained in the Messaging Network Configuration dialog box cannot be printed.

When to print configuration information

Although configuration information is always available in the most recent backup of your network database, you may find it convenient to make printouts as well.

Printouts of the configuration information are especially useful in the following situations:

- You must fax information to a remote network administrator.
- You are keeping a network history.
- You are planning to change a configuration or delete an item from the Messaging Network Configuration tree view and want a hard copy of the original configuration.

Getting there Nortel SMI > Meridian Application Server > CallPilot > Networking > Message Delivery Configuration or Messaging Network Configuration

To print configuration information

1. Open the dialog box that contains the information to be printed.
2. With the dialog box open, click the Print button.

   Result: The content of the dialog box, including all tabs, is printed.

Regularly scheduled maintenance tasks

In this section

Reviewing OM reports and alerts

Introduction

Operational Measurement (OM) reports and alerts provide detailed information on the status and performance of VPIM Messaging.

Open Networking Activity report

The Open Networking Activity report provides information on AMIS Networking and VPIM Networking activity with open sites. The VPIM Networking statistics are combined with AMIS Networking statistics to open sites if AMIS Networking is implemented.

Networking Activity report

The Networking Activity report provides summary information on network message traffic to sites within the messaging network. The report identifies the protocol used to exchange messages with each remote site.

Failed Networking Sessions alert

The Failed Networking Sessions alert is triggered when the number of networking session failures exceeds a threshold percent of total attempts.

Review schedule

Although you can review OM reports at any time, you should review them at least weekly.

Access to OM reports is restricted

The generation of OM reports is a restricted activity that is determined by access level. If you do not have the necessary access, you must ask your system administrator to generate the reports.

See also

For additional information on reports and alerts, including how to generate and interpret them, consult the *Reporter Guide*.

As-required maintenance tasks

In this section

Overview

Introduction

As-required maintenance tasks are performed only when necessary.

Typical as-required maintenance tasks include

- clearing a disk full condition
- modifying the configuration of the local site
- adding a remote site to the messaging network
- deleting a remote site from the messaging network
- modifying the configuration of a remote site
- disabling and enabling the messaging network

Maintenance coordination

Most as-required maintenance tasks must be coordinated with the network administrators of the remote sites.

Changes that you make to the local site configuration must be communicated to all remote sites. These changes must be reflected in the remote network databases.

Similarly, if the configuration of a remote site is changed, these changes must be communicated to you. You must make the changes in your local network database.

Coordination must be timely

Coordination among the sites in the messaging network must also be timely. All network databases must correspond with one another, or VPIM Networking cannot work properly.

Clearing a disk full condition

Introduction

VPIM Networking messages consume more system memory resources than those of other networking solutions. Under some circumstances, especially during periods of intense usage, the hard disk may become full.

Impact of a disk full condition

If the hard disk of the Meridian Application Server cannot store anymore messages, VPIM Networking is shut down.

When a disk full condition occurs,

- Incoming messages, in any protocol, are not delivered to local mailboxes.
- Outgoing VPIM Networking messages are not delivered to remote destinations, because temporary disk space is required for message conversions.

To clear a disk full condition

Ask users to remove all unnecessary messages from their mailboxes.

If this does not create sufficient free space, manually clear old messages from the disk.

See also

For a detailed discussion of the disk full condition and ways to avoid it, consult the *Maintenance and Diagnostics Guide*.

Disabling and enabling VPIM Networking

Introduction

You may need to disable VPIM Networking sometimes. When you disable VPIM Networking, users cannot compose, send, or receive VPIM messages.

You might disable VPIM Networking to

- Prevent system abuse.
- Clear the system of undeliverable messages that are using up system resources.

When VPIM Networking is disabled, messages sent with other networking solutions are still permitted. Each messaging solution is disabled and enabled independently.

Degrees of disabling

There are three degrees of disabling VPIM Networking:

- disabling outgoing VPIM Networking messages
- disabling incoming VPIM Networking messages
- disabling both outgoing and incoming VPIM Networking messages

Disabling outgoing VPIM Networking messages

When outgoing messages are disabled, the local system cannot send messages using VPIM Networking to open addresses or integrated addresses. However, the system can still receive incoming VPIM Networking messages.

Disabling incoming VPIM Networking messages

When incoming messages are disabled, the local system cannot receive messages using VPIM Networking from open addresses or integrated addresses. However, the system can still send outgoing VPIM Networking messages.

Disabling both outgoing and incoming VPIM Networking messages

When both outgoing and incoming messages are disabled, the local system cannot send or receive messages using VPIM from open addresses or integrated addresses.

ATTENTION!

Disabling VPIM Networking may affect desktop users with IMAP clients. If your site uses IMAP, review the settings carefully.

Messages sent while system is disabled

When you disable outbound VPIM Networking, your local users can continue to compose and send messages. The messages composed by your local users are held in queue until the option is enabled or the message becomes stale.

When you disable the Incoming SMTP/VPIM networking check box, messages from remote systems are rejected. The remote system that sends the message is informed of the status, and messages are not accepted. The way the remote system handles this information depends on the system. For example, if the remote system is CallPilot, the sender receives a non-delivery notification that states that the system of the intended recipient is not accepting messages. VPIM-compliant systems from other vendors may handle this scenario differently.

Getting there Nortel SMI > Meridian Application Server > CallPilot > Networking > Message Delivery Configuration > SMTP/VPIM tab

To disable and enable AMIS Networking

1 Do the following:

IF you want to	THEN
disable your system from receiving VPIM messages	clear the Incoming VPIM Networking check box.
disable your system from sending VPIM messages	clear the Outgoing VPIM Networking check box.
enable your system to receive VPIM messages	select the Incoming VPIM Networking check box.
enable your system to send VPIM messages	select the Outgoing VPIM Networking check box.

2 To save your settings, click Save.

When to disable a remote site

Disable a remote site if

- The remote site is being modified.
- There are problems with the switch network that are affecting a particular remote site.
- The system at the remote site is down because of hardware problems or a system upgrade.
- The remote site is in error status and you are trying to determine why.
- The site is being removed from the messaging network.

Impact of disabling a remote site

Disabling a remote site prevents any messages from being delivered to that site. However, messages can still be delivered to other remote sites.

Messages sent to a disabled remote site remain in the message queue until the site is enabled or the message becomes stale.

Adding, modifying, and deleting VPIM open shortcuts

Introduction

To keep the exchange of VPIM Networking messages to open sites operating optimally, keep the list of VPIM open shortcuts up-to-date.

Add VPIM open shortcuts for all frequently addressed open sites. Changes to the details of a shortcut should be reflected in the shortcut list promptly. Shortcuts that are no longer used should be removed.

User needs determine shortcuts

The VPIM open shortcuts list is largely determined by the telephone users at your local site. Users who address open sites from the desktop do not need VPIM open shortcuts.

Telephone users need shortcuts to address a message to an open site. When they know of an open site, they will request that it be added to the list.

See also

For a review of how VPIM open shortcuts work, consult “Message delivery parameters—SMTP/VPIM tab” on page 119.

Getting there Nortel SMI > Meridian Application Server > CallPilot > Networking > Message Delivery Configuration > SMTP/VPIM tab

To add a VPIM open shortcut

1. Select the Add New button.

   Result: The VPIM Open Shortcut dialog box appears.

2. Enter the shortcut and the domain name.

3. Click Save.

   Result: The information is validated and saved to the network database. The new shortcut appears in the VPIM Open Shortcuts list box.

To modify a VPIM open shortcut

1. In the VPIM Open Shortcuts list, select the shortcut to be modified.
2. Click Open.

   Result: The VPIM Open Shortcut dialog box appears.
3. Modify the shortcut and domain information as required.
4. Click Save.

   Result: The information is validated and saved to the network database. The modified shortcut appears in the VPIM Open Shortcuts list.

To delete a VPIM open shortcut

1. In the VPIM Open Shortcuts list, select the shortcut to be deleted.
2. Click Remove.

   Result: A confirmation message appears.
3. To delete the shortcut, click OK.

   To keep the shortcut, click Cancel.
4. Click Save.

   Result: The information is validated and saved to the network database. The deleted shortcut no longer appears in the VPIM Open Shortcuts list.

Modifying the local site configuration

Introduction

Over time, it may be necessary to modify the configuration of the local site.

Before you begin

Before modifying the configuration, print out all configuration information that will be affected.

This printout becomes part of your network history. It is used if the modification is incorrect and you must return to the original configuration.

Communicate modifications

When you modify the configuration of the local messaging server or a local switch location, whether prime or satellite, communicate the modifications to all remote network administrators.

All remote network administrators must reflect your modifications in their network databases. If you make changes independently, the messaging network will not perform correctly.

Further information

Configuration modifications are made on the properties dialog box where the initial configuration was done. To review the configuration of any setting, consult the instructions for the initial implementation.

To review the settings on this Properties dialog box	Consult
Local Messaging Server	“Configuring the local messaging server” on page 137.
Local Prime Switch Location	“Configuring the local prime switch location” on page 142.

To review the settings on this Properties dialog box	Consult
Local Satellite Switch Location	"Configuring an NMS local site" on page 159. *NMS Implementation and Administration Guide*

Getting there Nortel SMI > Meridian Application Server > CallPilot > Networking > Messaging Network Configuration

To modify the configuration of the local site

1. From the Messaging Network Configuration tree view, select the item to be modified: local messaging server, local prime switch location, or local satellite switch location.
2. On the File menu, select Properties.

   Result: The Properties dialog box of the selected item appears.
3. Make all necessary modifications.
4. Click Save.

   Result: The information is validated and saved to the network database.
5. Repeat steps 1–4 for all items to be modified.
6. When all modifications are complete, click Close.

Add, modify, or delete a remote site

Introduction

As your messaging network grows and changes, you may need to add or delete a remote site, or to modify the configuration of an existing site.

It is important for all network administrators to keep their network databases up-to-date.

Before you begin

Before adding, modifying, or deleting a remote site, print out all configuration information that will be affected.

Add a remote site

When a site is added to the messaging network, all sites add it to their Messaging Network Configuration tree view. The remote network administrator must provide the information needed to add and configure a remote site.

Modify a remote site

The configurations of both the messaging server and the switch locations can be modified as needs change. For example, if a remote site upgrades its system, you must modify its configuration information in your network database.

Note: The information in your network database must reflect the actual configuration of the remote site. The remote network administrator is responsible for informing you of all necessary changes.

Delete a remote site

When a site is removed from the messaging network, all sites must delete it from their Messaging Network Configuration tree view.

Impact on network database

Any additions, modifications, or deletions to remote sites are reflected in your network database. For this reason, the VPIM Networking tests should be performed again and a backup should be performed.

Locating an item in the tree view

Introduction

It can be difficult to locate a particular remote site, messaging server, or switch location in the Messaging Network Configuration tree view in a large messaging network.

There are two ways to locate an item in a large messaging network:

- Scroll through the alphabetized list.
- Use the Find feature.

Getting there Nortel SMI > Meridian Application Server > CallPilot > Networking > Messaging Network Configuration

To locate an item using Find

1. On the File menu, select Find.

   Result: The Find dialog box appears.

2. Enter the name of the item to be located, and press the Find button.

   Result: The located item is highlighted in the Messaging Network Configuration tree view.

Modifying a remote site configuration

Introduction

The configuration of a remote site can be modified as needed.

Further information

Configuration modifications are made on the properties dialog box where the initial configuration was made. To review the settings, consult the instructions for the initial configuration.

To review the settings on this Properties dialog box	Consult
Remote Messaging Server	“Configuring a remote messaging server” on page 163.
Remote Prime Switch Location	“Configuring a remote prime switch location” on page 171.
Remote Satellite Switch Location	“Configuring a remote satellite switch location” on page 185.

Impact of modifications

Modifying the configuration of a remote system can affect the networking service between the remote site and your local site. Modifications to the following settings are especially important:

- site ID
- dialing plans
- message transfer protocol

Enterprise Site IDs

Do not change the remote Enterprise Site ID unless the administrator at the remote site notifies you of a change in that ID, or if the ID is incorrect.

If you change the site ID to an invalid number by mistake, the system is unable to send or receive messages from the site.

Dialing plans

Do not change the dialing plan unless the dialing plan on the switch is changed.

Network protocol

Do not change the network protocol unless all network administrators who use the protocol agree to the change.

For example, suppose the local site was originally configured to use Integrated AMIS Networking to exchange messages with a remote site. However, the remote site has decided to implement VPIM Networking and can now use VPIM Networking to exchange messages with your site. In this instance, the message transfer protocol has changed.

Getting there Nortel SMI > Meridian Application Server > CallPilot > Networking > Messaging Network Configuration

To modify the configuration of a remote site

1. In the Messaging Network Configuration tree view, select the remote messaging server or switch location to be modified.
2. On the File Menu, select Open.

   Result: The Properties dialog box for the selected item opens.
3. Make all required modifications.
4. Click Save.
5. Repeat steps 1–4 for all items in the tree view that must be modified.

After modifications are complete

Modifications to the configuration of a remote site must be tested. Complete the test suite to ensure that the modifications are working properly.

When you are satisfied that your system is working properly, perform a backup.

Deleting items from the tree view

Introduction

The Messaging Network Configuration tree view contains all the sites in your messaging network. A site always consists of a messaging server and a prime switch location. A site may also include satellite switch locations.

The messaging server, the prime switch location, and any satellite switch locations are listed in the tree view.

Sites and satellite switch locations are deleted from the Messaging Network Configuration tree view.

Note: You cannot delete the local site. You can delete local satellite switch locations.

ATTENTION!

When an item is deleted from the Messaging Network Configuration tree view, it is permanently removed from the local network database. The information cannot be recovered. For this reason, it is strongly recommended that you print out the complete configuration of all items to be deleted. If an item is accidentally deleted, you can use the printed information to add the item again.

Multi-administrator environments

If several administrators maintain your local network database ensure that your version of the Messaging Network Configuration tree view is up-to-date. The Messaging Network Configuration tree view is updated when it is initially opened. An open tree view is not updated when another administrator makes changes.

To check the status of the view

To see if another administrator has made changes to the Messaging Network Configuration tree view, on the View menu, click Refresh.

Getting there Nortel SMI > Meridian Application Server > CallPilot > Networking > Messaging Network Configuration

To delete a remote site

1. Print the configuration details of the site to be deleted.
2. Open the folder of the remote site to see the messaging server, prime switch location, and any satellite switch locations.
3. In a multi-administrator environment, on the View menu, click Refresh.
4. Highlight the messaging server of the site to be deleted.
5. Select File > Delete.

   Result: A confirmation box appears asking if you really want to delete the site from your local network database.
6. To delete the site, click OK.

   Tip: You can also delete a highlighted remote site by clicking the Delete button.

Deleting several remote sites at once

If you must delete several remote sites from the local network database, you may find it more efficient to delete them all at once instead of individually.

To delete several remote sites at once

1. Print the configuration details of all sites to be deleted.
2. Highlight all the remote sites to be deleted.

   Tip: To select more than one item in the tree view, press Ctrl and right-click the mouse.
3. Select File > Delete.

   Result: A confirmation message appears.
4. Click OK to delete the items. Click Cancel to keep the items.

Deleting a satellite switch location

If there are changes to an NMS site, you can delete one or more satellite switch locations from the local site or from any remote sites.

If a satellite switch location is removed from an NMS site, is must also be removed from the local network database.

To delete a satellite switch location

1. Print the configuration details of the satellite switch location.
2. In a multi-administrator environment, on the View menu, click Refresh.
3. Highlight the satellite switch location to be deleted.
4. On the File menu, click Delete.
5. Select File > Delete.

   Result: A confirmation message appears.
6. Click OK to delete the item. Click Cancel to keep the item.

Modifying dialing plan information

Introduction

After you establish a dialing plan, you rarely modify it. Modifications to a dialing plan affect users and may require considerable relearning of the system.

However, if modifications are necessary, they are usually guided by changes made by the switch technician. These changes can be local or remote.

Switch changes

If any changes to the dialing plan are made on a switch, the network databases of the sites in the messaging network must reflect these changes. If changes are made locally, ensure that all remote sites are notified.

To modify the dialing plan information

If you need to modify the dialing plan, follow the general instructions to modify the local and remote sites.

Modifying CDP steering codes

Modifications to the CDP steering codes are more complicated. For a detailed review of how to plan for and implement changes, consult Chapter 4, “Dialing plans and networking,” in the *Networking Planning Guide*.

chapter 8

Troubleshooting VPIM Networking

Although testing and regular maintenance ensure that VPIM Networking is working properly, the system may experience occasional problems.

This chapter describes how to diagnose and correct these problems.

In this chapter

Troubleshooting

In this section

Overview

Introduction

Troubleshooting a messaging network can be complicated. To simplify the task, use a systematic approach. The following table explains an approach that you can apply to troubleshooting.

Step	Action
Step 1	Define the problem clearly. Collect all symptoms.
Step 2	Gather information about the problem.
Step 3	Determine possible causes. Attempt to narrow the possible causes.
Step 4	Create a plan of action. Always begin with the most likely cause. The plan should focus on manipulating one variable at a time. For example, instead of changing all message delivery parameters at once, change just one and then test the system again.
Step 5	Work through the action plan. Whenever possible, test the system to see if the problem is solved. Gather information for all changes in your network history.
Step 6	If the problem is corrected, ensure that any additional actions are completed. For example, if you have to inform remote network administrators of any changes, contact them immediately. If the problem is not corrected, create another plan of action that is based on the next most likely cause.
Step 7	If you are unable to solve the problem, contact your technical support representative. Make sure you have detailed information about the problem and the solutions you have attempted to solve it and their results. For example, if you have performed tests, have the results.

Hardware problems

If you are unable to locate the problem in the CallPilot configuration, your system may be experiencing hardware problems that are not related to networking.

Perform a basic hardware check. Examine all connections.

Troubleshooting basics

Introduction

Most problems have simple causes that are easily missed. When troubleshooting always:

- Check all cables and connections.
- Check the error messages in the Event Browser.
- Check users' mailbox capabilities.

Error code range

VPIM Networking errors have the following ranges:

- Message Transfer Agent (MTA) errors: 54100–54199
- Internet Mail Agent (INA) errors: 54800–54899

TCP/IP troubleshooting

Introduction

Problems with the TCP/IP data network affect the performance of VPIM Networking.

This discussion is intended as a brief introduction to TCP/IP troubleshooting. For more detailed information, consult your local data network administrator.

Main steps

There are two steps to troubleshooting:

1. Ensure that you can ping successfully.
2. Ensure that you can establish a session with a host.

Definition: Ping

The ping utility measures the time that it takes for a packet of information to travel from one host to the next.

To ping

1 Ping the loopback address (127.0.0.1) to verify that TCP/IP was installed and loaded correctly.

Note: If this step is unsuccessful, check your TCP/IP installation.

2 Ping your IP address to verify that it was configured correctly.

Note: If this step is unsuccessful, check the configuration in the Network program of the Control Panel.

Check the following:

a. Address is entered correctly.

b. IP address is valid.

c. IP address follows addressing guidelines.

3 Ping the IP address of the default gateway to verify that the gateway is functioning and configured correctly.

Note: If this step is unsuccessful, check that the IP address is correct.

4 Ping the IP address of a remote host to verify the connection to the data network.

If this step is unsuccessful, do the following:

a. Ensure IP routing is enabled.

b. Verify that the IP address of the default gateway is correct.

c. Ensure the remote host is functional.

d. Verify that the link between routers is operating.

Messages are not delivered

Introduction

Sometimes messages sent with VPIM Networking are not delivered. There are several causes of messages that are not delivered.

However, before you assume that a message is not delivered, attempt to determine its status.

Determine if messages are not delivered

You must first determine if messages are actually not delivered.

On occasion, a message transmitted over the Internet can take several days to reach its destination. Determine when the message was sent before concluding that the message is not delivered.

A receiving system can be configured to not send confirmation of receipt notifications. Therefore, if you tag a message for acknowledgment, you may not receive an acknowledgment.

The routers that handle the message as it is transmitted over the Internet may be unable to handle certain message types, including acknowledgments and non-delivery notifications.

Not receiving a non-delivery notification should not be taken as evidence that a message is delivered. If a non-delivery notification is generated by a remote site, the routers that handled the message as it was transmitted back to the originator may not handle the message type correctly. It is possible for telephone users not to receive a non-delivery notification because of this format incompatibility.

If you suspect that messages are not delivered but need to confirm their status, you may need to contact the recipients directly.

appendix A

VPIM conformance

This appendix provides a detailed conformance table.

In this appendix

VPIM profile

In this section

VPIM-compliant messaging systems requirements

Introduction

To be considered VPIM-compliant, a messaging system must meet certain requirements.

Number of recipients and message length

The VPIM standard does not restrict the number of recipients in a single message. It also does not limit the maximum message length. The limitations of disk storage will affect the accepted message length.

However, CallPilot does have restrictions. CallPilot cannot deliver a message body that is longer than 120 minutes. This length is also affected by the limitations of disk storage.

Mail relays may also impose restrictions on message length.

Date and time stamps

The originating VPIM Networking system uses the date and time stamp passed from MC. If the time zone environment variable (TZ) is configured in Windows NT, VPIM Networking includes the time zone offset and time zone name when constructing the string.

The receiving system accepts time stamps and discards any time zone offset or time zone name fields. They are discarded because CallPilot treats time stamps as the originator's local time, so conversion to the recipient's local time is not required.

Voice encoding

To exchange messages between CallPilot and a VPIM-compatible system, G.726 voice encoding is used.

VPIM Version 2 conformance

To claim conformance and be recognized as VPIM-compliant, a messaging system must implement all mandatory features in the areas of content and transport. In addition, systems that conform to this profile must not send messages with features beyond this profile unless explicit per-destination configuration of these enhanced features is provided.

For a listing of VPIM features with which VPIM Networking complies, see the following table.

VPIM Version 2 conformance table

Introduction

VPIM Networking conforms to the VPIM Version 2 specifications established by the Internet Engineering Task Force (IETF). The conformance table that follows indicates what functionality a messaging system must support to be considered VPIM-compliant. This table also indicates CallPilot support for these requirements.

Conformance table description

The conformance table has the following columns:

- Feature: Name of the protocol feature.
- Area: Conformance area to which each feature applies.
  - C = content
  - T = transport
  - N = notification
- Status: Whether the feature is mandatory, optional, or prohibited. Five degrees of status are used in this table:
  - Must = mandatory
  - Should = encouraged optional
  - May = optional
  - Should not = discouraged optional
  - Must not = prohibited
- Nortel: CallPilot VPIM Networking compliance with the feature is marked with an X. Features ignored when messages are received are marked with an I.

Conformance table

Feature	Area	Must	Should	May	Should not	Must not	Nortel
Message addressing formats							
Use DNS host names	C	X					X
Use only numbers in mailbox IDs	C		X				X
Use alphanumeric mailbox IDs	C			X			
Support of postmaster@domain	C	X					X
Support of non-mail-user@domain	C		X				X
Support of distribution lists	C		X				
Message header fields: Encoding outbound messages							
From	C	X					X
From: addition of text name	C		X				X
To	C	X					X
CC	C		X				
Date	C	X					X
Sender	C			X			
Return-path	C			X			
Message ID	C	X					X
Reply to	C			X			

Feature	Area	Must	Should	May	Should not	Must not	Nortel
Received	C	X					X
MIME Version 1.0 (Voice 2.0)	C		X				X
Content-type	C	X					X
Content-transfer encoding	C	X					X
Sensitivity	C			X			X
Importance	C			X			X
Subject	C		X				X
Disposition-notification-to	N			X			
Other headers	C			X			X
Message header fields: Detection and decoding inbound messages							
From	C	X					X
From: utilize text personal name	C			X			X
To	C	X					X
CC	C			X			I
Date	C	X					X
Date: conversion of date to local time	C		X				
Sender	C			X			I
Return-path	C			X			I
Message ID	C	X					X

Feature	Area	Must	Should	May	Should not	Must not	Nortel
Reply to	C	X					X
Received	C			X			I
MIME Version 1.0 (Voice 2.0)	C			X			I
Content type	C	X					X
Content-transfer encoding	C	X					X
Sensitivity	C	X					X
Importance	C			X			X
Subject	C			X			X
Disposition-notification-to	N			X			
Other headers	C	X					I
Message content encoding: Encoding outbound audio/fax contents							
7bit MIME	C					X	
8bit MIME	C					X	
Quoted printable	C					X	
Base64	C	X					X
Binary	C		X				
Message content encoding: Detection and decoding inbound messages							
7bit MIME	C	X					X
8bit MIME	C	X					X
Quoted printable	C	X					X
Base64	C	X					X

Feature	Area	Must	Should	May	Should not	Must not	Nortel
Binary	C	X					X
Message content types: Inclusion in inbound messages							
Multipart/voice message	C	X					X
Message/RFC822	C			X			X
Application/directory	C		X				X
Application/directory: include TEL, EMAIL	C	X					X
Application/directory: include N, ROLE, SOUND, REV	C		X				X
Application/directory: only one per level	C	X					X
Audio/32KADPCM	C	X					X
Audio/32KADPCM: content-description	C			X			X
Audio/32KADPCM: content-disposition	C	X					X
Audio/32KADPCM: content-duration	C			X			X
Audio/32KADPCM: content-language	C			X			
Audio/* (other encodings)	C			X			X
Image/TIFF	C			X			
Multipart/mixed	C			X			X
Text/plain	C				X		X

Feature	Area	Must	Should	May	Should not	Must not	Nortel
Multipart/report	N	X					X
Multipart/report: human-readable part is voice	N	X					
Message/delivery status	N	X					X
Message/disposition-notification	N		X				
Other contents	C				X		X
Message content types: Detection and decoding in inbound messages							
Multipart/voice message	C	X					X
Message/RFC822	C	X					X
Application/directory	C		X				X
Application/directory: recognize TEL, EMAIL	C	X					X
Application/directory: recognize N, ROLE, SOUND, REV	C		X				X
Audio/32KADPCM	C	X					X
Audio/32KADPCM: content description	C			X			I
Audio/32KADPCM: content disposition	C		X				X
Audio/32KADPCM: content duration	C			X			X
Audio/32KADPCM: content language	C			X			I

Feature	Area	Must	Should	May	Should not	Must not	Nortel
Image/TIFF	C		X				X
Image/TIFF: send NDN if unable to render	C	X					X
Audio/* (other encodings)	C			X			X
Multipart/mixed	C	X					X
Text/plain	C	X					X
Text/plain: send NDN if unable to render	C	X					X
Multipart/report	N	X					X
Multipart/report: human-readable part is voice	N	X					X
Message/delivery status	N	X					X
Message/disposition-notification	N		X				
Other contents	C				X		X
Other contents: send NDN if unable to render	N		X				X
Forwarded messages: use message/RFC822 construct	C		X				X
Forwarded messages: simulate headers if none available	C		X				X
Reply messages: send to reply-to, else From address	C	X					X

Feature	Area	Must	Should	May	Should not	Must not	Nortel
Reply messages: always send error on non-delivery	C	X					X
Notifications: use multipart/ report format	N	X					
Notifications: always send error on non-delivery	C		X				
Message transport protocol: ESMTP commands							
HELO	T	X					X
MAIL FROM	T	X					X
MAIL FROM: support null address	T	X					X
RCP To	T	X					X
DATA	T	X					X
TURN	T					X	X
QUIT	T	X					X
RSET	T	X					X
VRFY	T						
EHLO				X			X
BDAT (5)	T		X				
Message transport protocol: ESMTP keywords and parameters							
PIPELINING	T		X				
SIZE	T	X					X
CHUNKING	T		X				

Feature	Area	Must	Should	May	Should not	Must not	Nortel
BINARYMIME	T		X				X
NOTIFY	N	X					X
ENHANCED STATUSCODES	N		X				
RET	N		X				X
ENVID	N			X			X
Message transport protocol: ESMTP-SMTP downgrading							
Send delivery report upon downgrade							
Directory address resolution							
Provide facility to resolve addresses	C		X				X
Use Vcards to populate local directory	C	X					X
Use headers to populate local directory	C				X		X
Management protocols							
Network management	T		X				

Field index

N

O

P

R

S

V

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

R

S

T

U

V

CallPilot

VPIM Networking Implementation and Administration Guide

Information is subject to change without notice. Nortel Networks reserves the right to make changes in design or components as progress in engineering and manufacturing may warrant.

The process of transmitting data and call messaging between the CallPilot server and the switch or system is proprietary to Nortel Networks. Any other use of the data and the transmission process is a violation of the user license unless specifically authorized in writing by Nortel Networks prior to such use. Violations of the license by alternative usage of any portion of this process or the related hardware constitutes grounds for an immediate termination of the license and Nortel Networks reserves the right to seek all allowable remedies for such breach.

Publication number:	555-7101-306
Product release:	2.5
Document release:	Standard 1.0
Date:	October 2003

NORTEL NETWORKS™