555-7101-102

CallPilot

Network Planning Guide

Product release 3.0 | Standard 1.0 | November 2004

NORTEL NETWORKS™

CallPilot

Network Planning Guide

Publication number:	555-7101-102
Product release:	3.0
Document release:	Standard 1.0
Date:	November 2004

Copyright © 2004 Nortel Networks. All Rights Reserved.
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.

This page is considered the title page, and contains Nortel Networks and third-party trademarks.

Nortel Networks, the Nortel Networks logo, the Globemark, and Unified Networks, BNR, CallPilot, DMS, DMS-100, DMS-250, DMS-MTX, DMS-SCP, DPN, Dualmode, Helmsman, IVR, MAP, Meridian, Meridian 1, Meridian Link, Meridian Mail, Norstar, SL-1, SL-100, Succession, Supernode, Symposium, Telesis, and Unity are trademarks of Nortel Networks.

3COM is a trademark of 3Com Corporation.

ADOBE is a trademark of Adobe Systems Incorporated.

ATLAS is a trademark of Quantum Corporation.

BLACKBERRY is a trademark of Research in Motion Limited.

CRYSTAL REPORTS is a trademark of Seagate Software Inc.

EUDORA and QUALCOMM are trademarks of Qualcomm, Inc.

ETRUST and INOCULATEIT are trademarks of Computer Associates Think Inc.

DIRECTX, EXCHANGE.NET, FRONTPAGE, INTERNET EXPLORER, LINKEXCHANGE, MICROSOFT, MICROSOFT EXCHANGE SERVER, MS-DOS, NETMEETING, OUTLOOK, POWERPOINT, VISUAL STUDIO, WINDOWS, WINDOWS MEDIA, WINDOWS NT, and WINDOWS SERVER are trademarks of Microsoft Corporation.

GROUPWISE and NOVELL are trademarks of Novell Inc.

INTEL is a trademark of Intel Corporation.

LOGITECH is a trademark of Logitech, Inc.

MCAFEE and NETSHIELD are trademarks of McAfee Associates, Inc.

MYLEX is a trademark of Mylex Corporation.

NETSCAPE COMMUNICATOR is a trademark of Netscape Communications Corporation.

NOTES is a trademark of Lotus Development Corporation.

NORTON ANTIVIRUS and PCANYWHERE are trademarks of Symantec Corporation.

QUICKTIME is a trademark of Apple Computer, Inc.

RADISYS is a trademark of Radisys Corporation.

ROLM is a trademark of Siemens ROLM Communications Inc.

SLR4, SLR5, and TANDBERG are trademarks of Tandberg Data ASA.

SONY is a trademark of Sony Corporation.

SYBASE is a trademark of Sybase, Inc.

TEAC is a trademark of TEAC Corporation.

US ROBOTICS, the US ROBOTICS logo, and SPORTSTER are trademarks of US Robotics.

WINZIP is a trademark of Nico Mark Computing, Inc.

XEON is a trademark of Intel, Inc.

Publication history

November 2004 Standard 1.0 issue of the CallPilot 3.0 *Network Planning Guide*

Contents

1 About this Guide 9

Overview . . . 10
How this guide is organized . . . 10
Related information sources . . . 11
Logging on to the CallPilot server with CallPilot Manager . . . 15
Multi-administrator access . . . 17

2 Getting started 19

About networking and networking protocols 20

Overview . . . 20
Network setup . . . 21
Messaging Protocols . . . 22
Analog and digital messaging protocols . . . 23

Messaging networks 25

Networks and messaging . . . 25
Network database . . . 26
Integrated and open sites . . . 27

3 Understanding CallPilot networking solutions 29

About CallPilot networking solutions 30

Overview . . . 30
AMIS Networking . . . 32
Integrated AMIS Networking . . . 32
Enterprise Networking . . . 33
VPIM Networking . . . 33
Network Message Service . . . 34
Combining networking solutions . . . 35
Connections . . . 35
Networking software options . . . 36

Messaging networks and users 38

Overview . . . 38
Message types supported . . . 38
Message lengths . . . 39
Telephone users and desktop users . . . 41
Teaching users how to use networking . . . 41
Non-delivery notifications . . . 43

Features 44

Overview . . . 44
Enhancements to Meridian Mail capabilities . . . 45
Migration from Meridian Mail . . . 46

Networking and other features 47

Overview . . . 47
Shared Distribution Lists (SDL) . . . 47
Personal Distribution Lists (PDL) . . . 48
Names Across the Network (NAM) . . . 48
System trigger mailboxes . . . 49

Networking solution considerations **50**
Overview . . . 50
General messaging network considerations . . . 50
AMIS Networking features . . . 51
Integrated AMIS Networking features . . . 53
Enterprise Networking features . . . 55
VPIM Networking features . . . 58
Network Message Service (NMS) features . . . 60
NMS dialing restriction scenarios . . . 62

Transmission times and traffic calculations **64**
Overview . . . 64
Message transmission times for analog protocols . . . 64
Transmission times for messages containing text information . . . 66
Transmission times for messages with Names Across the Network . . . 67
Traffic considerations for VPIM Networking messages . . . 67

Remote users **68**
Overview . . . 68
Temporary remote users . . . 69
Permanent remote users . . . 70
How remote users are added or deleted . . . 70
Adding remote users with Names Across the Network . . . 71

4 Dialing plans and networking **75**

About dialing plans and networking solutions **76**
Overview . . . 76
Uniform dialing plans . . . 77
Nonuniform dialing plans . . . 78
ESN dialing plan . . . 80
CDP . . . 82
Hybrid dialing plan—ESN and CDP combined . . . 85
Another dialing plan . . . 85
Dialing plans and addressing plans . . . 85
Modifying dialing plan information . . . 86
Modifying CDP steering codes . . . 87

Dialing plan information **89**
Gathering dialing plan information . . . 89
Create a messaging network representation . . . 89
Examples of messaging network diagrams . . . 90

5 Network and location-specific broadcast messages **95**
Types of network broadcasts . . . 95
Broadcast message addresses . . . 98
User capabilities for broadcast messages . . . 99
CallPilot server capabilities for broadcast messages . . . 100
Broadcast messages in a mixed messaging network . . . 102
Viewing or printing all broadcast addresses . . . 104

6 About Network Message Service **105**
Overview . . . 105
Dialing plans and NMS . . . 109
Implementing NMS . . . 111
NMS time zone conversions . . . 115

7 About VPIM Networking 119

Overview . . . 119
Sending VPIM Networking messages to other sites . . . 121
Receiving VPIM Networking messages . . . 122
TCP/IP . . . 125
TCP/IP protocols . . . 127
Implementation overview . . . 128
VPIM-compliant messaging systems requirements . . . 130
VPIM Version 2 conformance table . . . 131

8 CallPilot networking implementation concepts 139

About implementing networking 140
Overview . . . 140
Designing the messaging network . . . 142
Installation and implementation concepts . . . 145

Key concepts 147
Network views . . . 147
Performing local and remote administration . . . 147
Multi-administrator environments . . . 148

CallPilot Manager networking configuration pages 149
Message Delivery Configuration description . . . 149
Message Network Configuration description . . . 151
Working with the Message Network Configuration page . . . 153
Validation . . . 154
Ensuring information is unique . . . 155
Specifying time periods . . . 156

Coordination among sites 157
Coordinating network information . . . 157
Networking requirements and considerations . . . 158

9 Gathering information 161

Overview . . . 161
Data network information . . . 162
Switch information . . . 163
Information required from switch . . . 164
Evaluating the switch information . . . 166
Information from other sites . . . 166

10 Implementing & configuring CallPilot networking 167

Overview . . . 167
Configuring the switch using phantom DNs . . . 170
Configuring CallPilot . . . 171
SDN Table and message networking . . . 171
Implementing message networking . . . 175
Message Delivery Configuration parameters . . . 176
AMIS message delivery configuration . . . 178
Enterprise message delivery configuration . . . 183
VPIM message delivery configuration . . . 184

11 Configuring local and remote networking sites 191

Overview . . . 191
Configuring the local messaging server . . . 192
Configuring the local prime switch location . . . 195
Adding and configuring a remote site . . . 200
Configuring a remote messaging server . . . 200
Configuring a remote prime switch location . . . 207
Configuring a remote satellite switch location . . . 210

12 Security and encryption 211

Networking and security 212

Overview . . . 212
Open AMIS Networking and security . . . 212
VPIM Networking and security . . . 213
Switch security and networking . . . 216

SMTP security 217

Overview . . . 217
Unauthenticated mode . . . 219
Authenticated mode . . . 220
Mixed authentication mode . . . 221
SMTP authentication methods . . . 222
Authentication failures . . . 224
Enabling CallPilot SMTP authentication . . . 227
Configuring unauthenticated access restrictions . . . 227
Monitoring suspicious SMTP activity . . . 227

Encryption 230

CallPilot encryption description . . . 230
How CallPilot encryption works . . . 231
Implementing encryption on CallPilot . . . 233

A Appendix: Implementation and planning tools 235

Overview . . . 236
Section A: Implementation checklists . . . 238
Section B: Configuration worksheets . . . 248

B Appendix: How AMIS and Enterprise Networking handle messages 261

Networking messages . . . 261
MTA and ANA . . . 262
What the MTA does . . . 263
What the ANA does . . . 264
Example of message handling with AMIS Networking . . . 266

Index 269

chapter 1

About this Guide

In this chapter:

Overview 10

How this guide is organized 10

Related information sources 11

Logging on to the CallPilot server with CallPilot Manager 15

Multi-administrator access 17

Overview

The *Networking Planning Guide* is your key to CallPilot networking. It should be read before any networking solution is implemented. The guide provides an overview of key concepts and terminology necessary to implement a messaging network. It introduces all of the networking solutions offered with CallPilot and describes specific feature interactions. It also explains the process that you follow to implement one or more networking solutions.

For actual procedural instructions to perform a specific task, you must refer to the CallPilot Manager online Help files. Topics are indexed and the system also contains extensive context-sensitive Help information.

How this guide is organized

The *Networking Planning Guide* provides an overview of key CallPilot concepts and terminology. This guide is designed to help you to understand and implement a messaging network.

Contents

The *Networking Planning Guide* is organized into the following chapters:

Chapter title	Description
Chapter 1, About this Guide	This chapter describes this guide and how to log on to the CallPilot Manager.
Chapter 2, Getting started	This chapter introduces networking and networking protocols. It also describes the key concepts necessary to understand messaging networks.
Chapter 3, Understanding CallPilot networking solutions	This chapter describes each the networking solutions, their features, and how they work.
Chapter 4, Dialing plans and networking	This chapter describes each dialing plan supported by CallPilot. This chapter also describes how to create a network representation using the dialing plan information.
Chapter 5, Network and location-specific broadcast messages	This chapter provides an overview of the CallPilot network broadcast feature and the types of network broadcasts available.
Chapter 6, About Network Message Service	This chapter provides an overview of the CallPilot's Network Message Service (NMS) feature that enables messaging services to users in a network of compliant switches.
Chapter 7, About VPIM Networking	This chapter provides an overview of the CallPilot's VPIM Networking capabilities.
Chapter 8, CallPilot networking implementation concepts	This chapter provides an overview of how networking solutions are implemented. This chapter stresses the importance of organizing all sites in the messaging network and coordinating information.

Chapter title	Description
Chapter 9, Gathering information	This chapter describes how to gather the information required to implement message networking. This chapter provides a checklist for all information that is needed about the switch configuration.
Chapter 10, Implementing & configuring CallPilot networking	This chapter provides implementation and configuration information required for CallPilot's networking solutions.
Chapter 11, Configuring local and remote networking sites	This chapter describes how to configure the local messaging server and prime switch location. It also explains how to add and configure remote messaging servers and switch locations.
Chapter 12, Security and encryption	This chapter provides an overview of security and encryption as they apply to CallPilot networking.
Appendix A, Implementation and planning tools	This appendix provides checklists and worksheets that you can use while setting up your messaging network.
Appendix B, How AMIS and Enterprise Networking handle messages	This appendix describes the roles of the Message Transfer Agent (MTA) and Analog Networking Agent (ANA) in the handling of messages via AMIS and Enterprise networking.

Related information sources

The 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 application
- My CallPilot application
- 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.

Product guides

The CallPilot documentation suite is organized into six categories to provide specific information for the various personnel involved in implementing and/or using CallPilot. The categories are as follows:

Fundamentals

The Fundamentals category contains the CallPilot Fundamentals Guide, which is the primary initial reference for the CallPilot product.

Planning and Engineering

The Planning and Engineering guides are used to help plan your system and networks before you install CallPilot, or to plan a migration of data from Meridian Mail to CallPilot.

Installation and Configuration

The Installation and Configuration guides describe how to install the following:

- CallPilot server hardware and software
- Desktop Messaging and My CallPilot software

Administration

The Administration guides provide specialized information to help you configure administer and maintain CallPilot, and use its features. Guides for ancillary applications (Reporter and Application Builder) are also included.

Maintenance

The Maintenance section provides maintenance and diagnostics guides for the specific supported server types. Also included is the *CallPilot Troubleshooting Guide,* which describes symptoms that can appear on all CallPilot server platforms, and describes ways to resolve them.

End User information

The End User Information category contains documents required by CallPilot users, such as telephone set users and Desktop Messaging users. Specific guides are included for various desktop applications, as well as a host of printable quick reference cards.

CallPilot Documentation Map

The entire documentation suite is shown on the CallPilot Customer Documentation map.

For a thumbnail summary of each document in the suite, refer to the *CallPilot Fundamentals Guide*. Summaries are organized on a personnel task basis (i.e. installers, administrators, end users, etc.), making it easy to identify the particular guide you require.

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

NORTEL NETWORKS

CallPilot Customer Documentation Map

NTP Number 555-7101-(nnn)

- **Fundamentals**
  - CallPilot Fundamentals (-010)
- **Planning and Engineering**
  - Planning and Engineering Guide (-101)
  - Network Planning Guide (-102)
  - Data Networking for Voice over IP (553-3001-160)
- **Installation and Configuration**
  - Installation and Configuration Task List (-210)
  - **Server Installation Guides**
    - 201i Server Hardware Installation (-220)
    - 703t Server Hardware Installation (-226)
    - 1002rp Server Hardware Installation (-205)
  - **Configuration and Testing Guides**
    - Meridian 1 and CallPilot Server Configuration (-222)
    - Succession 1000 System and CallPilot Server Configuration (-510)
  - **Unified Messaging Software Installation**
    - Desktop Messaging and MyCallPilot Installation Guide (-505)
- **Administration**
  - Administrator's Guide (-301)
  - Software Administration and Maintenance Guide (-202)
  - Desktop Messaging and MyCallPilot Administration Guide (-503)
  - Meridian Mail to CallPilot Migration Guide (-801)
  - Application Builder Guide (-325)
  - Reporter Guide (-310)
- **Maintenance**
  - Troubleshooting Guide (-501)
  - **Server Maintenance and Diagnostics**
    - 201i Server Maintenance and Diagnostics (-119)
    - 703t Server Maintenance and Diagnostics (-227)
    - 1002rp Server Maintenance and Diagnostics (-206)
- **End User Information**

End User Cards	End User Guides
Unified Messaging Quick Reference Card	Multimedia Messaging User Guide
Unified Messaging Wallet Card	Speech Activated Messaging User Guide
Command Comparison Card A-Style	Desktop Messaging User Guide for Microsoft Outlook
Command Comparison S-Style	Desktop Messaging User Guide for Lotus Notes
Menu Interface Quick Reference Card	Desktop Messaging User Guide for Novell Groupwise
Alternate Command Interface Quick Reference Card	Desktop Messaging User Guide for Internet Clients
	MyCallPilot User Guide

Online resources

CallPilot administration online Help

The CallPilot Manager and CallPilot Reporter software contain administration and procedural 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.

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 Nortel Networks distributor’s technical support organization to get help with troubleshooting your system.

Logging on to the CallPilot server with CallPilot Manager

You must use a web browser to log on to and administer the CallPilot server.

ATTENTION CallPilot Manager can be installed on the CallPilot server or on a stand-alone server. If CallPilot Manager is installed on a stand-alone server, you must know the CallPilot Manager server host name or IP address, as well as the CallPilot server host name or IP address.

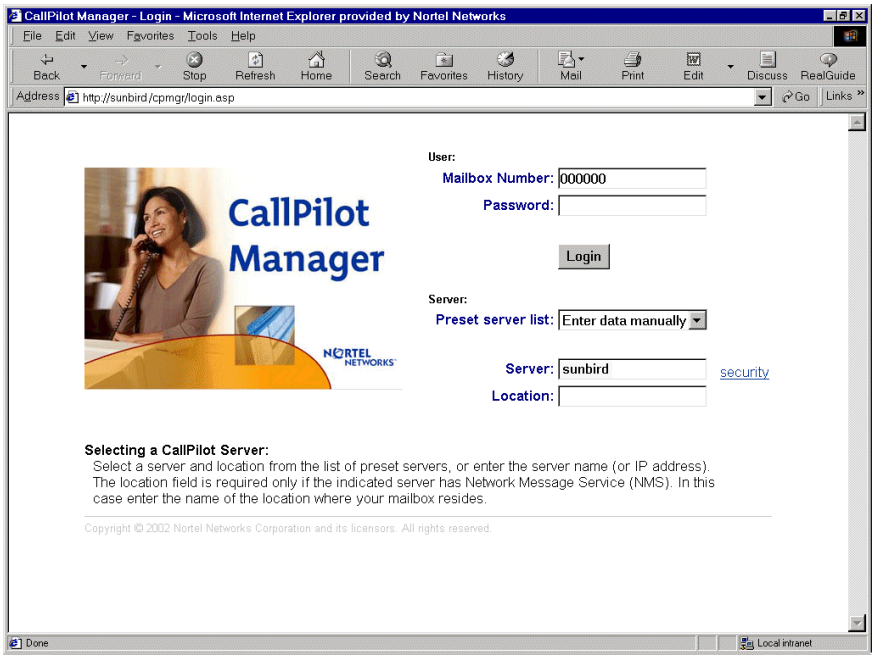
To log on to CallPilot Manager

1 Launch the web browser on a PC or on the CallPilot server.

2 Type the CallPilot Manager web server URL in the Address or Location box of the web browser, and then press Enter.

Example: http://sunbird/cpmgr/

Result: When the connection is established, the CallPilot Manager Logon screen appears.



Note: The URL automatically appears as http://<*web server host name or IP address*>/cpmgr/login.asp.

3 Type the administration mailbox number and password.

The supplied administrator mailbox number is **000000**. The default password is **124578**.

4 Do one of the following:

- If connection information has been pre-configured, you can select a server or location from the Preset server list box.
- Type the CallPilot server host name or IP address in the Server box.
- If the CallPilot server you are connecting to has Network Message Service (NMS) installed, type the CallPilot server's host name or IP address in the Server box, then type the name of the switch location on which the administration mailbox resides in the Location box.

- If you are using Microsoft Internet Explorer, you can reuse information you entered during a prior session on the same PC. Do the following:

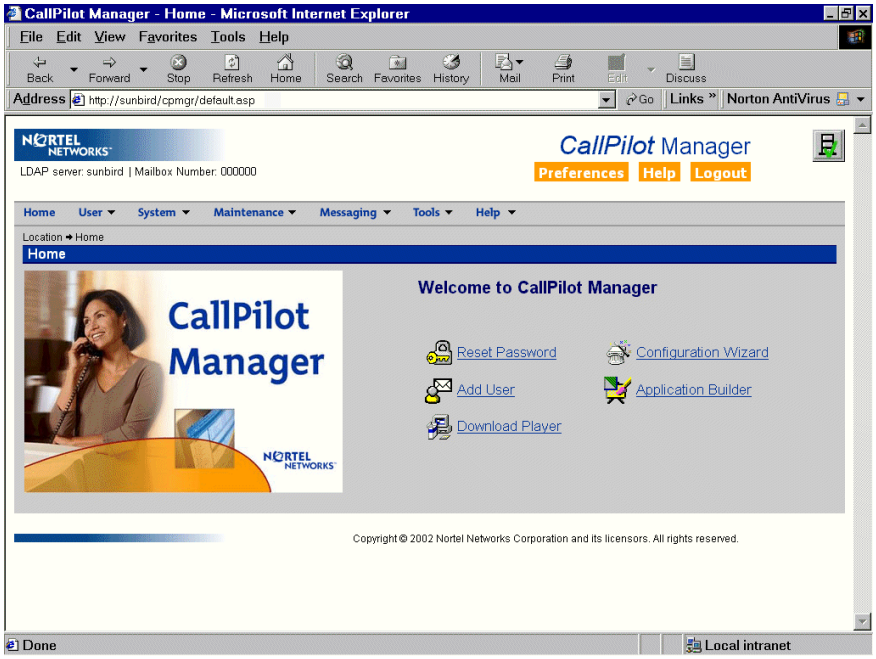
a. Clear the contents in the box.

b. Click once inside the box.

c. Choose the item you need from the list that appears.

5 Click Login.

Result: The main CallPilot Manager screen appears.



6 Work on the site as if you are working locally.

Multi-administrator access

Multiple administration is a standard database management feature that enables many administrators to work on a database at the same time. There is no limit to the number of administrators who can work on the network database at the same time.

Multiple administration offers several advantages, including:

- shared knowledge of network database maintenance
- faster and more efficient implementation

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.

Administrator privileges

For security reasons, administrators should be given access only to those parts of the system that relate to their role. An individual can be assigned full, partial or no administrative privileges.

Refer to the *CallPilot Administrator's Guide, NTP 555-7101-301* for detailed information on assigning administrative privileges.

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, indicating 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

The Message Network Configuration tree does not automatically refresh the views for all messaging network administrators. For this reason, if you are working in a multiple administration environment, click the web browser's Refresh or Reload button frequently. This ensures that you see the most current tree.

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.

Refreshing the view is especially important if you are deleting a remote site with satellite switch locations. A remote site cannot be deleted unless all satellite switch locations, in addition to the remote messaging server, are selected.

chapter 2

Getting started

This chapter introduces some basic networking concepts and terms that are necessary to understand CallPilot messaging solutions.

In this chapter

About networking and networking protocols 20

Messaging networks 25

About networking and networking protocols

In this section

Overview 20
Network setup 21
Messaging Protocols 22
Analog and digital messaging protocols 23

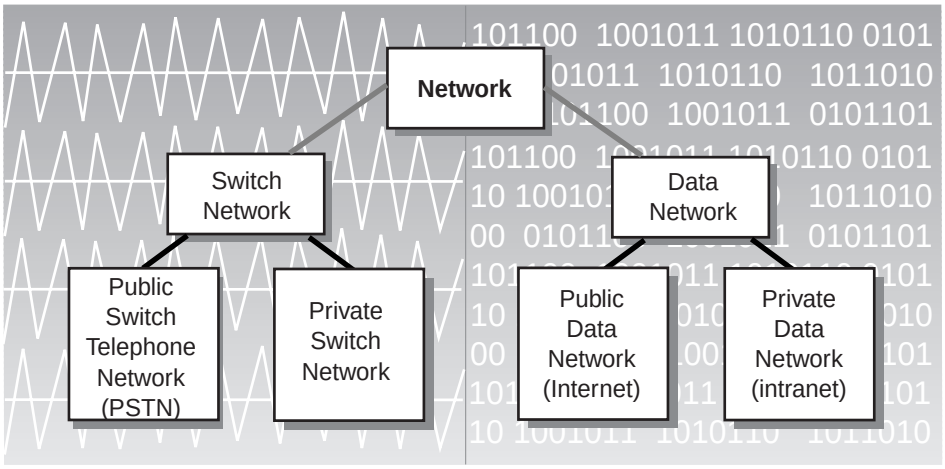
Overview

Basic networking concepts and terms are a useful background for CallPilot messaging networks.

Definition: Network

At its simplest, a network is a communication system that connects two or more sites. A network allows users at all sites to exchange information and to share specified resources.

Data networks and switch networks are two of the most common types of networks. Both types can be either public or private.



G100951

Definition: Switch network

Traditionally, telephone systems have been organized into switch networks.

There are three basic parts to a switched network:

- terminals (such as telephones or computers)
- transmission links (such as lines or trunks)
- one or more switches

In a switch network, a physical line is used to carry signals between the sender and the receiver. The sender uses a terminal and connects to a series of private and public telephony switches that terminate at the terminal of the receiver. The path of connection is maintained for the duration of the call and is destroyed when the call is completed. The signals are delivered in their original order.

Public switched network

If the switched network is maintained by a telecommunications service provider and is used by more than one customer, it is considered the public switch network. The public switched telephone network (PSTN) is the public telephone network used around the world.

Private switch network

If the switched network is privately owned and operated, and its use is restricted, it is considered a private switch network.

Definition: Data network

A data network is a communication system that enables two or more computers to communicate with each other and share resources.

In a data network, a stream of communication, such as a spoken message, is broken down into a series of packets. These packets contain information that identifies their origin, their intended recipient, and their correct order. The packets are routed through a network and are reconstructed, in their proper order, at their destinations.

There are many types of data networks, including local area networks (LANs), wide area networks (WANs), metropolitan area networks (MANs), and global area networks (GANs).

Public data network

A data network can make use of the publicly available infrastructure to transmit information. The Internet is an example of a public data network.

Private data network

A data network can be privately controlled. An intranet is an example of a private data network.

Definition: Messaging network

A network that exists for the purpose of exchanging messages is called a messaging network. When you implement any of the CallPilot networking solutions, you are creating a messaging network. In this context, a CallPilot networking solution is Nortel's implementation of a specific messaging protocol.

Messaging networks are built on an existing switch or data network infrastructure. A message network uses the voice or data network to transport messages between message servers. The existing structure is often called the backbone. A messaging network is usually private, although it is possible to exchange messages with sites that are not within the private messaging network.

Network setup

All networks have a physical setup that determines how the network operates.

The setup of a messaging network is an important factor in determining how you implement networking solutions and how users are able to exchange messages. The network setup consists of the sites and the connections between them. This setup is often called a network topology.

Possible setups

CallPilot supports different network setups to ensure that your messaging network is designed for the specific needs of your organization.

Two common types of network setup are the mesh network and the non-mesh network.

Mesh network

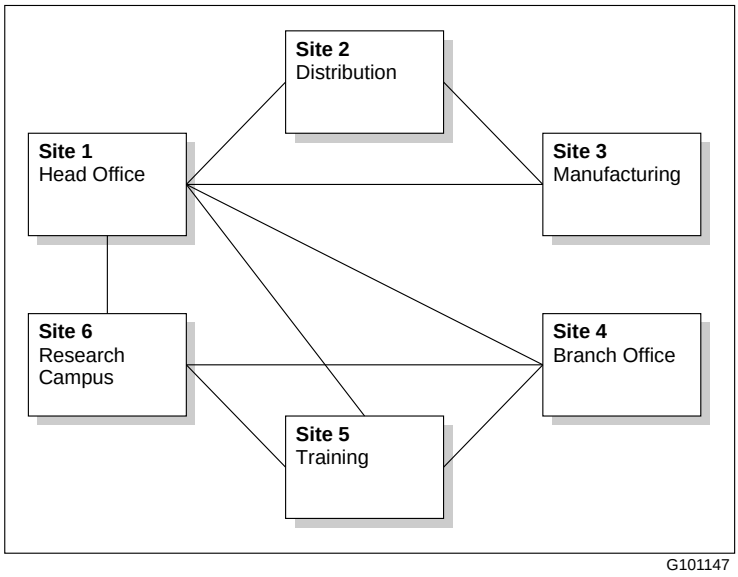
One of the most common network setups is the mesh network, also known as a point-to-point network. In a mesh network, every site is connected to every other site in the messaging network.

For small messaging networks, a mesh network setup is common. Every site can exchange messages with every other site in the network.

Non-mesh network

For larger messaging networks, a mesh network may be impractical or unnecessary. In fact, in most messaging networks, a site is connected only to those remote sites with which it commonly exchanges messages, such as in the hub-and-spoke network configuration. NMS Networking is an example of this.

The following diagram illustrates a non-mesh network. In this example, only the head office is connected to every other site. All other sites are connected only to those sites with which messages are exchanged. The manufacturing center, for example, is connected only with the distribution center and the head office.



This type of network setup also greatly simplifies the implementation and administration of the messaging network. Site 1 is the most complicated site to administer, because records for all other sites must be maintained. Site 3, however, is much simpler to administer, because records for only the two sites with which messages are exchanged must be maintained.

Messaging Protocols

Communication among sites in a messaging network is achieved by messaging protocols. A messaging protocol is a set of rules that defines how sites exchange information.

A messaging protocol must be used to exchange information between transmitting and receiving sites.

Types of messaging protocols

CallPilot uses two types of messaging protocols for exchanging messages: analog and digital.

Analog protocols run over voice networks. Digital protocols are used over data networks.

Within these two main categories there are both industry-standard and proprietary messaging protocols.

Industry-standard messaging protocols

Industry-standard messaging protocols are based on industry-recognized rules and conventions.

Proprietary messaging protocols

Proprietary messaging protocols are based on specifications defined by a closed group or organization for its own use within its own products.

Analog and digital messaging protocols

A network can use analog messaging protocols and digital messaging protocols.

Analog messaging protocols

Analog messaging protocols send voice signals that are similar to the original signal.

CallPilot supports two analog messaging protocols:

- **Audio Messaging Interchange Specification–Analog (AMIS-A)** Issued in 1990, AMIS-A is an industry standard that allows the voice messaging systems produced by different vendors to exchange voice messages.
- **Enterprise Networking** Nortel's proprietary protocol for analog transmission of voice messages. Enterprise Networking is an extension of AMIS-A and adds many important improvements, including longer voice message length and the ability to address a single message to multiple recipients.

Digital messaging protocols

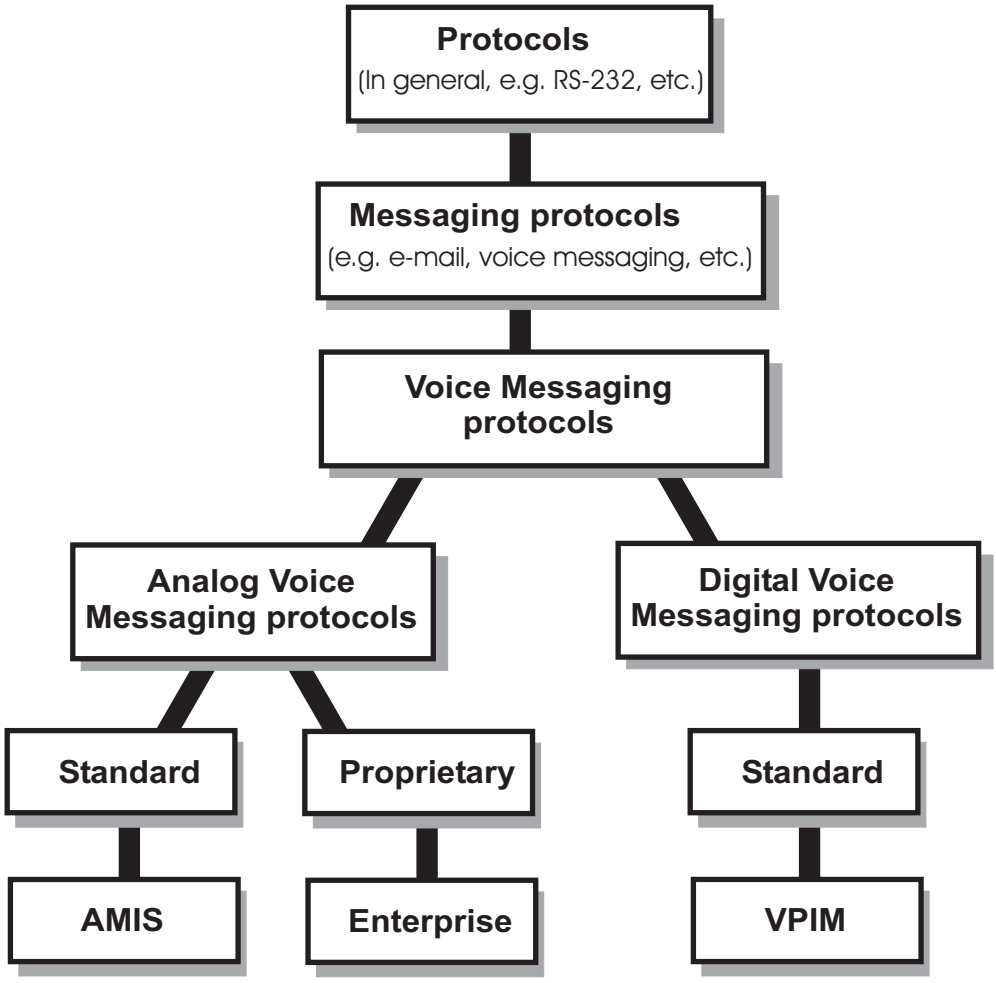
Digital messaging protocols convert analog signals into binary format before transmission.

Voice Profile for Internet Mail

Voice Profile for Internet Mail (VPIM) is a unified messaging protocol (voice, text and fax) that specifies the use of SMTP as the message transfer protocol and the use of MIME to format messages. CallPilot uses the SMTP and MIME protocols in compliance with industry-standard specifications.

- **Simple Message Transfer Protocol (SMTP)**
  A protocol for sending electronic mail (e-mail).
- **Multipurpose Internet Mail Extensions (MIME)**
  A means of representing the format of multimedia messages, including graphics, audio, and text files, over the Internet.

Messaging protocol hierarchy



Analog and digital messaging protocols compared

In an analog transmission, the signal may pick up stray or random noise. Messages sent with analog protocols may become degraded when they are forwarded, because of rerecording.

In a digital transmission, the signal does not pick up stray noise and may be cleaner than an analog signal.

Because computers use digital information, digital protocols allow telephone messaging to use the latest technologies available, including greater integration with electronic messaging, such as fax and e-mail, and desktop applications. Messages consist of digital parts that contain different media, including voice, fax, and text.

Digital messages are generally less expensive than analog messages, since no long-distance toll charges are currently associated with the Internet.

Messaging networks

In this section

Networks and messaging 25
Network database 26
Integrated and open sites 27

Networks and messaging

Messaging network

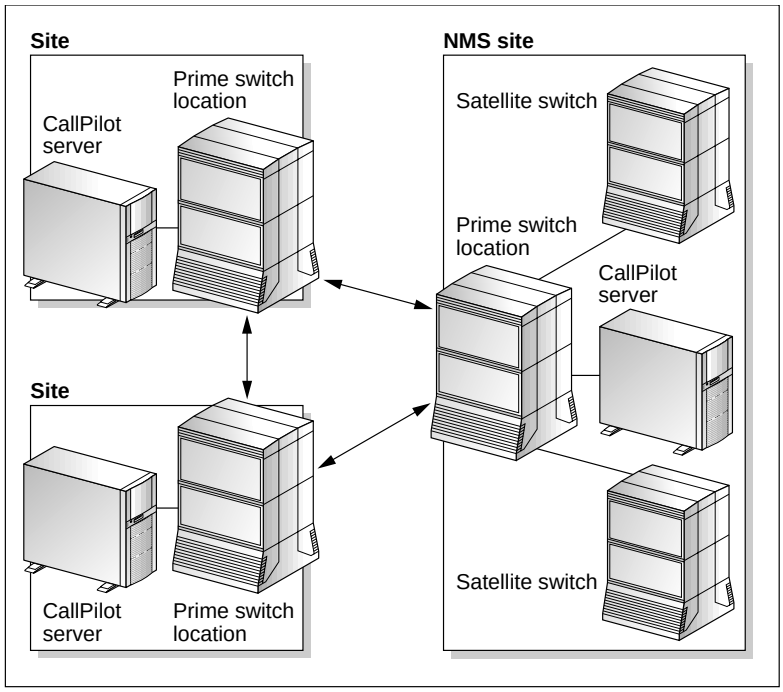
Messaging is the exchange of information, a common function of a network. CallPilot enables networks to function as messaging networks. A messaging network is a private network, whether data or switch, that allows users at one site to send messages to and receive messages from users at other sites.

CallPilot handles voice, fax, and text messages. Digital messaging protocols must be used for this, since analog messaging protocols only handle voice messages. Messages are sent and received through the telephone, the computer desktop, or a combination of both.

Message networking transports messages from one messaging server to another. Note that NMS networking uses the M1/CS1000 MCDN network to deliver calls from remote switches to a central CallPilot server.

Sites and connections

A messaging network consists of sites and connections. Connections are the agreed-upon protocols used between two sites.

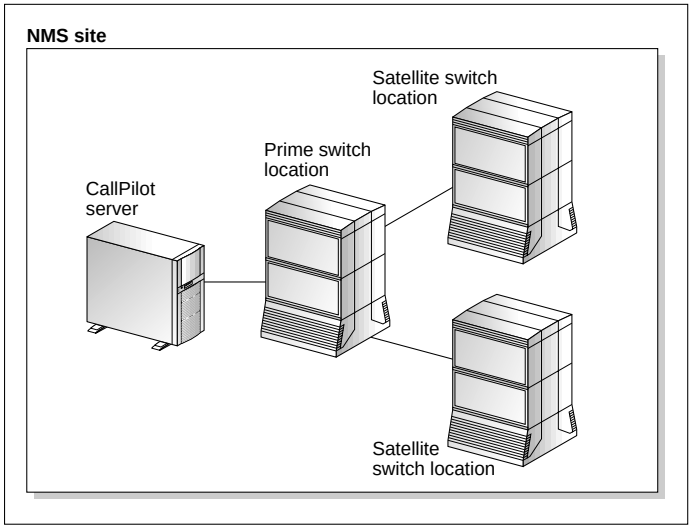


Definition: Site

In a messaging network, a site consists of a messaging server and a prime switch location. The messaging server is the computer that is running CallPilot. The network database resides on the messaging server. The prime switch location is the switch that is directly connected to the messaging server.

NMS site

If a site has Network Message Service (NMS) implemented, it is called an NMS site. An NMS site consists of a messaging server, a prime switch location, and up to 59 satellite switch locations.



Implementation is incremental

A messaging network is constructed on top of existing switch and data networks. It defines a portion of the network that CallPilot will use for messaging.

To implement a messaging network is basically to create a network database that contains information about the sites included in the messaging network and how they will communicate with one another.

Network database

The network database is the foundation of a CallPilot messaging network.

Every site in a CallPilot messaging network has its own network database. The network database resides on the messaging server. It can hold information for up to 500 networking sites.

Contents

The network database for a site contains information about the local site and all the remote sites with which the local site exchanges messages.

Local site information

A network database contains the following types of configuration information for the local site:

- local messaging network configuration

- local messaging server
- local prime switch location
- local satellite switch locations, if an NMS site

Remote site information

A network database also contains the following types of configuration information for each remote site with which the local site exchanges messages:

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

When this information about a remote site is added to a local network database, it becomes an integrated site.

Network database and the implementation process

When you implement a CallPilot networking solution, you add information to the network database.

Integrated and open sites

Messaging networks exchange messages with two types of remote sites: integrated sites and open sites. Whether a remote site is integrated or open depends on how the local network database is configured.

Integrated site

A remote site is integrated if information about it is added to the local network database.

Open site

A remote site is open if information about it is not added to the local network database. In most instances, an open site is a site that is not part of the private messaging network.

Protocols and open sites

The exchange of messages with open sites is possible through the use of industry-standard protocols. By using industry-standard protocols, systems can exchange messages regardless of the hardware platforms. Communication is possible if both systems use the same protocol.

Two CallPilot protocol implementations exchange messages with open sites:

- AMIS Networking—over a switch network
- VPIM Networking—over a data network

Integrated and open messaging networks

A private messaging network consisting of integrated sites is self-contained but is built on the infrastructure of switch and data networks, both public and private. The ability to exchange messages with open sites means that users can go beyond the integrated network, into switch and data networks, both public and private.

Exchanging messages in open messaging networks

The concept of open sites does not imply that a user in a private messaging network can automatically exchange messages with other systems that use the same industry-standard protocol.

Instead, an open site indicates that there is potential for users at the sites to exchange messages if they agree to do so and set up their networks to accept the communication.

When networking solutions that can exchange messages with open sites are implemented, access to open sites can be restricted.

Combining open and private sites

Many large messaging networks consist of integrated sites but can also exchange messages with open sites. Within an organization, it may be important to have messaging capabilities with external sites as well as internal sites.

chapter 3

Understanding CallPilot networking solutions

This chapter introduces the CallPilot networking solutions. This chapter lists the features of each solution and describes interactions with other CallPilot features. The characteristics of each solution are also detailed.

In this chapter

About CallPilot networking solutions 30

Messaging networks and users 38

Features 44

Networking and other features 47

Networking solution considerations 50

Transmission times and traffic calculations 64

Remote users 68

About CallPilot networking solutions

In this section

Overview 30
AMIS Networking 32
Integrated AMIS Networking 32
Enterprise Networking 33
VPIM Networking 33
Network Message Service 34
Combining networking solutions 35
Connections 35
Networking software options 36

Overview

CallPilot offers a range of coordinated messaging networking solutions that provide great flexibility and service. In this context, a networking solution is Nortel's implementation of a messaging protocol.

Overviews of each networking solution are provided in this guide that explain how the networking solutions work. The online Help system provides detailed procedural information about the implementation process for each solution.

To fully implement a networking solution, you will also need access to the relevant messaging server and switch documentation.

CallPilot networking solutions

CallPilot message networking can be implemented with three different protocols:

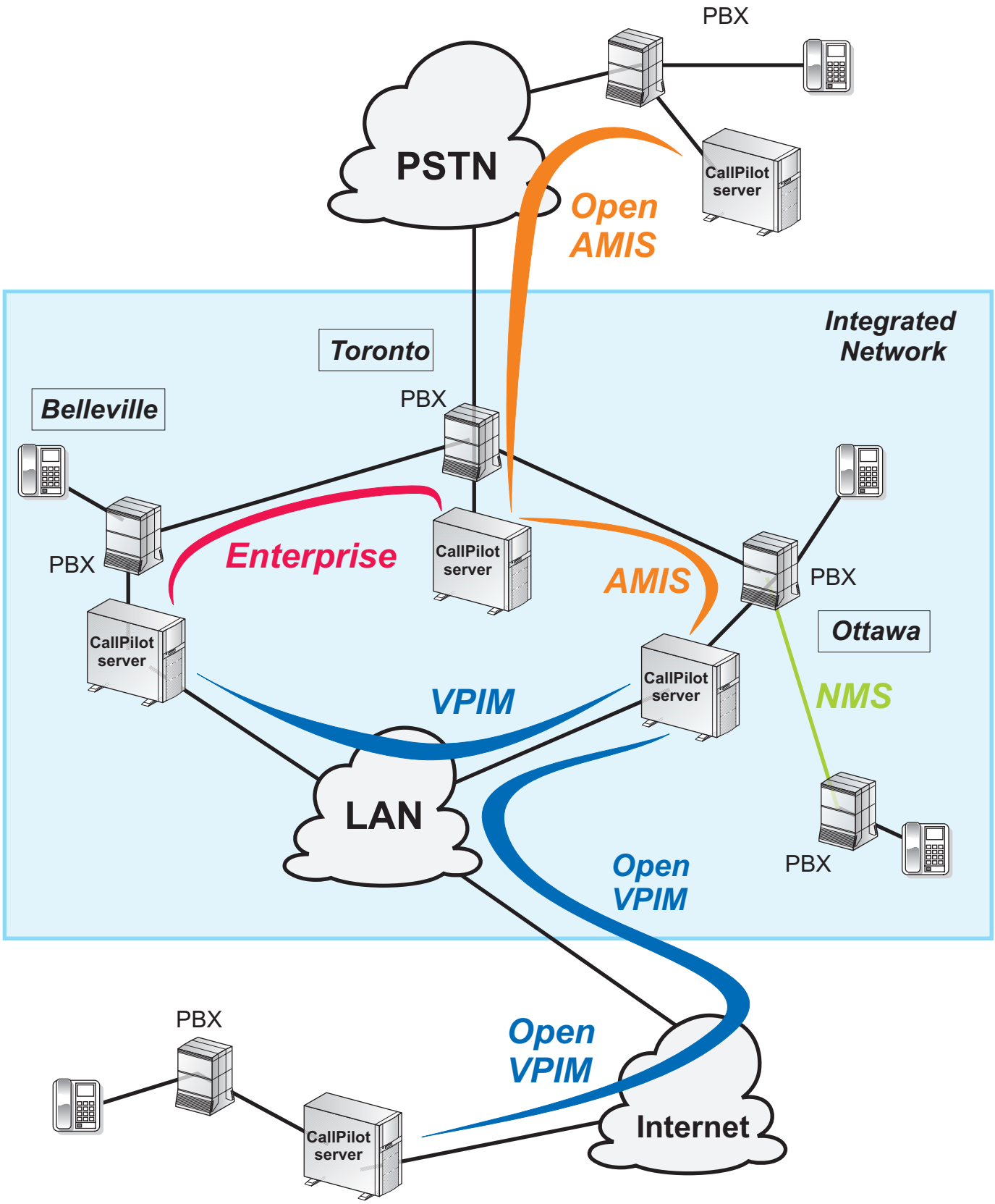
- AMIS/Integrated AMIS
- Enterprise
- VPIM

CallPilot also supports switches which are networked using Network Message Service (NMS).

These message networking protocols require the CallPilot Networking software option. NMS requires a separate CallPilot software option.

It is also important to note that Message Networking networks two or more messaging systems, while NMS networks two or more voice switches to a common CallPilot.

The following diagram shows a hypothetical network that makes use of all the available CallPilot networking solutions. Different solutions are implemented between different sites, depending on the corporate requirements.


PBX
PSTN
CallPilot server
Open AMIS
Integrated Network
Toronto
Belleville
PBX
PBX
Enterprise
CallPilot server
AMIS
PBX
Ottawa
CallPilot server
CallPilot server
VPIM
NMS
LAN
PBX
Open VPIM
PBX
Open VPIM
CallPilot server
Internet

AMIS Networking

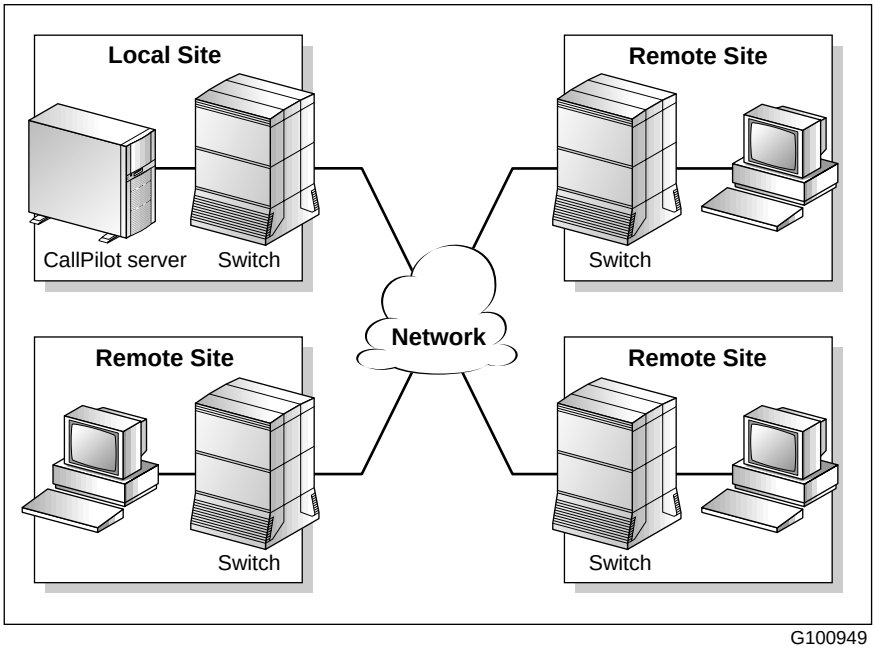
AMIS Networking uses “AMIS open addressing” which allows users to send messages to any other AMIS compliant messaging system (subject to the Restriction/Permission List) on the PSTN. While AMIS Open addressing is extremely powerful in its reach, it is more complex for users and has fewer features than Integrated AMIS addressing. It is usually used to exchange messages with open sites that are not part of the private messaging network.

AMIS Networking uses dual-tone multi-frequency (DTMF) tones to send information and supports voice messages, but does not support fax and text messages.

Integrated AMIS Networking

Integrated AMIS Networking also uses the industry-standard analog Audio Messaging Interchange Specification (AMIS) protocol and offers the same functionality as AMIS Networking. However, Integrated AMIS Networking is used to exchange messages with integrated sites. When a remote site that uses the AMIS protocol is defined within the local network database, it is called an “integrated site”. As such, users sending messages to other users at integrated sites can use the private network number addresses. This means they simply address a remote user using that user's DN. Additionally, AMIS messages sent and received from an integrated site have increased functionality, such as “Call Sender”.

Remote sites may use any voice messaging system that supports the AMIS protocol.



It is important to note that the functionality of AMIS Networking is contained within Integrated AMIS Networking. This means that if you implement Integrated AMIS Networking, users can also, if allowed, exchange messages with open sites.

Enterprise Networking

Enterprise Networking uses the Enterprise Networking protocol, a Nortel proprietary analog networking protocol supported only on Meridian Mail and CallPilot systems. The Enterprise Networking protocol is based on proprietary extensions to the AMIS protocol, and as such, offers many advantages over AMIS Networking.

Enterprise Networking uses dual-tone multi-frequency (DTMF) tones to send information. Enterprise Networking supports voice messages but does not support fax and text messages.

Advantages

The Enterprise Networking protocol offers several advantages over the AMIS protocol.

Feature	AMIS protocol	Enterprise Networking protocol
Multiple recipients	Sends one message to each recipient; requires greater system resources and long-distance toll charges	Sends a single message to multiple recipients; requires less system resources and lowers long-distance toll charges
Message length	8-minute maximum	120-minute maximum of all parts, where any individual part can be up to 99 minutes long
Security	Uses no special security features	Uses initiating and responding passwords between the sending and receiving sites before exchanging messages
Increased features	Limited feature availability	Supports additional features such as message privacy, message read acknowledgments, sending Username and Subject information, and Names Across the Network.

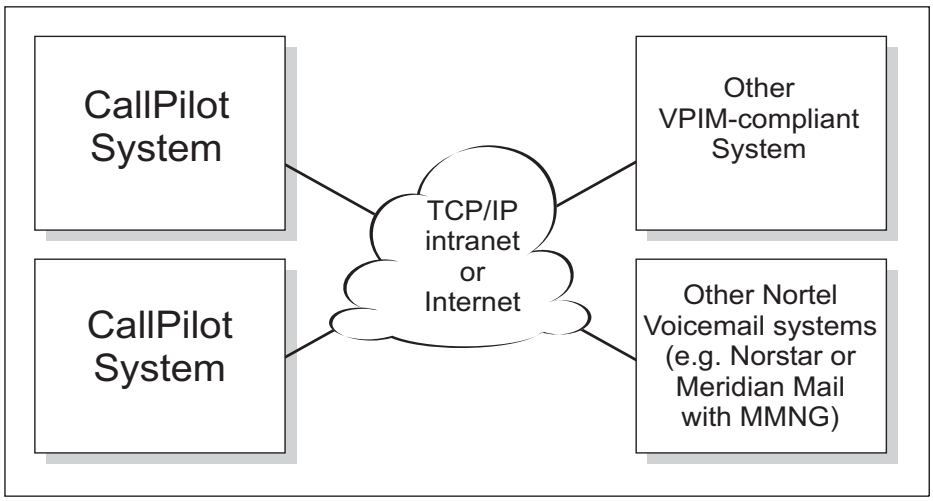
When networking CallPilot to a Meridian Mail, you should use Enterprise Networking. When networking a CallPilot to a non-Nortel messaging system, use Integrated AMIS.

VPIM Networking

VPIM Networking provides CallPilot with the capability to exchange multimedia messages using an IP intranet or the Internet. VPIM Networking can exchange messages with any other system that uses the same data communications protocol, regardless of vendor. VPIM Networking formats and sends messages using industry-standard application protocols. Messages are sent across either a private data network, such as an intranet, or a public data network, the Internet, for delivery. VPIM Networking also allows messages to be exchanged with both open and integrated sites. For VPIM Networking to work within a private network, the destination must support VPIM and be in the local network database.

In addition, since VPIM Networking transmits messages over data networks, the messages do not incur long-distance toll charges.

The following diagram shows the block interconnection between a CallPilot system and other voicemail systems.



G100948.eps

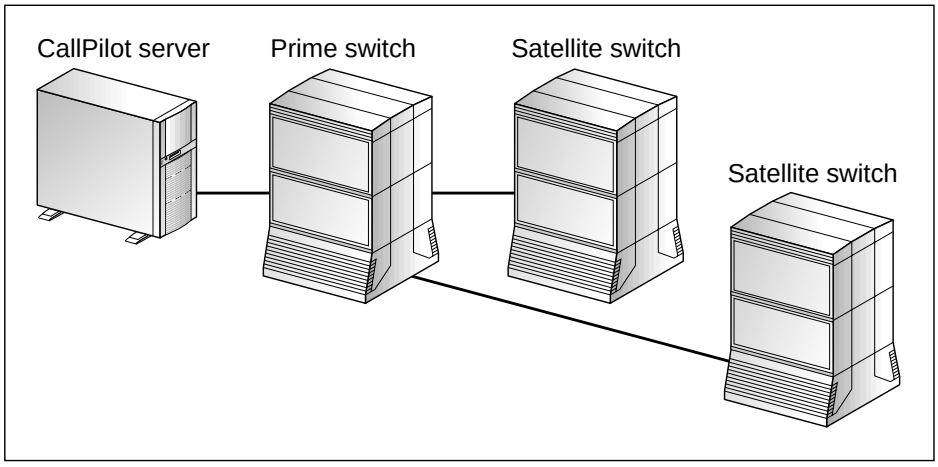
Network Message Service

Network Message Service (NMS) permits one CallPilot messaging server to provide messaging services to users on more than one switch location. The CallPilot messaging server is directly connected to a prime switch location. Up to 59 satellite switch locations can be attached to the prime switch location. The CallPilot messaging server provides messaging services to all switch locations.

NMS is transparent to users. A user whose telephone or desktop is attached to a satellite switch location can receive the same services as a user attached to the prime switch location. All users dial the same way to reach the same services.

NMS networks and NMS sites

The collection of switch locations, connections, and the messaging server is known as an NMS network. If an NMS network is a site in a private messaging network, it is called an NMS site.



G100947

Combining networking solutions

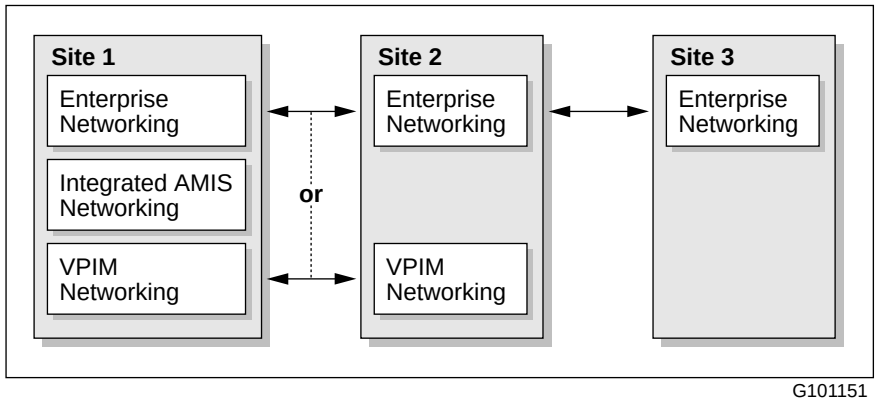
A messaging network can combine several networking solutions. Many messaging networks are combinations of several solutions at various sites. In addition, one or more of the sites in a messaging network can be NMS sites. This ability to combine networking solutions allows you to optimize your messaging network and create a customized solution for different business requirements.

However, to exchange messages between any two sites in a messaging network, both sites must have a common networking solution implemented and agree to use it.

Example

The following diagram shows three sites that are part of a larger messaging network.

- Site 1 has Enterprise Networking, Integrated AMIS Networking, and VPIM Networking implemented.
- Site 2 has Enterprise Networking and VPIM Networking implemented.
- Site 3 has Enterprise Networking implemented.



Sites 1 and 2 can exchange messages using either Enterprise Networking or VPIM Networking. The sending site is configured as to which protocol to use to connect to the remote site. Sites 2 and 3 can exchange messages using only Enterprise Networking.

Connections

A CallPilot system can connect to different systems, depending on the protocols installed.

CallPilot can be connected to the following systems using the following networking solutions:

System	Networking solution
CallPilot	■ Enterprise Networking ■ VPIM Networking ■ AMIS/Integrated AMIS Networking
Norstar Voice Mail (Release 3 and higher)	■ VPIM Networking ■ AMIS/Integrated AMIS Networking

System	Networking solution
Meridian Mail (Release 11 and higher)	■ Enterprise Networking ■ AMIS/Integrated AMIS Networking
Meridian Mail (Release 11 and higher) with Meridian Mail Net Gateway (Release 1 and higher)	■ VPIM Networking
Third-party system (must be compliant)	■ VPIM Networking ■ AMIS/Integrated AMIS Networking

Third-party systems

If you are connecting a CallPilot system to a third-party system, check the documentation for that system to ensure that the system is compliant. You may need to adjust the configuration of a third-party system.

Networking software options

The five networking solutions are available as optional additions to CallPilot software. Software options are required to make the networking solutions available.

The following software options are used to enable networking solutions:

Option	Action
Networking	Enables the following networking solutions: ■ AMIS Networking ■ Integrated AMIS Networking ■ Enterprise Networking ■ VPIM Networking Enables a maximum of 500 integrated sites. **Note:** Enables remote NMS sites to be added to the network database. Does not allow the local site to be added as an NMS site.
NMS	Enables use of NMS on the local site. **Note:** Enables a maximum of 60 switch locations, including prime switch location.

Installation

When you purchase the networking software option, all networking solutions, except for NMS, are available on your site.

However, during the installation of CallPilot, you can select which networking solutions you want to install. Install only the networking solutions that you plan to use to simplify the implementation process.

If you install networking solutions that you do not plan to use, you are asked to provide information that you may not have available. The implementation process becomes more complicated if you install unnecessary networking solutions.

ATTENTION!

Once installed, a networking solution cannot be uninstalled. Therefore, install only the networking solution or solutions that you require. You can add additional networking solutions at any time.

Messaging networks and users

In this section

Overview 38
Message types supported 38
Message lengths 39
Telephone users and desktop users 41
Teaching users how to use networking 41
Non-delivery notifications 43

Overview

The networking solutions offered by CallPilot are designed to make it easier for users to exchange messages.

Terminology note

Although users have mailboxes on the CallPilot Server, their telephones are attached to the switch. Their desktops are on the local area network (LAN). For convenience, users are said to be “on a switch.”

Ease of use

When you implement a networking solution, you provide information that the system uses to make it easy for local users to use networking. While the implementation process can seem complicated, the end result is a system that is easier to use. Whenever possible, CallPilot networking is designed so that users can address a message to a remote site in the same way they dial that remote site. That is, there are no additional numbers to memorize.

Message types supported

CallPilot networking supports the exchange of different types of messages and message attachments.

Comparison

The following shows the message types supported by each networking solution.

Networking solution	Voice	Fax	Text
AMIS Networking	Yes	No	No
Integrated AMIS Networking	Yes	No	No

Networking solution	Voice	Fax	Text
Enterprise Networking	Yes	No	No
VPIM Networking	Yes	Yes	Yes
NMS	Yes	Yes	Yes

Message type and non-delivery notifications

When users send a message type that is not supported, they receive non-delivery notifications.

Sending voice messages to external users

When composing a voice message to:

- an Open VPIM address: the voice message will be transcoded to G.726 and delivered to the remote voice mailbox
- an e-mail address using CallPilot desktop or My CallPilot messaging: the voice message will be transcoded to WAV format and delivered to recipients' e-mail accounts

Message lengths

Each networking solution supports different system message lengths.

A message consists of the message header, the message body, and all attachments. A message can contain a mixture of message types, since each message can be one of different media types: voice, fax, or text.

Note: The Class of Service granted to a mailbox determines the message length limits that can be sent and received by a user. The length can be shorter than the system maximum.

Comparison

The following table compares the message lengths supported by each networking solution.

Networking solution	Approximate byte limit	Approximate maximum voice length time limit	Notes
AMIS Networking	1.2 Mbytes	8 minutes	■ Voice supported only
Integrated AMIS Networking	1.2 Mbytes	8 minutes	■ Voice supported only
Enterprise Networking	17.3 Mbytes	120 minutes	■ Limit of each part is 99 minutes ■ Voice supported only

Networking solution	Approximate byte limit	Approximate maximum voice length time limit	Notes
VPIM Networking	17.3 Mbytes	120 minutes	■ Voice, fax, and text supported ■ A single part can be 120 minutes long ■ Affected by voice encoding format used and other factors
NMS	17.3 Mbytes	120 minutes	■ Same as limit for local messages

Message length and non-delivery notifications

All messages are sent in their entirety. A message that exceeds the length limit is not broken into smaller units and sent as a series of messages.

If a message exceeds the length limit or is rejected by the receiving system due to length, the message is not delivered and a non-delivery notification is sent to the sender.

Length checking

The length of a message is not checked before it is sent, because a message may be addressed to multiple recipients using different networking solutions that allow for different maximum message length.

This means that a sender does not know that the limit is exceeded until a non-delivery notification is received.

Enterprise Networking

A non-delivery notification is sent if an Enterprise Networking message

- exceeds the total limit of 120 minutes, or
- any part of the message exceeds the 99-minute limit

Approximate equivalents

A message can contain a mixture of media. This means that only an approximate equivalent can be determined from the total bytes of storage needed for a message.

To determine the approximate length of voice, fax, and test messages, the following conversion guideline factors are used:

Voice

144 kbytes = approximately one minute

Fax

41 kbytes = one fax page (normal resolution, standard page size)

Text

- 1 byte = 1 ASCII character
  2 bytes = 1 Unicode character

Telephone users and desktop users

CallPilot networking solutions support computer telephony.

Computer telephony brings together two communications systems—the telephone system and the computer system. Merging these systems offers a richer information channel and a way to improve the capabilities of two communication systems. However, computer telephony has special requirements in terms of implementing CallPilot networking.

When you implement a networking solution, much of the configuration is designed to make networking as transparent as possible for users. That is, you configure the system so that users address a message to another site in almost the same way they dial to that site.

Telephone users

Telephone users can use networking features as allowed by the system administrator.

Desktop users

The desktop is another way for users to access messages. It offers the same capabilities as the telephone, but can also be used to view fax and text messages.

If your site has desktop users, there is an impact only on the implementation of VPIM Networking. For all other networking solutions, the implementation is the same whether the local site supports telephone users, desktop users, or both.

Terminology note

Throughout the networking documentation, a distinction is made between telephone users and desktop users, where necessary. All CallPilot users have telephone access and use the telephone interface. However, only some (or perhaps all) users may have desktop access. These users may use the desktop interface.

However, if there is no difference between the actions of the two types of users or no differences between the functionality they can expect, the term *user* applies to both groups.

It is important to remember the distinction between the two types of users while implementing a networking solution. Some information that you must provide during implementing applies specifically to telephone users or desktop users.

Teaching users how to use networking

After you have implemented CallPilot networking, you must let local users know how to use it.

Addressing integrated sites

During implementation, you specify various access codes and other information for each remote site that can exchange messages with the local site. Some of this information must be made available to your local users. It supplements the information in their user's guides.

Example

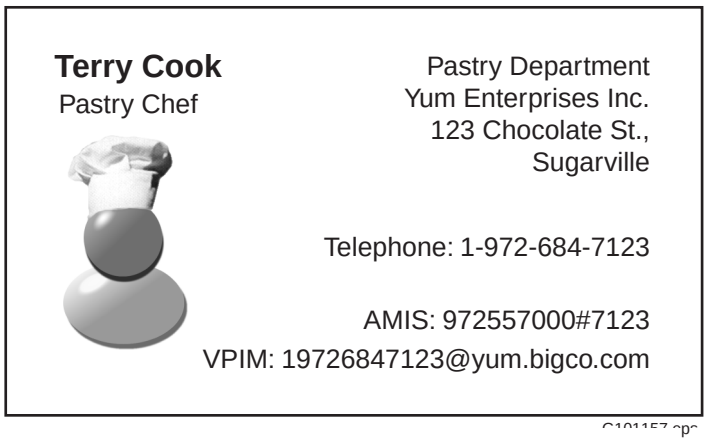
You configure the system with a VPIM Networking access code, 15. This access code must be entered before a VPIM shortcut to an open site or an integrated site is entered. You must announce what the code is and when to use it.

Addressing open sites

To exchange messages with open sites, users must know that an open site uses a compliant protocol and must know how to address users at that open site.

Example

The following business card provides an AMIS address and a VPIM address, as well as a telephone number.



Open AMIS Networking

To exchange messages with a remote open site using the AMIS protocol, users must know the system access number of that remote site.

Open VPIM Networking

To exchange messages with a remote open site using the VPIM protocol, users must know the VPIM address of that remote site.

A VPIM address resembles a standard e-mail address.

- e-mail address: username@institution.com
- VPIM address: 14165975555@institution.com

The composition of a VPIM address creates some problems. Because the address contains alphabetic, as well as numeric, characters, only desktop users can enter an Open VPIM address. If local telephone users want to exchange messages with open sites using VPIM networking, you must create an Open VPIM shortcut for them.

An Open VPIM shortcut translates an alphanumeric VPIM address into a numeric address. This enables telephone users to enter VPIM addresses.

See also

For a detailed discussion on addressing VPIM Networking messages and how VPIM shortcuts work, consult Chapter 7, About VPIM Networking in this guide.

Non-delivery notifications

If users attempt to use CallPilot in ways that are not supported, they receive non-delivery notifications. A non-delivery notification provides a brief description of why a message could not be delivered. Usually, a non-delivery notification contains enough information for a user to identify and correct a problem without assistance from the network administrator.

Non-delivery notifications and the Event Monitor

Most networking activities that generate non-delivery notifications also trigger an event listed in the Event Monitor. In this way, the network administrator can monitor how users are attempting to use the messaging network.

Too many events indicates that users need additional training on how to use networking features.

Exception

One activity generates a non-delivery notification for a user but does not trigger an event.

If a user sends a message to a nonexistent mailbox on a remote site, a non-delivery notification is generated. An event is not triggered even if several attempts are made to reach this nonexistent mailbox.

Users can contact their local network administrator to help resolve the problem.

See also

For detailed information about the Event Monitor, consult the *Maintenance and Diagnostics Guide*.

Features

In this section

Overview 44
Enhancements to Meridian Mail capabilities 45
Migration from Meridian Mail 46

Overview

Each CallPilot networking solution supports different features.

Feature comparisons

The following table lists the CallPilot features that are supported by each of the networking solutions. Detailed discussions of these features are available in the sections that follow.

In the following table, Yes may be qualified. Check the detailed discussions for more information.

Feature	AMIS	Integrated AMIS	Enterprise	VPIM	NMS
Call Sender	No	Yes	Yes	Yes	Yes
Names Across the Network	No	No	Yes	Yes	n/a
Name Addressing	No	Yes	Yes	Yes	Yes
Personal Distribution Lists	Yes	Yes	Yes	Yes	Yes
Shared Distribution Lists	No	Yes	Yes	Yes	Yes
Multiple Recipients	No	No	Yes	Yes	Yes
Reply To	Yes	Yes	Yes	Yes	Yes
Reply All	No	No	Yes	Yes	Yes
User-Recorded Personal Verification	No	No	Yes	Yes	Yes
Administrator-Recorded Personal Verification	No	Yes	Yes	Yes	Yes
Remote Site Spoken Names	No	Yes	Yes	Yes	Yes

Feature	AMIS	Integrated AMIS	Enterprise	VPIM	NMS
Privacy Tag	No	No	Yes	Yes	Yes
Acknowledgment Tag	Yes	Yes	Yes	Yes	Yes
Urgent Tag	Yes	Yes	Yes	Yes	Yes
Received Time Announced	Yes	Yes	Yes	Yes	Yes
Sent Time Announced	No	No	Yes	Yes	Yes
120-Minute Messages	No	No	Yes	Yes	Yes
Sender's Name (Text)	No	No	Yes	Yes	Yes
Recipient's Name (Text)	No	No	Yes	Yes	Yes
Message Subject (Text)	No	No	Yes	Yes	Yes
Timed Delivery	Yes	Yes	Yes	Yes	Yes
Time Zone support	No	No	Yes*	Yes	Yes

* Must be supported at both ends

Enhancements to Meridian Mail capabilities

If you are familiar with Meridian Mail, you will notice that CallPilot expands and enhances the networking capabilities offered by Meridian Mail.

CallPilot offers networking enhancements in the following areas:

- site capacity
- steering code capacity
- VPIM Networking

Site capacity

A CallPilot messaging network can contain 500 integrated sites. A Meridian Mail messaging network can contain 150 integrated sites.

Steering code capacity

CallPilot increases the number of CDP steering codes supported from 50 to 500.

VPIM Networking

VPIM Networking is a new networking solution. Meridian Mail does not include a digital networking solution. Meridian Mail sites that want to use digital networking have to attach Meridian Mail Net Gateway to their existing Meridian Mail system.

Note: The Bulk Provisioning feature in Meridian Mail is called AutoAdd in CallPilot.

For more detailed information, consult the *Meridian Mail to CallPilot Migration Guide*.

Migration from Meridian Mail

If your implementation of a CallPilot networking solution is an upgrade of an existing Meridian Mail networking solution, you can use the Migration utility to capture most of the legacy information. The migration utility saves you time and ensures that information is upgraded accurately and completely.

Note that since CallPilot provides many enhancements to Meridian Mail, the migration is not a straightforward transfer of information. Some information must be modified after migration. Additional information must be provided.

For detailed information on migrating networking information, consult the *Meridian Mail to CallPilot Migration Guide*.

Networking and other features

In this section

Overview 47
Shared Distribution Lists (SDL) 47
Personal Distribution Lists (PDL) 48
Names Across the Network (NAM) 48
System trigger mailboxes 49

Overview

CallPilot networking solutions have special interactions with the following features:

- Shared Distribution Lists
- Personal Distribution Lists
- Names Across the Network
- System trigger mailbox

Shared Distribution Lists (SDL)

Shared Distribution Lists (SDL) can be used in a messaging network. An SDL is a list of recipients that is created by a system administrator. It can include both local and remote users. To be included in an SDL, a remote user must be defined on the local site.

If a message is sent by a local user to an SDL, all local and remote users on the list receive the message. In addition, a user at one site can send a message to an SDL that is defined on another site.

If a message is sent by a remote user to an SDL on the local system, only local users on the list receive the message. Remote users on the list will not receive a copy of the message.

Examples

The following example describes how SDLs are used.

Using SDLs with Enterprise Networking

Sam Hicks in New York wants to send a message to everyone on an SDL that includes local users and remote users in Boston.

- New York SDL = 2201

Sam composes a message and enters 2201. Users at both sites receive Sam's message.

For more information about shared distribution lists, consult the CallPilot Manager online Help.

Personal Distribution Lists (PDL)

Personal distribution lists (PDL) can be used in a messaging network.

As its name implies, a PDL is created and maintained by a user, not an administrator. A PDL contains the addresses that are used frequently by a user. The list saves time, because a user does not have to enter each recipient's address each time a message is sent.

Network addresses can be included in a PDL. A list can include local users, remote users, Open AMIS users, Open VPIM users, broadcast addresses, SDLs (but not other PDLs), and NMS users. Network addresses are validated. If a network address from a PDL is found to be invalid after a message addressed with a PDL is sent, the user receives a non-delivery notification.

Possible causes of invalid network addresses include the following:

- Changes have been made to the network configuration. PDLs are not automatically updated when changes are made.
- The user's permissions, such as the ability to use AMIS Networking, have been revoked.

Names Across the Network (NAM)

The Names Across the Network feature is available with Enterprise and VPIM Networking only. NAM is not needed with NMS since users on remote switches are on the same server as local users. Local user messaging to users on remote switches is completely transparent. The only networking protocol that can not provide network transparency is AMIS.

The Names Across the Network feature allows the spoken names of senders of messages to be reproduced at recipient sites. If a sender does not exist at the recipient site as a remote user, a temporary remote user is added to the site with the sender's text name and spoken name.

Names Across the Network eliminates the need for a system administrator to manually add a permanent remote user and record a spoken name on the user's behalf.

Enterprise Networking and Names Across the Network

System administrators can configure Enterprise Networking to handle Names Across the Network according to their needs. System administrators can:

- define whether the local site accepts and stores spoken names received using Names Across the Network.
- define whether the local site sends spoken names with Enterprise Networking messages to a particular remote site.
- define which remote sites the local site sends spoken names to.

The ability to configure these definitions is useful if the local site is placing calls to remote sites that incur long-distance toll charges. The administrator can choose to send spoken names to toll-free sites, but not to sites that incur toll charges.

For a general description of remote users and how Names Across the Network works, see the section Remote users on page 68.

System trigger mailboxes

A system trigger mailbox is a mailbox that is defined by the system administrator for a specific purpose.

Two types of system mailboxes are used by networking:

- *Alarm mailbox*: An alarm mailbox receives messages generated by errors. You specify the type of error messages that are placed in the alarm mailbox.
- *Broadcast mailbox*: A mailbox that has been assigned the rights to send network broadcasts

In an NMS network, system mailboxes exist on the prime switch, not on a satellite switch.

See also

For more information about system mailboxes, consult Chapter 5, Network and location-specific broadcast messages and the CallPilot Manager online Help.

Networking solution considerations

In this section

Overview 50
General messaging network considerations 50
AMIS Networking features 51
Integrated AMIS Networking features 53
Enterprise Networking features 55
VPIM Networking features 58
Network Message Service (NMS) features 60
NMS dialing restriction scenarios 62

Overview

There are some important considerations that you must keep in mind when implementing CallPilot networking solutions. Understanding these considerations before implementation will help you recognize what functionality to expect from each networking solution.

There are two main types of considerations:

- general—apply to all networking solutions
- specific—apply to a particular networking solution

General messaging network considerations

General considerations that apply to all messaging solutions must be considered when planning a network.

Number of sites

CallPilot supports a maximum of 500 integrated sites.

Channels supported

AMIS and Enterprise networking protocols use voice channels. VPIM protocol does not generate traffic on voice channels because it uses the IP network.

Networking solutions can also use fax and speech recognition channels if the resources are available.

Delivery sessions

The maximum number of simultaneous delivery sessions to a single remote site depends on the networking solution.

This networking solution	supports
AMIS Networking	up to five sessions.
Integrated AMIS Networking	up to five sessions.
Enterprise Networking	up to five sessions.
VPIM Networking	up to 10 sessions outgoing (CP 3.0). up to 10 sessions incoming (CP 3.0).

Other considerations

In addition to these general considerations, each networking solution has specific considerations that must be kept in mind. These are described in the following sections.

AMIS Networking features

The following table lists the CallPilot features that are or are not supported by AMIS Networking.

CallPilot feature	Supported	Notes
Call Sender	No	
Names Across the Network	No	
Name Addressing	No	
Name Dialing	No	
Personal Distribution Lists	Yes	AMIS addresses can be included in a user's personal distribution list.
Shared Distribution Lists	No	
Multiple Recipients	Yes	When a message is sent to more than one recipient, a separate message is transmitted for each AMIS recipient.
Reply To	Yes	Restriction/Permission Lists can be set up to block return messages to certain sites, such as international long-distance sites.
Reply All	No	AMIS messages only contain information about the originator of a message, not all recipients of the message.
User's Actual Personal Verification	No	

CallPilot feature	Supported	Notes
Administrator-Recorded Personal Verification	No	
Remote Site Spoken Names	No	
Private Tag	No	AMIS does not support private message tags. For this reason, messages tagged as private are returned to the sender with a non-delivery notification.
Acknowledgment Tag	Yes	Acknowledgment tags indicate that the message was delivered to the remote site, not that it was listened to.
Urgent Tag	Yes	When users tag a message as urgent, the system treats it as urgent for the prioritizing of delivery. However, the recipient of an urgent message does not know it was tagged as urgent.
Economy Tag	Yes	When users tag a message as economy, the system treats it as economy for the prioritizing of delivery. However, the recipient of an economy message does not know it was tagged as economy.
Received Time Announced	Yes	The time when the message was deposited into the mailbox is announced to the recipient.
Sent Time Announced	No	
120-Minute Messages	No	Message body length is limited to eight minutes. Messages longer than eight minutes are not sent, and a non-delivery notification is sent to the originator.
Sender’s Name (Text)	No	
Recipient’s Name (Text)	No	
Message Subject (Text)	No	
Sender’s Department	No	
Timed Delivery	Yes	
Time Zone Support	No	

Mailbox length

For AMIS Networking, mailboxes cannot exceed 16 digits.

Message handling

AMIS Networking delivers all messages in their entirety or not at all. Messages are never delivered in part. A non-delivery notification (NDN) indicates that no part of the message was received.

Other considerations

The considerations described in General messaging network considerations on page 50 also apply to AMIS Networking.

Integrated AMIS Networking features

The following table lists the CallPilot features that are or are not supported by Integrated AMIS Networking.

CallPilot feature	Supported	Notes
Call Sender	Yes	Call Sender can be used for both call answering and composed messages from Integrated AMIS Networking users if ■ the mailbox numbering plan follows the dialing plan, or ■ a remote user is added for the network user
Names Across the Network	No	
Name Addressing	Yes	This feature is available if users at the remote site are defined as remote users at the local site.
Name Dialing	Yes	This features is available if users at the remote site are defined as remote users at the local site.
Personal Distribution Lists	Yes	Integrated AMIS Networking addresses can be included in a PDL.
Shared Distribution Lists	Yes	A remote user is required. A network address cannot be entered into the shared distribution list unless the address corresponds to a remote user.
Multiple Recipients	No	
Reply To	Yes	
Reply All	No	A message has only one recipient.
Users Actual Personal Verification	No	The user's actual personal verification is not carried across sites.

CallPilot feature	Supported	Notes
Administrator-Recorded Personal Verification	Yes	The administrator can record a personal verification for remote users who are defined at the local site.
Remote Site Spoken Names	Yes	A spoken name can be recorded for each remote switch location when configuring the remote site maintenance screen.
Private Tag	No	AMIS does not support private message tags. For this reason, messages tagged as private are returned to the sender with a non-delivery notification.
Acknowledgment Tag	Yes	Acknowledgment tags indicate that the message was delivered to the remote system, not that it was listened to.
Urgent Tag	Yes	Users can tag a message as urgent, and the system treats it as urgent for the prioritizing of delivery. However, the recipient of an urgent message does not know it was tagged as urgent.
Economy Tag	Yes	Users can tag a message as economy, and the system treats it as economy for the prioritizing of delivery. However, the recipient of an urgent message does not know it was tagged as economy.
Received Time Announced	Yes	The time when the message was deposited into the mailbox is announced to the recipient.
Sent Time Announced	No	
120-Minute Messages	No	Message body length is limited to eight minutes. Messages longer than eight minutes are not sent, and a non-delivery notification is sent to the originator.
Sender’s Name (Text)	No	
Recipient’s Name (Text)	No	If the recipients are defined as remote users, their names are provided.
Message Subject (Text)	No	
Sender’s Department	No	
Timed Delivery	Yes	

Mailbox length

For Integrated AMIS Networking, mailboxes cannot exceed 16 digits.

Message handling

Integrated AMIS Networking delivers all messages in their entirety or not at all. Messages are never delivered in part. A non-delivery notification (NDN) indicates that no part of the message was received.

Other considerations

The considerations described in General messaging network considerations on page 50 also apply to Integrated AMIS Networking.

Enterprise Networking features

The following table lists the CallPilot features that are or are not supported by Enterprise Networking.

CallPilot feature	Supported	Notes
Call Sender	Yes	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	Yes	
Name Addressing	Yes	Name addressing is available if users at the remote site are defined as remote users at the local site. This can be done automatically with Names Across the Network or manually by the administrator.
Personal Distribution Lists	Yes	This feature is available if users at the remote site are defined as remote users at the local site, which can be done by Names Across the Network.
Shared Distribution Lists	Yes	A remote user is required. A network address cannot be entered into the shared distribution list unless the address corresponds to a remote user.
Multiple Recipients	Yes	The Enterprise Networking message contains all the recipients of the message who are at integrated sites. Recipients at open sites are not included.

CallPilot feature	Supported	Notes
Reply To	Yes	This feature can be used with all network messages. It can also be used with call answering messages left by network users if the calling line identification (CLID) is present on the message and all other conditions listed for Call Sender are met.
Reply All	Yes	This feature works with all recipients at integrated sites. It does not include recipients at open sites.
User's Actual Personal Verification	Yes	The user's personal verification is played to callers in voice messaging scenarios if recipients are defined as remote users at the local site. AutoAdd or Names Across the Network can be used to create the user's personal verification.
Administrator- Recorded Personal Verification	Yes	The administrator can record a personal verification for remote users who are defined at the local site.
Remote Site Spoken Names	Yes	A spoken name can be recorded for each remote site when configuring a remote site.
Private Tag	Yes	Messages tagged as private are announced to the recipient and may not be forwarded by the recipient to anyone else.
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 treated with priority for transmission as determined by the scheduling parameters.
Economy Tag	Yes	
Received Time Announced	Yes	The time when the message was deposited into the mailbox is announced to the recipient. The time reflects the time zone of the recipient.
Sent Time Announced	Yes	The sent time announced to the recipient reflects the time zone of the sender, not the recipient.

CallPilot feature	Supported	Notes
120-Minute Messages	Yes	Enterprise Networking supports messages containing up to 120 minutes of voice, including any attachments.
Sender's Name (Text)	Yes	Only supported if American English character set (ASCII 32–126) used.
Recipient's Name (Text)	Yes	If the recipients are defined as remote users, their names are provided. Only supported if American English character set (ASCII 32–126) used.
Message Subject (Text)	Yes	Only supported if American English character set (ASCII 32–126) used.
Sender's Department	No	
Timed Delivery	Yes	Any message can be tagged for future delivery.

Message body length

The maximum length of an Enterprise Networking message, including the voice recording and all attachments, is 120 minutes. Any single part of the message can be up to 99 minutes long.

The length of an Enterprise Networking message is not restricted by the number of recipients.

Message handling

Enterprise Networking delivers all messages in their entirety or not at all. Messages are never delivered in part. A non-delivery notification (NDN) indicates that no part of the message was received.

Other considerations

The considerations described in General messaging network considerations on page 50 also apply to Enterprise Networking.

VPIM Networking features

The following table lists the CallPilot features that are or are not supported by VPIM Networking.

CallPilot feature	Supported	Notes
Call Sender	Yes	Supported for messages 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 ■ mailbox addressing follows dialing plan for the remote site, or ■ a remote user entry is added for the network user
Names Across the Network	Yes	This feature is currently not supported.
Name Addressing	Yes	A remote user must be defined.
Personal Distribution Lists	Yes	A remote user must be defined.
Shared Distribution Lists	Yes	A remote user must be defined.
Multiple Recipients	Yes	Recipients to non-VPIM sites are not included in the VPIM message.
Reply To	Yes	
Reply All	Yes	Replies are sent to the VPIM recipients of the message only.
User's Actual Personal Verification	Yes	
Administrator-Recorded Personal Verification	Yes	A remote user must be defined.
Remote Site Spoken Names	Yes	To integrated VPIM sites only.
Private Tag	Yes	Messages tagged as private are announced as such to the recipient. Private messages may be forwarded.
Acknowledgment Tag	Yes	Acknowledgment tags result in a message to the sender indicating that the message was actually listened to.

CallPilot feature	Supported	Notes
Urgent Tag	Yes	Messages tagged as urgent trigger urgent-related features, such as Remote Notification or Message Waiting Indication. Messages tagged as urgent are announced as such to the recipient.
Economy Tag	Yes	
Received Time Announced	Yes	
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 and other factors.
Sender's Name (Text)	Yes	Only supported if American English character set (ASCII 32–126) used.
Recipient's Name (Text)	Yes	Only supported if American English character set (ASCII 32–126) used.
Message Subject (Text)	Yes	Only supported if American English character set (ASCII 32–126) used.
Sender's Department	No	
Timed Delivery	Yes	

Planning and engineering considerations

The following issues must be considered for VPIM Networking implementation:

- impact of VPIM on the local area network (LAN)
- message handling capabilities (throughput)
- message queuing capacities
- message delivery times

LAN load

The VPIM Networking protocol requires an average of 180 kbytes of data per second of voice to transport a voice message over the IP network. The peak load on the IP network is equal to the "pump rate" of the SMTP delivery process. The "pump rate" is independent of the aggregate number of SMTP connections on allocated IP ports (specified as five inbound and five outbound). Rather, the "pump rate" is dependent more on of contention of the SMTP service with other services for CPU and disk resources.

When VPIM is compared to four active Enterprise Networking channels, the equivalent data rate imposed on the IP Network by VPIM is 21 kbytes per second (less than 1 percent of 10BaseT bandwidth).

Message handling

VPIM Networking delivers all messages in their entirety or not at all. Messages are never delivered in part. A non-delivery notification (NDN) indicates that no part of the message was received.

Other considerations

The considerations described in General messaging network considerations on page 50 also apply to VPIM Networking.

Network Message Service (NMS) features

The following table lists the CallPilot features that are or are not supported by NMS.

CallPilot feature	Supported
Call Sender	Yes
Names Across the Network	n/a
Name Addressing	Yes
Name Dialing	Yes
Personal Distribution Lists	Yes
System Distribution Lists	Yes
Multiple Recipients	Yes
Reply To	Yes
Reply All	Yes
User’s Actual Personal Verification	Yes
Administrator-Recorded Personal Verification	Yes
Remote Site Spoken Names	Yes
Private Tag	Yes
Acknowledgment Tag	Yes
Urgent Tag	Yes
Received Time Announced	Yes
Sent Time announced	Yes
120-Minute Messages	Yes
Sender’s Name	Yes
Recipient’s Name (Text)	Yes

CallPilot feature	Supported
Message Subject (Text)	Yes
Sender's Department	Yes
Deferred Delivery	Yes

Recipient's Name (Text)

This feature is available for use if it is implemented on the local system. This feature is not available if the recipient is a user at a remote site and is not defined as a remote user.

Signaling

NMS has the following signaling considerations:

ISDN signaling

NMS uses the signaling capabilities of the ISDN primary rate access (ISDN PRA) and ISDN signaling link (ISL) to provide messaging servers. Therefore, NMS is subject to the assumptions and considerations of the ISDN Network Numbering Plan Enhancement feature.

If a non-PRA or -ISL trunk is involved in an NMS call, NMS is not supported, because the original called number and calling party number are not sent.

Virtual signaling

Virtual signaling is used between the prime switch and the satellite switches to

- Turn the Message Waiting Indicator (MWI) on and off at a user's telephone.
- Transport necessary call information for a networked voice messaging feature, such as Call Sender.

These capabilities are supported by using ISDN non-call associated transaction messages.

End-to-end signaling

End-to-end in-band signaling (EES) is required to access CallPilot features from a satellite switch.

ISDN Network Call Redirection

NMS is based on the Network Call Redirection (NCRD) features of the switch. Therefore, NMS is subject to the assumptions and considerations of the NCRD features.

Dialing plans

NMS supports the following dialing plans:

- Electronic Switched Network (ESN)
- Coordinated Dialing Plan (CDP)
- hybrid dialing plan, which combines ESN and CDP

NMS does not support another dialing plan, such as public switched telephone network (PSTN).

NMS dialing restriction scenarios

A uniform dialing plan is required for an NMS network. This requirement has important implications for implementing an NMS network and may require the re-configuration of an existing dialing plan.

The uniform dialing plan requirement applies in the following scenarios:

- calls to other users in the NMS environment
- calls to other users in the private messaging network but not part of the local NMS network
- calls to public switched telephone network (PSTN) users beyond the private messaging network

Dialing restrictions for calls within an NMS network

Dialing among all users on all switches in an NMS network must be done uniformly, but the ESN access code may be different.

Dialing restrictions for calls within a private messaging network

A uniform dialing plan is also necessary when an NMS network is a site in a larger private messaging network and the local users dial remote switch locations in the messaging network.

Dialing from all users on all switches in an NMS network to a remote site in the private network must be done uniformly, but the ESN code may be different.

Dialing restrictions for calls beyond the private messaging network

A uniform dialing plan is also necessary when local NMS network users call PSTN destinations.

The PSTN access code must be the same on all NMS locations.

Implications

Dialing plan restrictions for calls beyond the private messaging network have important implications for implementing an NMS network.

For all switches in an NMS network to dial PSTN destinations in the same way, the following must occur:

- All switches in the NMS network must be located in the same area code.
- All switches must be located close to one another.
- All switches must use the same prefixes to reach the PSTN.

If these requirements are not met, when a user in the NMS network dials a PSTN destination using features such as Thru-Dial, Call Sender, and Remote Notification, the system operation may not be as expected.

All switches must be located in the same country and area/city code

For example, switch A is in the 416 area/city code, and switch B is in the 905 area code. To dial from switch A to (416)597-1234, a user dials 95971234. However, a user on switch B must dial 614165971234. NMS is not supported in this environment.

All switches must be close to one another

For example, to reach the PSTN number (905)555-1234, a user on switch C may dial 619055551234. A user on switch D, however, may only dial 95551234. Because the switches have different local and long-distance dialing areas, and use different dialing formats to reach the same PSTN number, the dialing plan is not uniform. NMS is not supported in this environment.

All switches must use the same prefixes to reach the PSTN

For example, all switches in the NMS network must use the same local, long-distance, and international dialing prefixes. If users at switch E dial 61 for long distance and users at switch F dial 71, the dialing plan is not uniform and NMS is not supported.

Transmission times and traffic calculations

In this section

Overview 64
Message transmission times for analog protocols 64
Transmission times for messages containing text information 66
Transmission times for messages with Names Across the Network 67
Traffic considerations for VPIM Networking messages 67

Overview

Transmission time is the length of time it takes to transmit a message. Transmission times are an important consideration in networking, especially if long-distance toll charges are incurred when messages are sent to remote sites.

Factors affecting transmission times

Transmission times depend on several factors, including the following:

- the protocol used
- the number of recipients
- whether recipients are at the same site or different sites
- length of the message body
- whether the message contains remote user information for the Names Across the Network feature

Digital networking

The transmission times of digital messages depend on the amount of traffic on the network and the network connection bandwidth.

Transmission time concerns

There are two types of transmission time concerns:

- general issues that affect all CallPilot networking solutions
- issues that are specific to the nature of the message being sent

Message transmission times for analog protocols

The amount of time that a voice channel is used to transmit a networking message depends on the networking solution being used.

Assumptions

The following discussion of message transmission times in a messaging network is based on these assumptions:

- a network consists of three sites.
- five percent of recipients of composed messages are remote.
- the average message contains 40 seconds of voice.
- communication patterns among sites are symmetrical.

AMIS Networking messages

AMIS Networking messages are transmitted separately for each recipient (e.g. a message to ten recipients is transmitted ten times).

NMS messages

Within an NMS network, messages are not transmitted. All users on the switches that make up the NMS network are added as mailbox users on the CallPilot server. The CallPilot server functions as the message center for the NMS network. When a message is sent to one or more users within an NMS network, the message is deposited into each recipient's mailbox.

Transmission time comparisons

The following tables compare the transmission times when:

- all recipients are at the same site.
- there is one recipient at each site in the network.

All recipients at the same site

Number of recipients at receiving site	AMIS Networking	Enterprise Networking
1 recipient	54.4 seconds	76 seconds
10 recipients	544 seconds	111 seconds
50 recipients	2720 seconds	262 seconds

One recipient at each site

Number of sites	AMIS Networking	Enterprise Networking
1 site	54.4 seconds	76 seconds
10 sites	544 seconds	760 seconds
66 sites	2176 seconds	3040 seconds

See also

For more detailed information on traffic calculations, consult the *Planning and Engineering Guide*.

Transmission times for messages containing text information

VPIM Networking and Enterprise Networking can transmit the following text information with a message:

- sender name
- all recipient names
- message subject

CallPilot displays this information on the recipient's desktop.

VPIM Networking
Transmitting this information over a digital network with VPIM Networking has no real impact on transmission times.

Control of text information transmission

With Enterprise Networking, text information may take a long time to deliver.

You can define the sites to which text information can be sent. This is useful when the local site is exchanging messages with sites that incur long-distance toll charges. You can choose to send text to toll-free sites, but not to sites that incur long-distance toll charges.

Text information transmission times

The sender's and the recipient's names can be included as text in a message. Each name can consist of up to 19 characters. Each character requires two DTMF tones. Based on five DTMF tones per second, it may take as long as 7.8 seconds to transmit a single name.

Transmission times comparison

The following table compares the transmission times of a standard message and a message that includes text.

Number of recipients at receiving site	Standard message (in seconds)	Enterprise Networking message with text	VPIM Networking message with text
1	76	89.6 seconds	Not applicable
10	111	132.8 seconds	Not applicable
50	262	324.8 seconds	Not applicable

Transmission times for messages with Names Across the Network

The Names Across the Network feature is available with Enterprise Networking and VPIM. This feature provides the ability to have the spoken name of a message sender reproduced at the recipient site. The user at the remote site is added to the local network database and becomes a remote user.

The Names Across the Network feature adds the sender's spoken name to the message body.

When Names Across the Network information is sent

When an Enterprise Networking message is sent, the sending and receiving sites negotiate whether spoken names are to be sent.

If the system administrator of the receiving site has configured the site to receive Names Across the Network, the sending site includes the spoken name with the message. If the system administrator of the receiving site has configured the site not to receive Names Across the Network, the sending site does not send the spoken name. This results in a shorter transmission time.

For detailed information on Names Across the Network and remote users, consult Chapter 11, Configuring local and remote networking sites in this guide.

Traffic considerations for VPIM Networking messages

Traffic calculations

It is difficult to provide precise measurements for VPIM Networking traffic. Performance depends on the total CallPilot server load at any given moment. However, some indication of capacity can be provided.

Assumptions

These measurements are based on the following assumptions:

- the maximum number of messages created each minute is 96 for the entire CallPilot system.
- networking traffic does not exceed 10 percent of total data network traffic. Therefore, VPIM Networking is designed to handle approximately ten messages every minute.
- the average message length is 30 seconds.

Traffic calculations

The above assumptions lead to the following average traffic load on the IP network:

10 * 30 * 4 kbyte/60 s = 40 kbyte/s

The practical bandwidth of a typical LAN is approximately 1 Mbyte/s. This should be sufficient to support a network data rate of 40 kbyte/s.

Note: Peak traffic loads from VPIM could significantly exceed the average, should a message be sent to a large distribution list with recipients on many different messaging systems.

Remote users

In this section

Overview 68
Temporary remote users 69
Permanent remote users 70
How remote users are added or deleted 70
Adding remote users with Names Across the Network 71

Overview

Definition: Remote user

A remote user is a messaging user whose mailbox resides on a remote messaging system, networked to the local site, and who has been added to the directory of the local site. The presence of remote user information in the local system enables local users to message with the remote user transparently, as if they were also a local user on the same system.

It is important to distinguish between a remote user and a user at a remote site. A remote user is added to your database. A user at a remote site is not added to your database.

Benefits

There are many benefits to adding users from remote sites as remote users to the local site, including the following:

- When a user at the local site addresses a message to a remote voice user, the remote voice user's personal verification (spoken name) is played.
- Local users can use the Name Dialing and Name Addressing features to call and compose messages to remote voice users.
- While listening to a voice message left by a remote voice user, a local user can use Call Sender to call back the originator of the message immediately.
- External callers can name-dial remote voice users if this feature is enabled.
- Remote voice users can be added to system and personal distribution lists.

Example

Patricio Simpson is a local user at your office in Buenos Aires. Maria Andres is a user at the Berlin office. Maria has been added to the local site as a remote user.

Patricio can use name addressing when composing a voice message to Maria. During message addressing, he hears Maria's spoken name as a verification of the mailbox number he has entered.

When Patricio listens to a voice message from Maria, he presses 9, Call Sender, to call Maria back.

Status of remote users

You can grant a remote user temporary status or permanent status, and this can be changed as required.

The status that you grant to a remote user determines not only how the remote user works with the system. The status also determines, in part, how you administer the remote user.

Temporary remote user status

Temporary remote users are created by the Names Across the Network option of Enterprise and VPIM networking and are managed by the system. When system resources for remote users become limited, CallPilot automatically deletes the temporary remote users who have been inactive for a long time. This ensures that system resources are available to active users.

Permanent remote user status

Permanent remote users remain on your local system until you decide to manually delete them. Permanent remote users require more administration than temporary remote users.

Temporary remote users

A temporary remote user is a remote user who can be removed from the network database automatically.

When a remote user is granted temporary status, the remote user's position in the network database is determined by that user's activity and the needs of the system. If the system must delete some temporary remote users, it selects those users who have been inactive for the longest time. The temporary status simplifies the administration of remote users, since they can be added and deleted automatically by the system.

Temporary remote user capacity

The number of temporary remote users that can be added to the system is limited. The system capacity cutoff is the maximum number of temporary remote users that the local system can contain. The limit is 5000 temporary remote users. The system will accept more than 5000 temporary remote users during the day, however, temporary remote users in excess of 5000 must be removed from the system before the following day.

Example

Your system currently has 4990 temporary remote users. During the day, the system receives 40 additional temporary remote users. These are accepted by the system and 5030 remote users are able to use the system during that day. However, during the nightly audit, the system removes 30 temporary remote users, based on their time stamp records.

Time stamps and nightly audits

Every remote user has a time stamp, which is a record of the user's activity. An initial time stamp is created when a remote user is originally added to your local database. The time stamp is updated automatically when:

- the user is modified through User Administration
- an Enterprise Networking message is received from the remote user
- a remote voice user's personal verification, or mailbox number, is played

The nightly audit removes temporary remote users when the total number exceeds the system capacity of 1000 remote users. During the nightly audit, the remote users with the oldest time stamps are deleted in groups of 10 until the number does not exceed the capacity cutoff limit.

Protecting a temporary remote user from deletion

To ensure that a specific temporary remote user is not deleted from the database during the automatic nightly audits, you must change that user's status from temporary to permanent.

Permanent remote users

A permanent remote user is created by an administrator on the local system and remains there until manually deleted. Therefore, permanent remote users require more administration than temporary remote users. They must be manually maintained. The nightly audit, which automates much of the routine administration of temporary remote users, does not affect permanent remote users.

Since they take up system resources, permanent remote users should be active users. If a permanent remote user is not active, change the user's status to temporary and let the system automatically maintain the user's status.

There are two ways to verify when a remote user was last active:

- Check the last Access Time box in the View/Modify Remote Voice User dialog box.
- Use the Find function, and list all permanent remote voice users. Remote users can be selected and modified from the List dialog box.

How remote users are added or deleted

There are two ways to add remote users to your local database:

- Names Across the Network
- User Administration

It is likely that you will use both methods to add and administer remote users, depending on which is best suited to your particular needs.

Names Across the Network

Names Across the Network is available with Enterprise Networking and is an ideal way to keep temporary remote users up-to-date in your database. Temporary remote users are automatically added to the local system when they send messages to the local site if both the remote system and the local system are configured for Names Across the Network. Select this option when configuring your system to simplify the task of maintaining temporary remote users. This feature is explained in detail below.

User Administration

User Administration is used to add both temporary and permanent remote users. It is an entirely manual process that must be repeated for each individual user that you want to add or delete. It is the most appropriate method to use when you want to perform basic administration and maintenance on just a few users, but it is not practical when you are initially setting up your system and adding many remote users.

How remote users are deleted

There are two ways to delete a remote user from the local system:

- User Administration
- Nightly audits

User Administration

You can remove either permanent or remote users manually, one at a time, through User Administration. Permanent remote users remain on the local system until they are deleted in this way.

Nightly audits

Nightly audits are performed to ensure the temporary remote voice user database does not get too large. When the number of temporary remote users exceeds 5000, the oldest temporary remote users, indicated by their time stamps, are removed automatically.

Adding remote users with Names Across the Network

Names Across the Network is a feature that automatically adds temporary remote users to a local database and maintains them. You can only use Names Across the Network if Enterprise Networking is implemented on your system and at your remote sites.

Incoming and outgoing messages treated separately

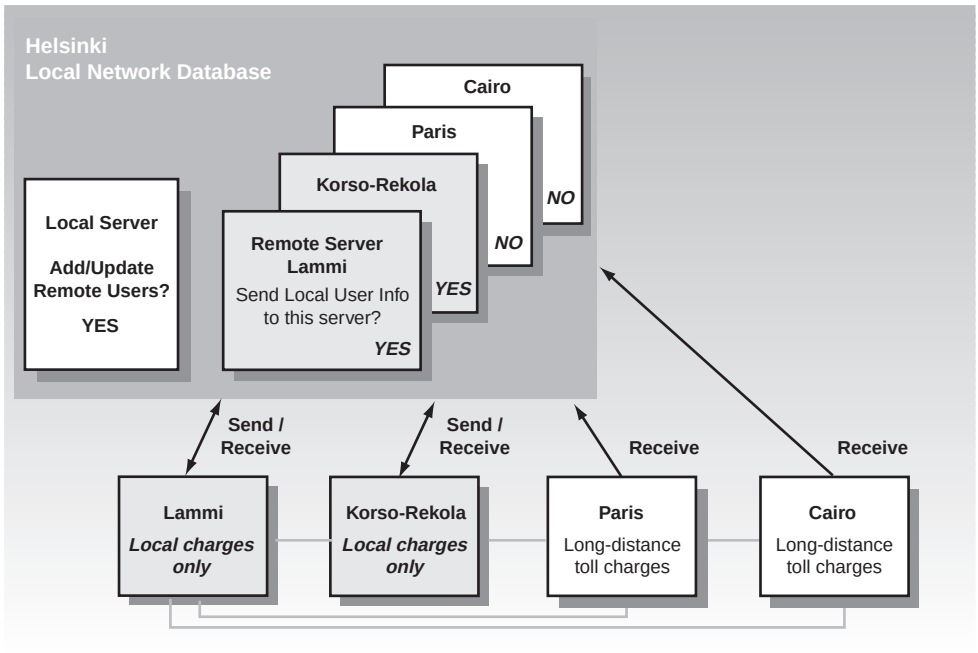
Names Across the Network is enabled for incoming and outgoing messages separately. A temporary remote user can be added when:

- a local user addresses a message to a user at a remote site
- a user at a remote site addresses a message to a local user

When you select Names Across the Network for incoming messages, you add temporary remote users from all sites in the messaging network. However, because outgoing messages must carry additional information with them, resulting in longer transmission times, you can select Names Across the Network for outgoing messages for individual sites. For example, you might enable the feature for outgoing messages to a site that will not incur long-distance toll charges, but disable the feature for a site that incurs these charges.

Example 1

The following example shows a messaging network consisting of five sites.

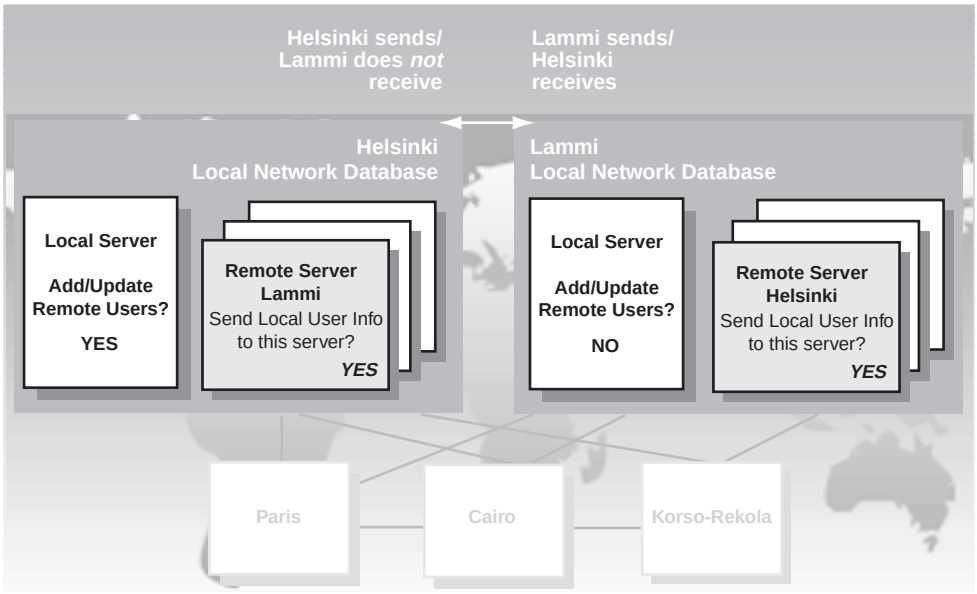


As the local administrator of the Helsinki site, you set your system to receives Names Across the Network. You receive messages from all other sites. However, when configuring information about the remote servers in your local database, you clear the Send Local User Information to this Server option for the sites that you do not want to send remote user information to. In this case, you do not want to incur the extra long-distance toll charges associated with Names Across the Network. Therefore, you clear the Send Local User Information to this Server option for Cairo and Paris.

However, Names Across the Network is also affected by the way the network administrator at a remote site configures the system.

Example 2

In the following example, the network administrator in Lammi decides to disable the Send Local User Information to this Server option when configuring the Helsinki remote server in the local messaging database. This means that even though you are willing to receive Names Across the Network information from Lammi, it is not sent to your site in Helsinki.



In this case, when a user from Helsinki sends a message to a user in Lammi, the Helsinki user is not added to the Lammi database as a remote user.

To add remote users with Names Across the Network

The setting to add remote users with Names Across the Network is on the Messaging Network Configuration dialog box for your local messaging server.

This setting controls your local server. You must coordinate with the system administrator of each remote site with which you want to enable Names Across the Network.

When remote users are added and updated

Names Across the Network adds a temporary remote user to the local site when a user at a remote site sends a network message to a user at the local site. The remote user information is taken from the header of the message that is received.

Considerations

Names Across the Network has the following considerations:

- Users at remote sites are added to your system as temporary remote users only when messages are received from them. Users at remote sites who do not send network messages are not added, even if they are regularly name-dialed or have messages sent to them.
- Operational measurements are not collected for remote users.
- If the sender's site does not have mailbox numbers that match the dialing plan, the Call Sender and Name Dialing features are not available.

- During the nightly audit, temporary remote users cannot be added or updated.
- Only 18 characters of the remote voice user's text name are sent.

WHEN	THEN
the first and last names are 18 characters or less	the first and last names of the user are sent.
the initials and last name are 18 characters or less	the initials and last name of the user are sent.

Outgoing Enterprise Networking sessions

When the local site initiates an Enterprise Networking session to a remote site, the two sites negotiate whether spoken names are sent. This negotiation occurs as follows:

IF	THEN
the local site chooses to send spoken names AND the remote site has selected the Add/Update Remote Users on this Server option	the local site includes the sender's text and spoken name with each message. The remote site adds or updates the sender's remote user information.
the local site chooses not to send spoken names AND/OR the remote site has not selected the Add/Update Remote Users on this Server option	the local site does not include the spoken names for the senders. The remote site does not add or update the sender's remote user information.

Time stamps updated

When a message is received from a user who already exists in the local database as a temporary remote user, the time stamp of the remote user is updated with the current date and time.

See also

For detailed information about user templates and how to add users, consult the online Help.

chapter 4

Dialing plans and networking

This chapter provides a basic overview of each supported dialing plan and explains what information is required to implement networking.

In this chapter

About dialing plans and networking solutions 76

Dialing plan information 89

About dialing plans and networking solutions

In this section

Overview 76
Uniform dialing plans 77
Nonuniform dialing plans 78
ESN dialing plan 80
CDP 82
Hybrid dialing plan—ESN and CDP combined 85
Another dialing plan 85
Dialing plans and addressing plans 85
Modifying dialing plan information 86
Modifying CDP steering codes 87

Overview

When you implement a networking solution, you provide detailed information about the dialing plan used by the local site. It is important to understand dialing plans and their component pieces when implementing a CallPilot networking solution in order to:

- gather the required information
- analyze the dialing plan information
- implement a networking solution

Definition: Dialing plan

A dialing plan is the set of rules used by a switch to route a call or message through a network to its destinations. Before CallPilot can deliver a message to a remote site, it must first determine where that site is and how to connect to it.

System perspective

From a system perspective, the dialing plan determines how to route a message to its proper destination.

User perspective

From a user perspective, the dialing plan determines how users address a message to another user in a private messaging network.

There are two main options. You can give every user in the network a unique mailbox number. Callers will only have to use this number to call another user in the network. However, in very large networks, this may not be feasible. Therefore, you can assign different switches in the messaging network a unique number. A user on a switch can have the same mailbox number as a user on another switch, because the switch number and the mailbox number combined create a unique identifier.

Dialing plan setup

When you begin to implement a networking solution, the dialing plan used by your local site is already configured on the switch. Therefore, during implementation you are simply reflecting the existing plan in your network database.

Even though the dialing plan is already set up, you must understand how to gather the dialing plan information from the switch. You must also understand the implications of the dialing plan for your messaging network.

Dialing plans

CallPilot networking works with four dialing plans:

- Electronic Switched Network (ESN)
- Coordinated Dialing Plan (CDP)
- hybrid dialing plan—ESN and CDP combined
- another dialing plan, such as PSTN

Location code

The basis of an ESN, CDP, or hybrid dialing plan is the location code. A location code is a unique identifier that indicates a particular location within a network. All dialing plans use a location code. However, *location code* is a generic term and specific dialing plans refer to it using different terms, as shown below.

For this dialing plan	the location code is called
ESN	ESN prefix ■ consists of ESN access code and ESN location code
CDP	CDP steering code

Uniform dialing plans

Regardless of which dialing plan is used, it is strongly recommended that you use a uniform, or standardized, dialing plan for your network.

Definition: Uniform dialing plan

A dialing plan is uniform when all users, regardless of which switch they are on, dial the same way to reach the same recipient. The only exception is that ESN access codes can be different.

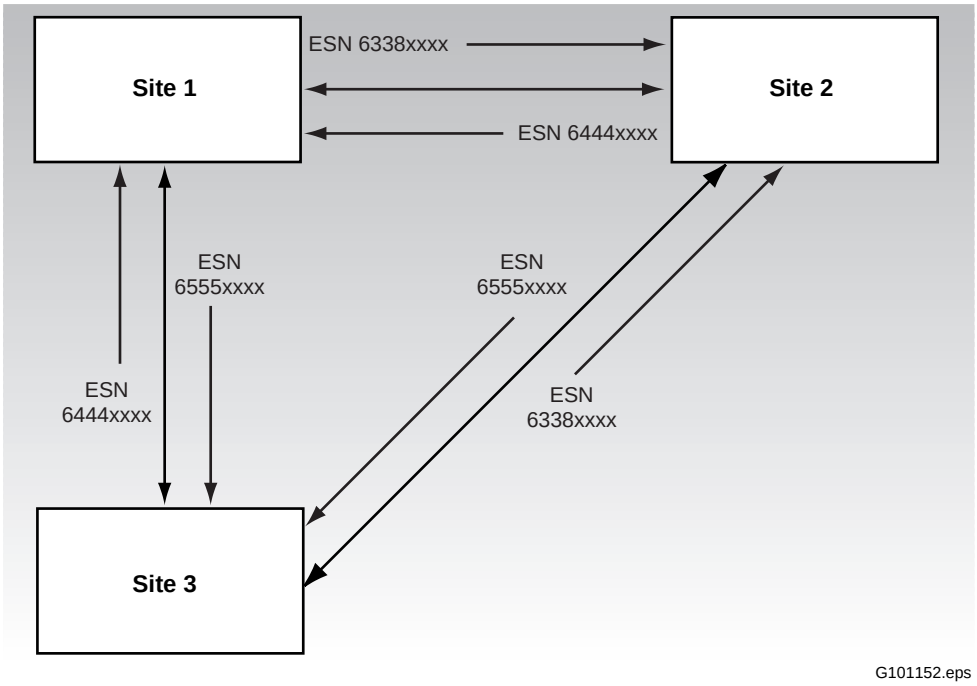
A uniform dialing plan offers the following benefits:

- the network is easier to configure and maintain.
- future growth of the network is allowed.
- users find it easier to use the network when visiting other sites.

If you are upgrading an existing system, analyze the current dialing plans. If necessary, modify them across the network to ensure a uniform dialing plan.

Example: Uniform dialing plan

The following diagram shows a uniform dialing plan. The messaging network uses an ESN dialing plan. Each site uses the same ESN prefix to reach the other sites in the network.



Nonuniform dialing plans

In some instances, creating a uniform dialing plan is not possible.

For example, suppose you are implementing CallPilot on an existing messaging network. If an established dialing plan is in place, it may be preferable to leave the nonuniform dialing plan alone. This ensures that users do not have to learn new ways to dial and exchange messages with one another.

However, a nonuniform dialing plan is not recommended and should be avoided whenever possible.

If it is not possible to design a uniform dialing plan, you should at least understand the impact of a nonuniform dialing plan on your messaging network configuration.

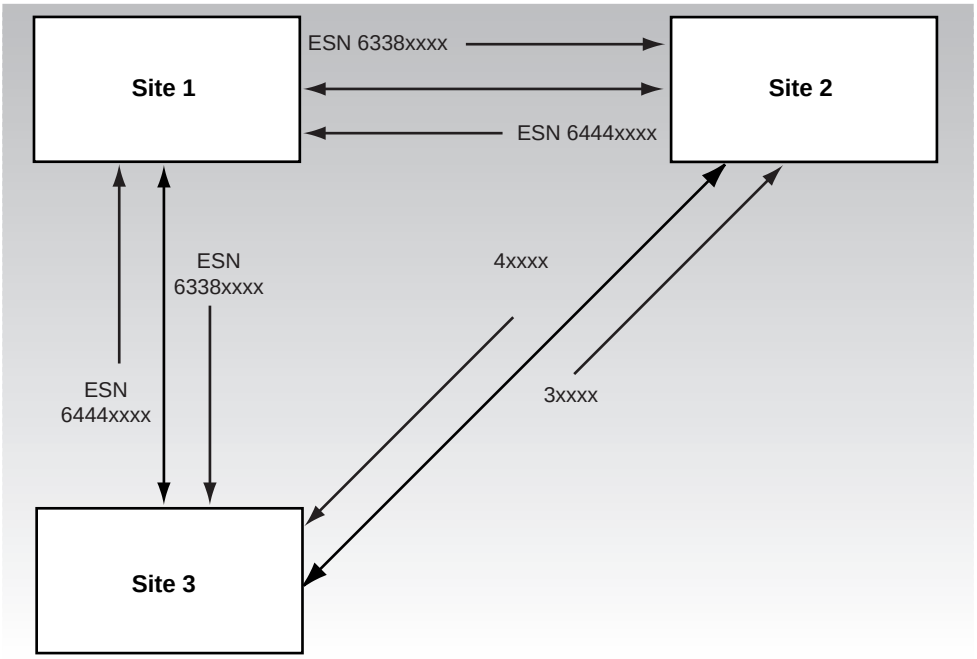
One of the biggest obstacles occurs as a messaging network with a nonuniform dialing plan grows. The network becomes increasingly difficult to administer and maintain. Users who visit different sites in the messaging network will have difficulties, because the dialing plan is unfamiliar.

Examples: Nonuniform dialing plan

The following diagrams show examples of networks that have nonuniform dialing plans.

Different addresses

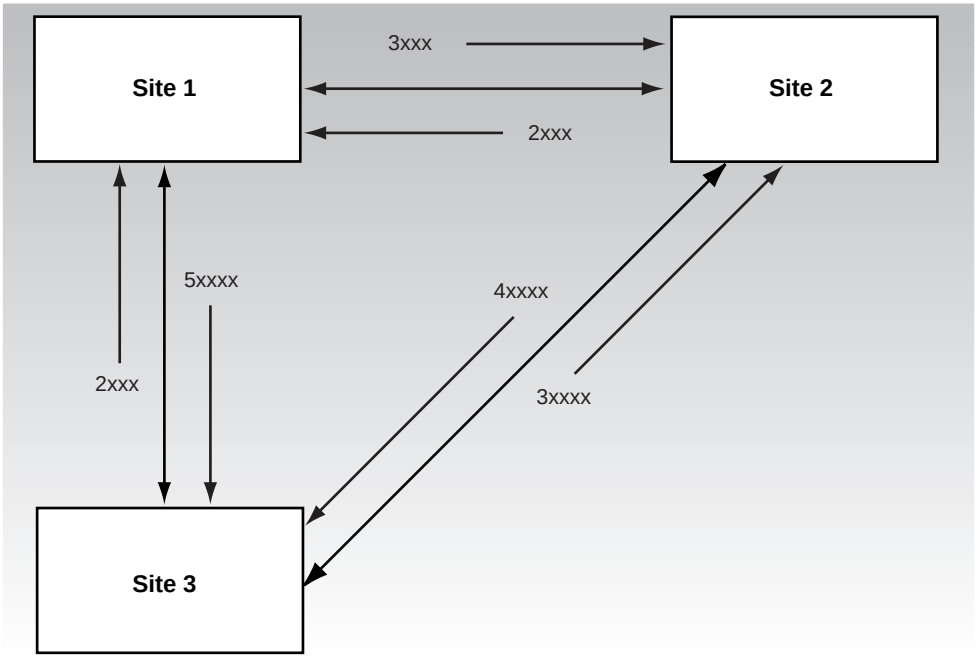
In this example, the dialing plan is nonuniform because users address sites in different ways.



Different CDP steering codes

A dialing plan is considered nonuniform if different sites in the network address other sites in different ways, including using CDP steering codes.

In this example, CDP is used throughout the network, but users at Site 1 send messages to Site 2 by entering 3xxxx, while users at Site 3 enter 4xxxx.



ESN dialing plan

Definition: ESN

An Electronic Switched Network (ESN) is a dialing plan used by organizations in a private messaging network.

ESN prefix

In an ESN dialing plan, every switch in the messaging network is assigned an ESN prefix. The ESN prefix can be up to seven digits long. The ESN prefix consists of:

- an access code
- a unique location code

Access code

An access code is used to access ESN routing in the same way an access code (often 9) is needed to dial out from a private network to a public network. An access code is usually one or two digits long.

Typically, all switches in an ESN network use the same ESN access code, although this is not required. Different ESN access codes do not make the dialing plan nonuniform. ESN access codes are similar to trunk access codes and are set independently for each switch.

Location code

The location code is a routing prefix that identifies a location within the network. It is usually three digits long but can be up to seven digits long.

Example:

- ESN access code = 6
- ESN location code = 444
- ESN prefix = 6444

Available directory numbers

To expand the range of available directory numbers, you can overlap the leading digits of the local extension with the trailing digits of the ESN prefix.

For example, the directory number 6644000 consists of the local extension, 4000, and the ESN prefix, 6644. The digit 4 is overlapped. It is both the first number of the extension and the last number of the ESN prefix. This overlap enables the use of local extensions in the 4000 to 4999 range.

Calling with an ESN dialing plan

The way a user calls another user depends on whether the recipient is at the local site or a remote site.

Local recipient

To make a telephone call to a user at the same site, the sender enters the extension number only.

Remote recipient

When a user makes a telephone call to a recipient at another site in the network, the ESN dialing plan is not transparent. The user enters additional numbers, the access and location codes, in addition to the recipient's mailbox number, to call a user at another site.

Addressing a message with an ESN dialing plan

An ESN message is addressed in the same way that an ESN call is placed.

Local recipient

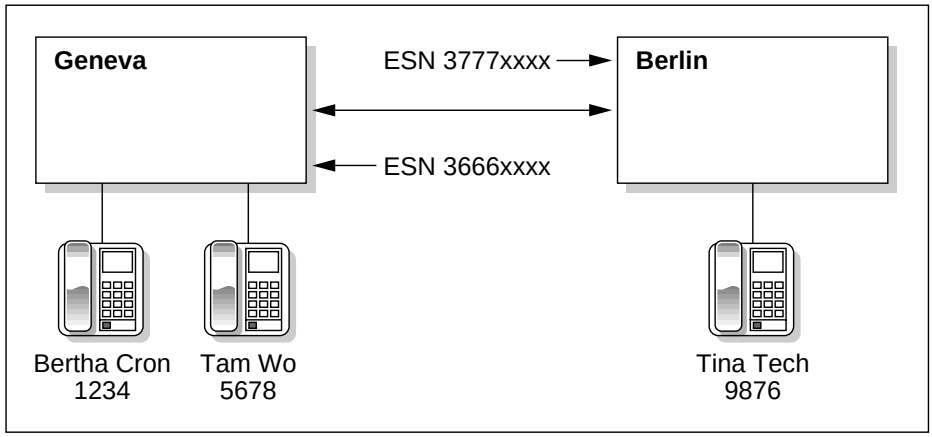
When a user addresses a message to a recipient at the same site, only the recipient's mailbox number is entered.

Remote recipient

When a user addresses a message to a recipient on another switch in the network, the user enters the access and location codes, as well as the recipient's mailbox number, to direct the message.

Example

To send a message to Tam, Bertha enters 5678. To address a message to Tina, Bertha enters the ESN prefix, 3777, and 9876.



Dialing plans and mailbox addresses

CallPilot uses the dialing plans as mailbox addresses if users have the same number for both their extension and their mailbox.

For	the mailbox consists of	Example
ESN	■ access and location codes. ■ user's extension.	■ access code = 6 ■ location code = 338 ■ mailbox number = 7460 ■ mailbox address = 63387460

CDP

A Coordinated Dialing Plan (CDP) is used by organizations in a private messaging network.

Definition: CDP

CDP is a switch feature used to coordinate the dialing plans of users on various switches in your messaging network.

CDP enables a user at one site to dial a user at another site by entering a unique number without access codes and associated pauses for dial tones. CDP is transparent to users.

To send a message to a recipient at the same site, a user enters the extension number.

When a user sends a message to a recipient on another switch in the network, the extension directory number is dialed. No additional numbers are needed, because the extension number itself contains a steering code that directs the call to the appropriate switch.

CDP codes

The number that a user enters to address a message consists of two parts:

- a CDP steering code (one to four digits long)
- the recipient's extension number (one to seven digits long)

Example

Patricia McKenna sends a message to Thomas Brish, who is located on the same switch. Patricia dials Thomas's full DN, 41112. When the system encounters the 4, it determines that the call is intended for a local user, strips off the 4, and sends the message to Thomas.

To send a message to Ana Trujillo, Patricia dials Ana's full address, 51234. When the system encounters the 5, it determines that the call is intended for a user at a remote site, and sends the message to Ana.

Definition: Steering code

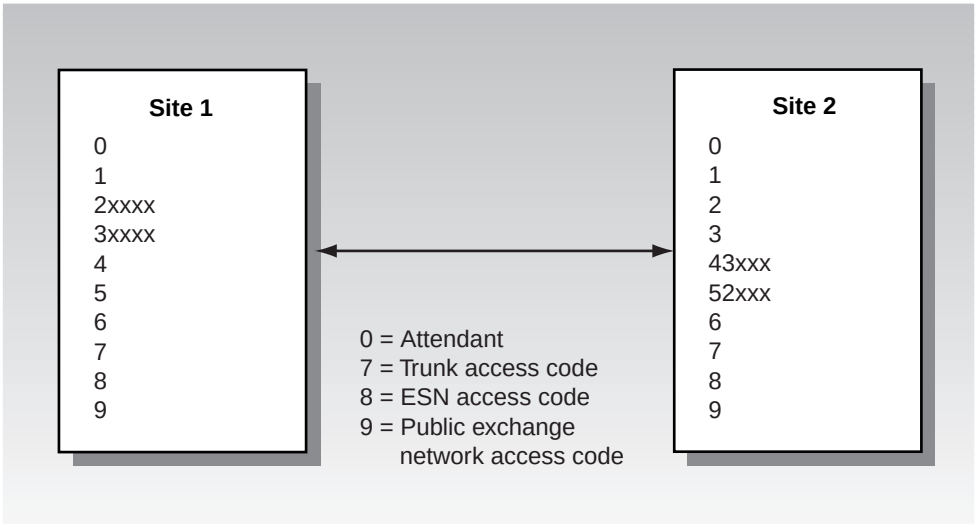
CDP uses steering codes. A steering code is a unique number that is entered by a user before the recipient's extension number. The steering code determines where the message is supposed to go. Each switch is assigned at least one steering code; each switch can have as many as 250 steering codes.

Unique steering codes

The steering codes on a switch must be different from any other assigned DN code on that switch.

The steering codes on a switch must also be different from the steering codes assigned on any other switch.

The following diagram shows an example of steering code availability for two switches. For Site 1, the digits 2–6 are available. Site 1 uses 2 and 3 for the steering code. Site 2 now has the digits 4–6 available. Site 2 uses 4 and 5 for the steering code. The digit 6 remains available.



G100975.eps

Creating steering codes

There are two ways to create a unique number from the CDP steering code and the extension number:

- Combine both parts.
- Keep both parts distinct.

A steering code and an extension number can overlap. For example,

- The extension number is 7121.
- The steering code is 7.
- The 7 is a single-digit overlap.
- A user enters 7121 to reach the recipient, not 77121.

This CDP setup is common. It is convenient for users because dialing any additional numbers is unnecessary, and only the recipient's extension number is required.

However, this CDP setup requires that every extension within the messaging network be unique. A user on one site cannot have the same extension as a user on another site.

The steering code and an extension do not have to overlap. For example, if the extension number is 8976 and the steering code is 44, there is no overlap. A user dials 448976 to reach the recipient.

How a CDP call is placed

To place a call to a recipient, the user dials the steering code followed by the recipient's extension number.

IF the call is being placed	THEN
to a user at the same site	the steering code is deleted, and the call is terminated locally.

IF the call is being placed	THEN
to a user at another site	the steering code identifies the recipient's site, and the call is terminated at the remote site.

Extension length

If the CDP steering code is two digits long and the mailbox directory numbers are three digits long, the total extension length is five digits.

If the length of the steering code and the mailbox directory numbers vary across the network, the total extension length must be the same.

For example, at Location 1 the steering code is one digit long and the mailbox directory numbers are four digits long. At Location 2 the steering code is two digits long and the mailbox directory numbers are three digits long. At both locations the total extension length is five digits.

Dialing plans and mailbox addresses

CallPilot uses the dialing plans as mailbox addresses if users have the same number for both their extension and their mailbox.

For	the mailbox consists of	Example
CDP	■ steering code and user's extension	■ steering code = 22 ■ mailbox number = 7460 ■ mailbox address = 227460
	■ steering code and user's extension that overlap	■ steering code = 7 ■ overlap = 1 ■ mailbox number = 7123 ■ mailbox address = 7123, not 77123

Hybrid dialing plan—ESN and CDP combined

A messaging network can use both ESN and CDP dialing plans. When both plans are used, the messaging network is said to use a hybrid plan.

Dialing plans and mailbox addresses

CallPilot uses the dialing plans as mailbox addresses if users have the same number for both their extension and their mailbox number.

For	the mailbox consists of	Example
ESN	■ the access and location codes. ■ the user's extension.	■ access code = 6 ■ location code = 338 ■ mailbox number = 7460 ■ mailbox address = 63387460
CDP	■ steering code and user's extension.	■ steering code = 22 ■ mailbox number = 7460 ■ mailbox address = 227460
	■ steering code and user's extension that overlap.	■ steering code = 7 ■ mailbox number = 7123 ■ mailbox address = 7123, not 77123

Another dialing plan

If ESN, CDP, or a hybrid dialing plan is not implemented, then the messaging network must use another dialing plan, such as PSTN. When another dialing plan is used, there are no private dialing codes. Therefore, a user must enter the following to send messages:

- trunk access code (such as 9)
- country and city/area code for long-distance
- exchange code
- mailbox number, typically the extension number

Dialing plans and addressing plans

When you implement a networking solution, you specify whether the dialing plan is the same as an addressing plan. If these plans are not the same, you must provide additional information.

ATTENTION!

It is strongly recommended that the dialing plan and the addressing plan be the same.

Dialing plan

A dialing plan specifies how a user makes a telephone call to another user.

Addressing plan

An addressing plan specifies how a user sends a message to another user.

Relationship

The following table shows the relationship between the dialing plan and the addressing plan.

Dialing plan	Addressing plan
ESN (for example, 6338xxxx)	Same as dialing plan strongly recommended
CDP (for example, 55xxx)	Same as dialing plan strongly recommended
Hybrid (for example, 6338xxxx, 55xxx)	Same as dialing plan strongly recommended
Another (for example, PSTN dialing prefix and mailbox, 61213777xxxx)	Choose either ■ format same as dialing plan, or ■ a shortcut (for example, 77xxxx)

Modifying dialing plan information

After a dialing plan is established it is rarely modified. Modifications to a dialing plan affect users and may require considerable retraining on the system.

However, in some cases modifications are necessary. In most cases, these modifications are guided by changes made by the switch technician. These changes might be local or remote.

Switch changes

If any changes to the dialing plan are made on a switch, the changes must be reflected in the network databases of all sites in the messaging network.

If changes are made locally, ensure that they are announced to all remote sites.

Messaging network changes

Modifications to the dialing plan are rarely guided by the network administrator. In most cases, the switch technician is responsible for changes to the dialing plan.

Modifying CDP steering codes

There may be instances when you must make modifications to the CDP steering codes.

For example, when a user in a messaging network moves from one site to another, the user can continue to use the CDP steering code of the original site. This makes it more convenient for other users who are attempting to reach the moved user.

However, this convenience for users requires considerable work by the switch administrators, system administrators, and network administrators.

ATTENTION!

It is strongly recommended that you weigh the benefits of modifying CDP steering codes for individual users before making the modifications.

Impact of modifications

Modifying CDP steering codes does not affect just the administration of the messaging network.The switches and the user administration records must also be modified.

Impact on switch settings

The switch changes should be made before you make changes to the CDP steering codes in the network database. Your changes must reflect the settings on the switch and cannot be done before the switch changes are made.

Impact on user administration records

Modifications to the CDP steering codes may also require changes to the basic system and User Administration. For example, if you are modifying the CDP steering codes because a user has moved from one site to another site, the following User Administration changes are required:

- The shared distribution lists (SDLs) at both sites must be modified.
- The user must be removed from the system and added to the other system.

Scenario

Tabitha Smithoc, a user in Cairo, moves to the Bahrain site. As Chief Financial Officer, it is important for her to keep her DN to make it easy for other users in the messaging network to reach her.

The Cairo site, which has exactly 1000 users, uses the extension DNs 7000 to 7999. The CDP steering code is 7, and the overlap is 1. Tabitha's extension DN is 7123.

The Bahrain site, which has exactly 1000 users, uses the extension DNs 8000 to 8999. The CDP steering code is 8, and the overlap is 1.

When Tabitha moves to Bahrain, the 7123 extension DN must be added to the Bahrain CDP steering codes as 7123, with an overlap of 4.

However, there is now a conflict between the steering codes in Cairo and Bahrain. Therefore, the CDP steering codes for Cairo must first be changed so that there is no possible conflict with the 7123 steering code used in Bahrain.

The CDP steering codes for Cairo must be changed to the following:

70, 72, 73, 74, 75, 76, 77, 78, 79 (not 71)

710, 711, 713, 714, 715, 716, 717, 718, 719 (not 712)

7220, 7121, 7124, 7125, 7126, 7127, 7128, 7129 (not 7123)

The network databases of all sites in the messaging network must be updated to reflect these changes.

In Bahrain, the CDP steering codes for the Cairo remote switch and the Bahrain local switch must be updated. In Cairo, the CDP steering codes for the Bahrain remote switch and the Cairo local switch must be updated. In Nairobi, the CDP steering codes for both the Cairo and the Bahrain remote switches must be updated.

Dialing plan information

In this section

Gathering dialing plan information 89
Create a messaging network representation 89
Examples of messaging network diagrams 90

Gathering dialing plan information

Gathering the required information is the first step in implementing every networking solution. Much of the required information is taken from the switch. The dialing plans that are configured on the switch for making telephone calls between sites are also used to exchange messages between sites.

Gather the dialing plan information and analyze it to make sure it is suitable for the networking solution you are implementing. Information from the switch must also be verified to ensure that it supports networking. Some of this information, such as dialing plan information, is used to configure CallPilot.

Refer to Chapter 9, Gathering information for a detailed description of the information gathering process.

Create a messaging network representation

The second major step in implementing any networking solution is to create a messaging network representation. A messaging network diagram is a graphical representation of your network. It shows all sites in the network, the protocols implemented at each site, how sites are connected, the protocol used between sites, location codes and names, and dialing plan information. If sufficiently detailed, a representation is the primary source of information used when implementing a networking solution.

For most messaging networks, a diagram is the most suitable form of representation. For very large messaging networks, however, a spreadsheet may be more appropriate.

Much of the information for your network representation must be provided by the administrators of other sites. For example, you need to know the site name and other information for every site. Although each site administrator creates a representation, ideally one site administrator should create a final version to distribute to all sites. This ensures that the representation is comprehensive and that each site uses the same information for implementation.

Remember also that your messaging network representation contains sensitive information. You should properly store and protect it as part of normal security procedures.

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 information required to implement a networking solution in one source
- provides useful information when planning future modifications
- helps during the analysis of traffic issues
- reveals areas where you can improve the messaging network

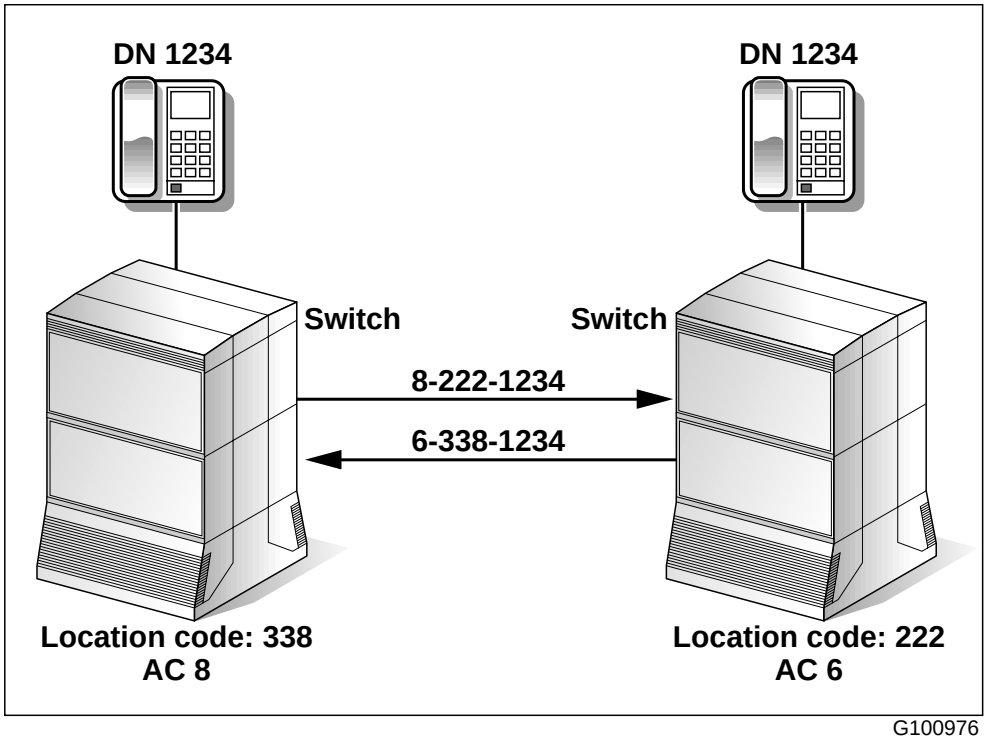
Examples of messaging network diagrams

The following examples of network diagrams show how each type of dialing plan is treated.

Typical ESN network diagram

A diagram of a typical ESN network provides information about the dialing plan and indicates how users send messages to each other.

In this diagram, users at one site dial the ESN access code, 6, the ESN location code 338, and the recipient's mailbox number to send messages to remote sites.

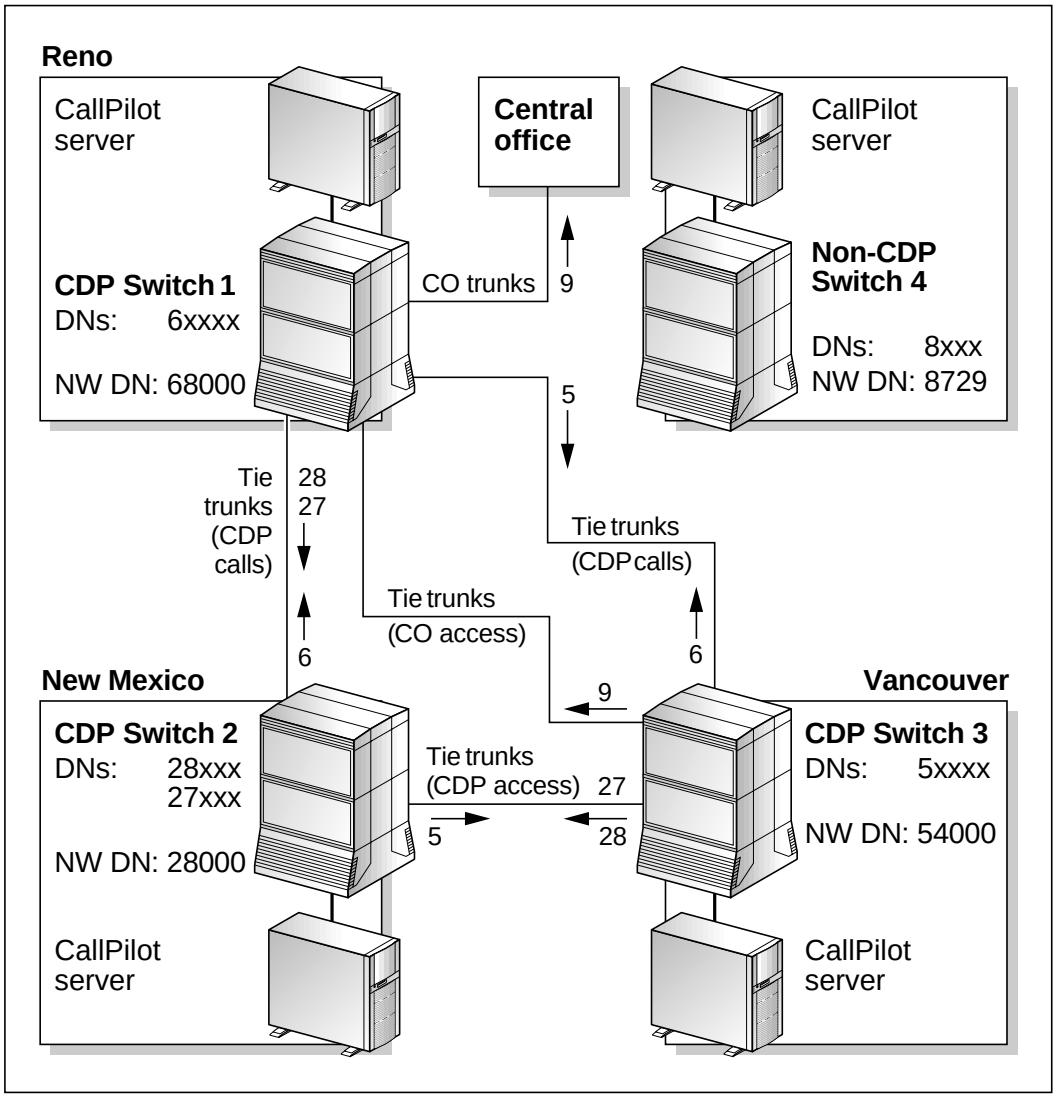


ESN network with an NMS site

When a messaging network includes an NMS site, it is important to include this information in the diagram. Information about all switches in an NMS network are entered when implementing a networking solution.

Typical CDP messaging network diagram

A diagram of a typical CDP messaging network provides information about the dialing plan and indicates how users send messages to one another.



In this example,

- the extensions in Reno are numbered 60000 to 69999, and the steering code is 6
- the extensions in New Mexico are numbered 27000 to 28999, and the steering codes are 27 and 28
- the extensions in Vancouver are numbered 50000 to 59999, and the steering code is 5

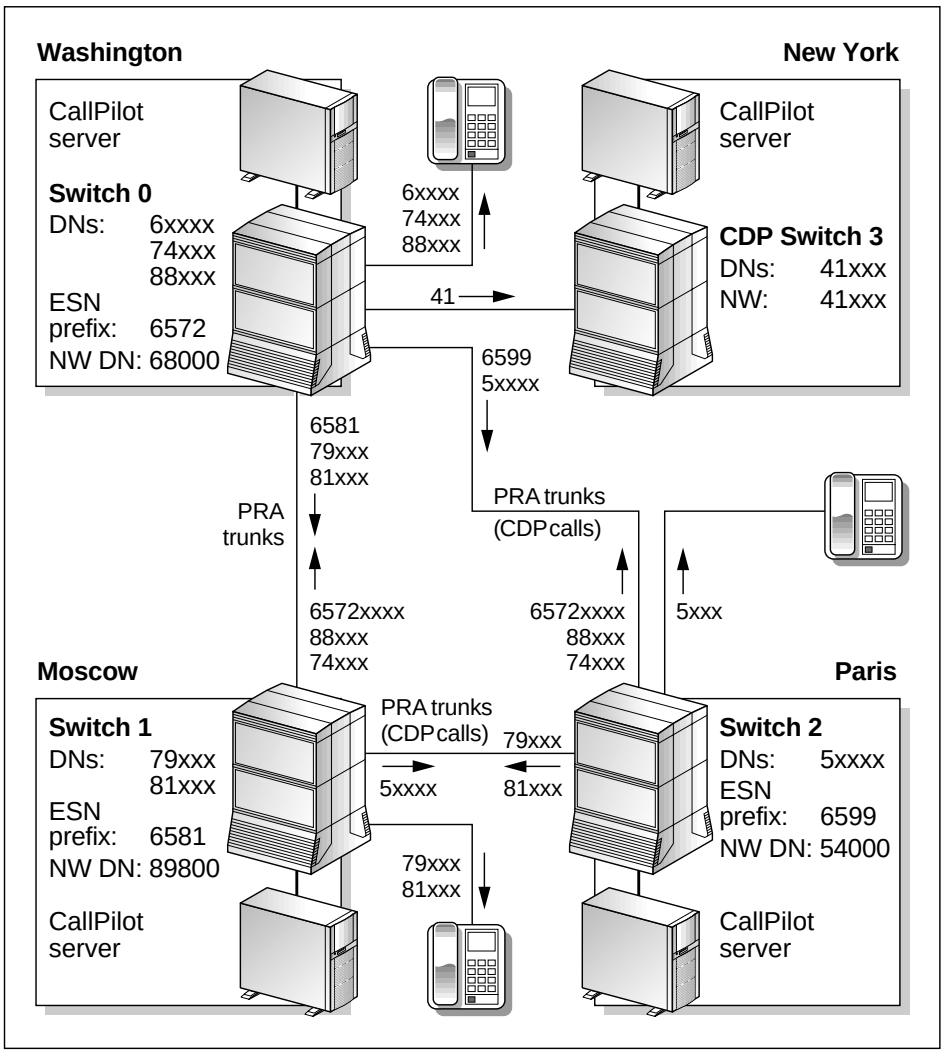
A user, regardless of site, uses the same extension to reach a particular user. For example, a user in Reno dials 27341 to send a message to a user in New Mexico. A remote prefix is not required because the first two digits of the extension, in this case 27, make up the steering code that identifies the site within the messaging network.

This diagram also shows that Reno provides centralized access to the public telephone network.

Hybrid messaging network diagram

A hybrid messaging network, which combines both ESN and CDP dialing plans, is often complicated. However, a messaging network diagram is an easy way to visualize how the sites exchange messages. By adding all dialing plan information to the diagram, you can see how the messaging network works.

In this diagram, Washington, DC, Moscow, and Paris support both ESN and CDP. New York supports CDP only.



How users send messages to other sites is described in the following table:

This site	dials
Washington, DC	Moscow with ■ 6581xxxxx using ESN. ■ 79xxx, 81xxx, 8xxxx using CDP. Paris with ■ 6599xxxxx using ESN. ■ 5xxxx using CDP.

This site	dials
Moscow	Washington with ■ 6572xxxxx using ESN. ■ 74xxx and 88xxx using CDP. Paris with ■ 6599xxxxx using ESN. ■ 5xxxx using CDP. New York with ■ 41xxx using CDP.
Paris	Washington with ■ 6572xxxxx with ESN. ■ 74xxx and 88xxx using CDP. Moscow with ■ 6581xxxxx using ESN. ■ 79xxx and 81xxx using CDP. New York with ■ 41xxx using CDP.
New York	Washington, DC with ■ 74xxx and 88xxx using CDP. Moscow with ■ 79xxx and 81xxx using CDP. Paris with ■ 5xxxx using CDP.

Messaging network with another dialing plan

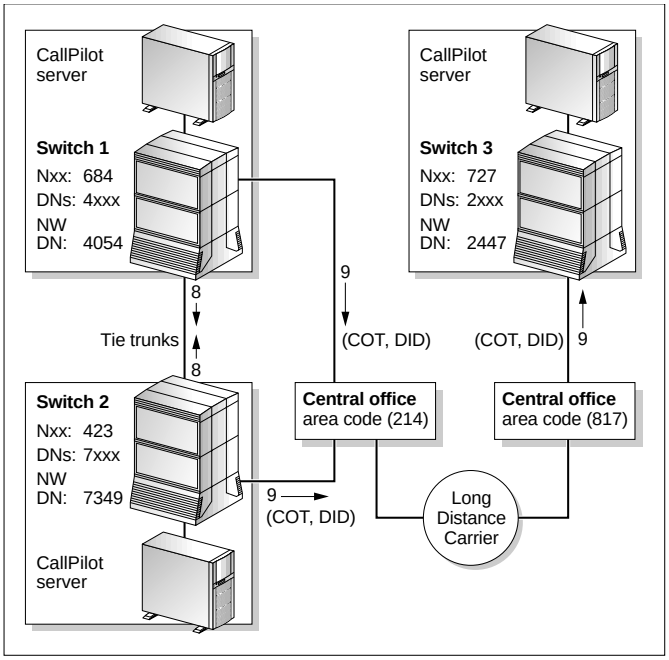
If your messaging network is not using ESN, CDP, or a hybrid dialing plan, you are using another dialing plan.

If you are using another dialing plan, you must use an alternate means of addressing messages. You can do this by designating a mailbox prefix for the site.

Users have some means of dialing the users at the site. For example, they can use an access code and a public switch number. The call may have to travel through a switchboard if the users are not directly dialable. You can set the mailbox prefixes to something related to the dialing plan if you want to make it easier for users to remember what to enter. For example, for a system in the 416 area code, use the prefix 8416.

Example 1

The following diagram illustrates a messaging network that uses another dialing plan, in this example, tie lines.



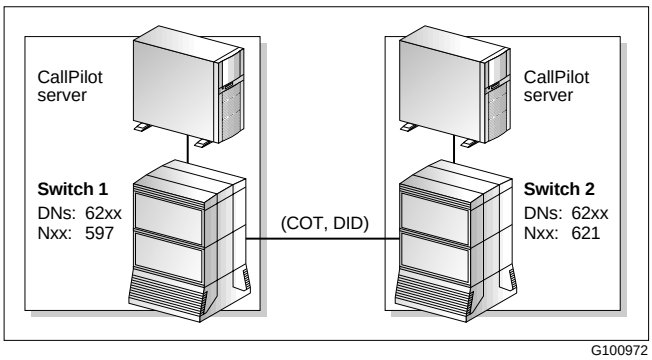
When a messaging network uses another dialing plan, sites may be configured to use different dialing prefixes to reach a specific remote site. However, CallPilot is unable to represent the dialing plan. A tie line between sites is an example of a network without a representable dialing plan. In this case, a mailbox prefix should be entered to allow users to compose to mailboxes at the remote site, because the mailbox numbering plan is independent of the dialing plan. When there is no specified dialing plan, CallPilot uses the trunk access code and the following:

For	the access code is followed by
long-distance calls	NPA + Nxx + xxxx
local calls	Nxx + xxxx
tie-line calls	xxxx

When entering network connection DNs for remote sites, you must provide for this format.

Example 2

The following diagram shows another network with another dialing plan. In this network, each site uses the same extension directory numbers. The exchange code makes each site in the network unique.



chapter 5

Network and location-specific broadcast messages

In this chapter

Types of network broadcasts 95

Broadcast message addresses 98

User capabilities for broadcast messages 99

CallPilot server capabilities for broadcast messages 100

Broadcast messages in a mixed messaging network 102

Viewing or printing all broadcast addresses 104

Types of network broadcasts

The CallPilot network broadcast feature enables a phoneset, or desktop or web messaging user to send a broadcast message to:

- all users at a specific network location (location broadcast)
- all users in the network (network broadcast)

This feature is in addition to the existing broadcast feature, which allows local users to send a broadcast message to all local users (including NMS users) on the CallPilot server (local broadcast).

Note: In order for a user to be able to send a local or network broadcast, their mailbox profile must have that privilege enabled. Typically, only a few users are given the right to send broadcast messages.

Broadcast requirements

To send a broadcast message, the following criteria must be met:

- The message must be addressed to the appropriate broadcast address.

  If the local user wants to send a broadcast message to all NMS locations associated with a remote site, the user must address the message to each location. To simplify this task, the user can create a personal distribution list containing the location-specific broadcast address for each location.

  Note: Broadcast addresses cannot be added to shared distribution lists (SDLs).
- The user must have sufficient capabilities as determined by his or her mailbox class.
- Broadcast messages must be enabled between the local CallPilot server and remote voice messaging systems.
- Broadcast messages must be supported on both the local CallPilot server and remote voice messaging system. For more information, see Broadcast messages in a mixed messaging network on page 102.

Location broadcast

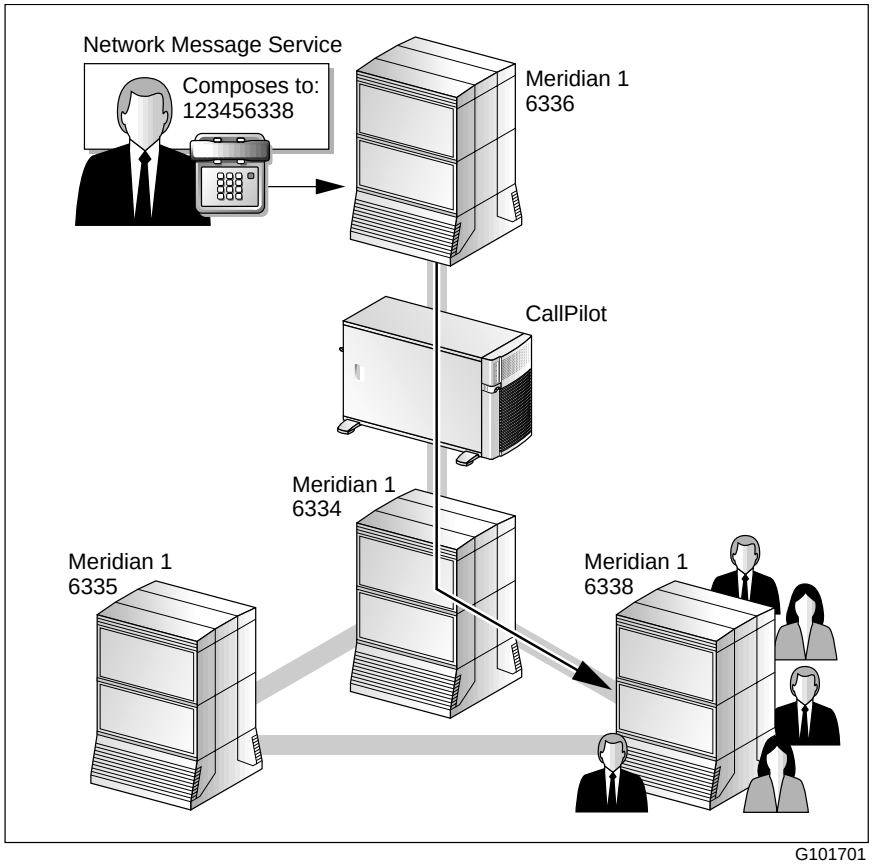
When a user sends a location broadcast, the message is delivered only to the users at the specified location. In this context, the location can be a remote site, or it can be a Network Message Service location associated with either a local or remote site.

Broadcast sent to a specific remote site

When a user sends a location broadcast to a remote site, the network broadcast prefix and the location prefix defined in the network database for the prime switch location at the remote site must be used. For this and the following examples, 12345 is the network broadcast prefix and 6338 is the prime switch location prefix.

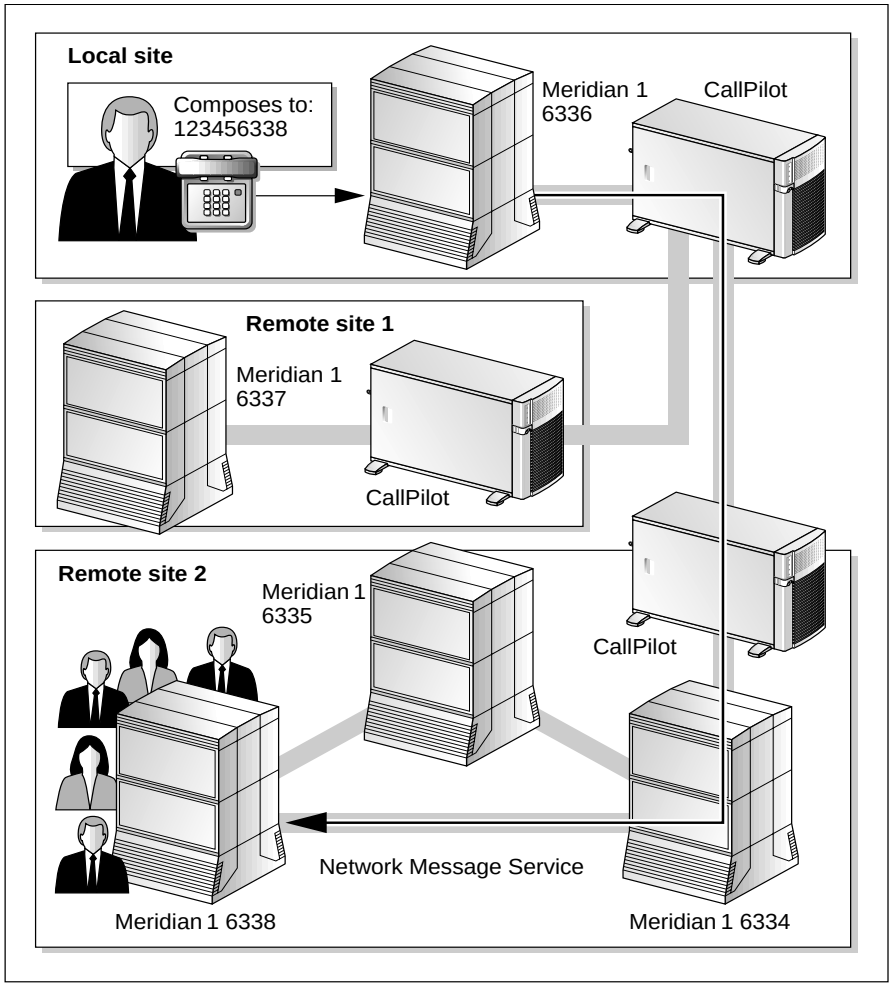
Broadcast sent to an NMS location at the local site

In the following illustration, the CallPilot system provides messaging services to four Meridian 1 switches at the local site. All users who are connected to these switches have mailboxes on the CallPilot system. 12345 is the network broadcast prefix and 6338 is the location prefix defined in the network database for the prime switch location. The location-specific broadcast is targeted to only the users whose phonesets reside at the switch location identified by the 6338 location prefix:



Broadcast sent to an NMS location at a remote site

In the following illustration, the CallPilot system at remote site 2 provides messaging services to users on three Meridian 1 switches. The location-specific broadcast is addressed by a user on the local CallPilot system to only the users whose phonesets reside at the switch location identified by the 6338 location prefix.

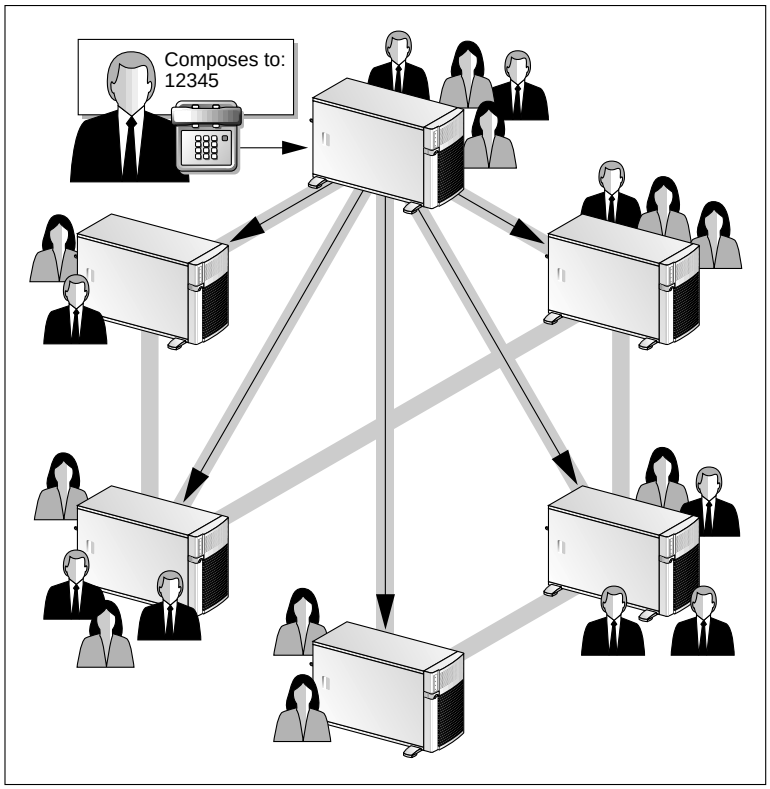


Note: If the local user wants to send a broadcast message to all NMS locations associated with a remote site, the user must address the message to each location. To simplify this task, the user can create a personal distribution list containing the location-specific broadcast address for each location.

Network broadcast

When a user sends a network-wide broadcast, the message is delivered to all users at both local and remote sites. This is accomplished by addressing the message to the network broadcast prefix.

In the following diagram, 12345 is the network broadcast prefix:



Broadcast message addresses

The following table shows the types of broadcasts, including local broadcasts, and how they are addressed.

Broadcast type	Address	Example
Local broadcast	Broadcast mailbox	5555
Network-wide broadcast	Network broadcast prefix	12345
Location-specific broadcast	Network broadcast prefix + Location prefix	12345+6338

Broadcast address rules

Network broadcast prefix

The network broadcast prefix must be between 5 and 18 digits long. The minimum length helps prevent users from accidentally composing network-wide broadcast messages.

The network broadcast prefix cannot conflict with any other prefix defined on the system. This includes, but is not limited to, the following:

- Open AMIS Compose Prefix
- Open VPIM Compose Prefix

- Delivery to Telephone (DTT) and Delivery to Fax (DTF) prefixes
- Name Dialing and Name Addressing prefixes
- network prefixes (ESN, CDP, and mailbox prefixes)

Location prefix

The location prefix is the portion of the telephone number that the user must dial to reach a user at a specific location. For example, if your dialing plan is ESN, the location prefix consists of the ESN access code used to make outgoing calls from your location (for example, 6), and the location code for the remote location (for example, 338).

For more information about dialing plans, refer to your switch documentation.

User capabilities for broadcast messages

To send a broadcast message, the user must have the appropriate mailbox capability. If CallPilot is configured to use authentication, and the user is a desktop or web messaging user, SMTP authentication must be successful before the broadcast message is sent to the remote destinations.

Mailbox capabilities

Each user must have one of the following capabilities in the mailbox class:

Broadcast capability	Description
Local broadcast only	The user can send broadcast messages to users at: ■ the local site ■ a specific NMS location associated with the local site (if Network Message Service has been installed)
Local and network broadcasts	The user can send broadcast messages to users at: ■ the local site (local broadcast) ■ a specific remote site (location-specific broadcast) ■ a specific NMS location associated with either the local or a remote site (if Network Message Service has been installed; location-specific broadcast) ■ all sites in the network (network-wide broadcast)
Disabled	The user cannot send any type of broadcast message.

Note: If Networking is not installed, the only options available for broadcast capability are enabled and disabled. When broadcast capability is enabled on a site that does not have networking installed, local broadcast capability is provided.

Distribution lists

Shared distribution lists

Broadcast addresses cannot be added to shared distribution lists (SDLs).

Personal distribution lists

Users can include broadcast addresses in their personal distribution lists (PDLs) according to their mailbox capability. If a user without broadcast capability attempts to add a broadcast address to his or her PDL, CallPilot informs the user that the address does not exist.

If a user wants to send a broadcast message to two or more NMS locations that are associated with a remote site, the user must address the message to each location, because each location has its own location prefix in the dialing plan. To simplify this task, the user can create a personal distribution list containing the location-specific broadcast address for each location.

Mailbox class validation for phoneset users

For phoneset users, the mailbox class includes an option to "send messages via DTT if mailbox not found." This option determines the type of system prompt that a user without broadcast capability hears when attempting to address a broadcast message. The user may hear one of the following prompts:

- "Phone number <string entered by user>."
- "There is no mailbox at <string entered by user>."

For security reasons, the prompt does not state that the address is a broadcast address or that the user does not have permission to send the broadcast message. Indication that the address is a broadcast address is valuable information for a hacker.

Mailbox class validation for desktop and web messaging users

The desktop or web messaging client cannot validate a user's mailbox class while sending a message. The message must be sent from the user's desktop to the CallPilot server before mailbox class validation can occur. If CallPilot determines that the user is not allowed to send the broadcast message, the user receives a non-delivery notification (NDN).

For security reasons, the NDN states that the address was not found. It does not state that the user did not have permission to send the broadcast message or suggest that the address is a broadcast address. Indication that the address is a broadcast address would be valuable information for a hacker.

SMTP authentication

To send a location-specific or network-wide broadcast message, a desktop or web messaging user must have the appropriate mailbox capability and be successfully SMTP-authenticated. If SMTP authentication fails while sending the message, the user receives an error message.

Note: For more information about SMTP authentication, see Chapter 12, "Security and encryption."

CallPilot server capabilities for broadcast messages

If Networking is installed on your CallPilot server, then users can send and receive both network-wide and location-specific broadcast messages, if broadcast capabilities are granted at both the user mailbox and CallPilot server level.

If only Network Message Service is installed on your CallPilot server, then users can send only local and location-specific broadcast messages, if broadcast capabilities are granted at the user mailbox level. Location-specific broadcast messages can be sent to any prime or satellite switch location in the local NMS network.

Levels of control

By default, broadcast capabilities at the CallPilot server level are enabled for VPIM and Enterprise Networking. If the networking protocol between the local and remote site is AMIS Networking, broadcast capability is not available because network-wide broadcast and location-specific broadcast are not supported by the AMIS protocol.

You can disable the exchange of broadcast messages between the local CallPilot server and remote voice messaging systems. When you disable the exchange of broadcast messages on the local server, you can quickly and temporarily turn off broadcasts without modifying other CallPilot settings.

You can control the exchange of broadcast messages in the local CallPilot networking database under Messaging ›- Message Network Configuration, as follows:

Where	How
On the local CallPilot server	Enable the following options, as required: ■ Send network broadcasts ■ Receive network broadcasts Both settings apply to the following broadcasts: ■ network-wide broadcasts ■ location-specific broadcasts to and from all locations associated with remote sites **Note:** Location-specific broadcasts to local locations are exempt because these types of broadcast messages are not actually sent over the network.
For each remote server that is defined in the network database	Enable the following options, as required: ■ Send network broadcasts to this server ■ Receive network broadcasts from this server Both settings apply to the following broadcasts: ■ network-wide broadcasts ■ location-specific broadcasts to and from this remote site ■ location-specific broadcasts to and from locations associated with this remote site

When to disable broadcast messages between sites

Use the following guidelines to determine when you should disable broadcast messages between the local and one or more remote servers:

Disable broadcast messages	when
to the local server	■ you observe a security breach, such as a hacker attempting to send messages to the local server. ■ you do not want to receive broadcast messages from remote servers.

Disable broadcast messages	when
from the local server	all users should not be allowed to send broadcast messages to other sites. For example, a small sales office may not be permitted to send network broadcast messages, whereas the corporate head office site can do so.
to a remote server	■ the remote server does not support network-wide and location-specific broadcasts. For more details, see Broadcast messages in a mixed messaging network on page 102. ■ the remote server does not want to receive broadcast messages from the local server.
from a remote server	■ you observe a security breach, such as a hacker attempting to send messages to the local server while pretending to be at the remote server. ■ you do not want to receive broadcast messages from the remote server.

Note: Another reason to disable broadcast messages is when you want to prevent high usage of network and CallPilot resources (network traffic, channel usage, and CPU resource usage).

See also

SMTP authentication can also restrict network broadcast messages from remote servers that are not required to authenticate before transmitting messages to the local CallPilot server. For more details, see Unauthenticated mode on page 219.

Broadcast messages in a mixed messaging network

If your messaging network contains a mixture of voice messaging systems, this may affect the ability for users to send network-wide and location-specific broadcast messages to other locations.

The type of content that a broadcast message can contain (voice, fax, or text) is affected by:

- the networking protocol used between two servers
- the networking solutions installed on your server
- whether the receiving server supports the content

Broadcast support between systems

The following table identifies whether network-wide and location-specific broadcast is supported on a specific type and release of voice messaging system:

Messaging system type	Network-wide broadcast	Location-specific broadcast
CallPilot 2.0 or later	yes	yes
CallPilot 1.0x	no	no

Messaging system type	Network-wide broadcast	Location-specific broadcast
■ Meridian Mail 12 ■ Meridian Mail 13	yes	yes
Meridian Mail 11	yes	no
Meridian Mail 11 and later *with* Meridian Mail Net Gateway	yes	no
Meridian Mail 10 and earlier	no	no
Norstar VoiceMail	no	no
Business Communications Manager 2.5	no	no
Voice messaging systems from other vendors	no	no

The type of network broadcast supported between two specific servers is the lowest common denominator of what both servers support. For example, only network-wide broadcast is supported between CallPilot 2.0 and Meridian Mail 11.

Multimedia support between systems

All types of broadcast messages can contain voice, fax, or text. However, to successfully arrive at their destinations, the following requirements apply:

- The networking protocol used to send the broadcast message must support the transmission of the content.
- The remote server must support the receipt of the content.

Example 1: VPIM Networking

VPIM Networking supports the transmission of voice, fax, and text messages. Therefore, broadcast messages can contain voice, fax, or text. However, if the receiving server does not support the content, a non-delivery notification may be returned to the sender.

Example 2: Enterprise Networking

Enterprise Networking supports the transmission of voice content only. Therefore, if a user composes a broadcast message containing fax or text, and the message is to be transmitted using the Enterprise Networking protocol, the message is rejected and the sender receives a non-delivery notification.

Example 3: AMIS Networking

AMIS Networking does not support network broadcast messages.

Broadcast message content policy

You should establish a policy for the type of content that users can include in a network broadcast message, and communicate this policy to your users. You can partially enforce the policy by granting desktop messaging and fax capability in each user's mailbox class.

Viewing or printing all broadcast addresses

To compose broadcast messages and ensure they arrive at the correct destination, users must know the broadcast addresses. It is relatively simple to remember the local broadcast mailbox and network broadcast prefix because there are only two numbers to memorize.

However, it becomes more complex for location-specific broadcast messages, because each site or NMS location in the network database has its own location prefix.

Viewing the broadcast addresses used by each switch location

Location-specific addresses can vary depending on the location from which the broadcast message is composed. The Print Broadcast Addresses page in CallPilot Manager contains a list box that lists all local switch locations. By default, the list is shown from the local prime location's point of view. To view the broadcast addresses from a particular local satellite location's point of view, you choose the satellite location from the list box.

Note: The Print Broadcast Addresses page also shows, for your reference, the local broadcast mailbox and network broadcast prefix used by the local server.

chapter 6

About Network Message Service

In this chapter

Overview 105
Dialing plans and NMS 109
Implementing NMS 111
NMS time zone conversions 115

Overview

Network Message Service (NMS) is a CallPilot feature that enables one CallPilot Server to provide messaging services to users in a network of compliant switches. The collection of switch locations, connections, and the messaging server is collectively known as an NMS network. An NMS network consists of the CallPilot Server, a prime switch location, and two satellite switch locations. Only the prime switch location is directly attached to the server.

An NMS network is often a site within a more complex messaging network. When an NMS network is part of a messaging network, it is called an NMS site. A messaging network can have many NMS sites.

An NMS network is a type of private messaging network that is set up and maintained by an organization for private use. In a typical private messaging network, every switch is connected to a messaging server. Users connected to a switch have mailboxes and can exchange messages with other users connected to the same switch. Users can also send messages to users on other switches in the network.

The following terms are used in discussions of NMS:

Term	Definition
NMS network	■ The interconnected switches and the CallPilot Server
NMS site	■ An NMS network when it is part of a larger messaging network in which each site has its own server
Prime switch location	■ The switch location directly attached to the CallPilot Server
Satellite switch location	■ A switch location that is directly connected to the prime switch
Tandem switch location	■ A switch location that is connected between the prime switch location and a satellite switch location

Term	Definition
User location	■ A logical grouping of mailboxes; may be the mailboxes on one switch or the mailboxes on two or more switches

Prime switch location and satellite switch locations

The switches are connected by Integrated Service Digital Network (ISDN) primary rate access (PRA), and ISDN signaling link (ISL) trunks. The prime switch communicates with the satellite switches with the D channel of Primary Rate Interface (PRI) (64 kbit/s).

The prime switch location and the satellite switch locations communicate through virtual signaling to turn the Message Waiting Indicator (MWI) on a user's telephone on and off. Virtual signaling is also used to transport necessary call information for a networking voice message feature, such as Call Sender. These calls are supported by using ISDN noncall-associated transaction signaling messages.

Prime switch location and CallPilot Server

The CallPilot Server is connected to the prime switch with two connections, one for voice and one for data. The CallPilot Server communicates with the prime switch using the Application Module Link (AML) protocol. If the AML link fails, NMS calls are routed to the default ACD DN configured for the CDN (DFDN).

Note: AML was previously known as Command and Status Link (CSL) and Integrated Services Digital Network/Applications Protocol link (ISDN/AP).

Switches and NMS

Switches provide the call handling required by CallPilot. All switches that are used by NMS are already configured and tested when you begin to implement NMS. However, you must check this configuration to determine if it is suitable for NMS. You must also do additional configuration to enable functionality that is required by NMS.

Confirming the Network Class of Service

On each switch location in the NMS network, confirm that the Network Class of Service (NCOS) level is adequate for NMS. If an NCOS level is inadequate, NMS may not work. A Network Class of Service level is a switch setting that controls access to trunks and call queuing. It also provides users with expensive route warning tones.

NCOS and NMS

NMS requires that the system be able to dial within the NMS network. Therefore, ensure that the NCOS level is sufficient to support a CallPilot system with all features. The NCOS level must allow the system to dial out of a switch location for Call Sender and Thru-Dial, but not create possible security breaches.

NMS access mechanisms

Desktop user logon

NMS is designed to be transparent to users. Users on one switch use the messaging system in the same way as users on all other switches and have access to the same features. The only time NMS is not transparent is when a desktop user logs on to the system. When desktop users at non-NMS sites log on to CallPilot, they enter their mailbox number and their password only. However, the first time desktop users at NMS sites log on to the system, they must also select their location name from a drop-down list. The location name is the name assigned to their switch location. After the first logon, the selected location name becomes the default.

Direct access

Direct access is initiated by a user dialing an NMS directory number, either by switch or network, or by pressing the Message Waiting key. Auto-logon on NMS is supported if the call is initiated from the user's station. For a direct access call, the call is presented to CallPilot at the prime switch through direct switches. This is a basic ISDN call that requires noncall-associated ISDN Q.931 messages.

However, to support NMS features that require transaction signaling to transport the noncall-associated information, such as Message Waiting Indicator notification and the Call Sender feature, the configuration between the originating switch and the prime switch must support the NMS transaction signaling transport. If the path used to transport the noncall-associated messages is relayed through a switch that does not support NMS transaction signaling, NMS is not supported.

Indirect access

Indirect access is initiated when a call is presented to NMS through call redirection. For any call redirected to NMS, the original called number from the ISDN Q.931 SETUP message is extracted when the call is forwarded to the prime switch. It is then passed to the CallPilot Server. This allows CallPilot to distinguish the address of the original called party.

For a redirected network call, NMS uses the Network Call Redirection (NCRD) feature to provide the original called number. The following Network Call Redirection types are supported:

- network call forward all calls (NCFAC)
- network call forward no answer (NCFNA)
- network call forward busy (NCFB)
- network hunting (NHUNT)

Indirect access requires the same NMS transaction signaling message.

Offnet access

A user can directly dial in to the prime switch, or a user can dial in to the user's own switch to access a remote switch. For this type of offnet access, the user's switch may need to support direct inward system access (DISA). This allows the user to dial another network location after dialing in to the user's own switch.

NMS considerations

All CallPilot features are available to users in an NMS network. The prime switch must be a Meridian 1 (Release 23C) switch. Satellite switches must be either Meridian 1 switches or other compliant switches. A CallPilot Server can support one prime switch and a maximum of 59 satellite switches.

Message center directory number

Only one message center directory number can be defined on each user telephone.

Local messaging server broadcast

NMS interprets a local messaging server message broadcast to include users on all switch locations in the NMS network. This feature is especially useful if, for example, you want to inform users of a server shutdown. To avoid excessive resource usage, non-delivery notifications are not generated for broadcast messages.

Feature interaction

Many switch features interact with NMS. The following features interact with ISDN Network Call Redirection (NCRD):

- Call Forward (Unconditional, No Answer, and Busy)
- Network Call Transfer
- Network Hunting
- Call Forward by Call Type Allowed to a Network DN
- Attendant Extended Call
- Call from CO Loop Start
- Conference Call
- Barge-in Attendant

Call Forward (Unconditional Call Forward, Call Forward No Answer, Call Forward Busy)

All three types of Call Forward are supported by the ISDN Network Call Redirection features. These are the basis for NMS indirect access. In the case of an indirect NMS access call, the original called number and the redirecting reason are extracted from the original called number information element in the PRA SETUP message. The original called number and the redirected reason are put into the AML PCI message when presenting a call to the CallPilot Server. If the original called number information element is not present, the redirecting information element is used instead. Similarly, the redirecting number and reason are extracted and transported to the server through a PCI message.

Network Call Transfer

Network Call Transfer is supported by the ISDN Network Call Redirection feature. If an NMS location is involved in a Network Call Transfer scenario, the connected party number is extracted from the PRA NOTIFY message and put into the AML DNP message when the transfer is complete. The DN update message informs CallPilot that a call transfer has occurred.

Network Hunting

Network Hunting is supported by the ISDN Network Call Redirection feature. Indirect NMS access can be presented to CallPilot through Network Hunting. The messaging is the same as for Call Forward Busy. Therefore, the original called number information element in the PRA SETUP message is used to construct the ISDN/AP PCI message.

Call Forward by Call Type Allowed to a Network DN

The definition of the Call Forward by Call Type Allowed class of service is changed by the ISDN Network Call Redirection feature. This means that private network calls are treated as internal calls and are forwarded, using the Call Forward No Answer feature or the Network Hunting feature, to the Flexible Directory Number or Hunt DN rather than to the External Flexible Number or External Hunt DN. The Call Forward feature is implemented through the ISDN Network Call Redirection feature. With this feature, the switch is able to provide different messaging treatments for different types of calls, such as offnet calls instead of on-net calls.

A location can be configured so that all off-net calls are handled by a centralized attendant, while internal calls are handled by CallPilot. However, there is a limit of one message center DN for each location. This means that a user can be served by two message centers, one that handles internal calls and one that handles external calls, but only one can control the Message Waiting Indicator (MWI) activation.

Attendant Extended Call

Attendant Extended Call has an impact that is similar to Network Call Transfer. There is one important difference, however. The DN update message is sent to CallPilot when the attendant releases the call. Therefore, the connected party number is updated only when the attendant is released.

Call from CO Loop Start

Calls that come in to the switch from the CO Loop Start trunk cannot be redirected to another trunk through attendant extension or call redirection. These calls should be blocked when redirection is activated.

The ISDN Network Call Redirection feature does not redirect calls from CO Loop Start. Therefore, NMS does not support these calls.

Conference Call

When another party has a conference call with a CallPilot system, a DN update message is sent indicating a conference call type. The connected party DN is the same as the station initiating the conference call, which is always the same as the DN in the PCI message. If additional parties are added to the conference, no additional DNP messages must be sent. When a conference call drops back to a simple call, a DNP message is sent indicating a simple call as call type and showing the remaining party as the connected DN. When the conference is established and is dropped at a satellite switch, a FACILITY message with TCAP protocol is transported to notify the prime switch of the conference call activities. The DNP message is then triggered and sent to the CallPilot Server.

Barge-in Attendant

The attendant can barge in on an NMS call on the prime switch location. During barge-in, users cannot use the features that require switch effort, such as Call Sender.

Dialing plans and NMS

The dialing plan that connects the switch locations in a NMS network can affect the way your NMS network is implemented. As well, if the dialing plan is set up incorrectly, NMS cannot work. The dialing plan can also affect the configuration of the switch locations. NMS supports the following dialing plans:

- Electronic Switched Network (ESN)
- Coordinated Dialing Plan (CDP)

- hybrid, which is a combination of ESN and CDP

Note: NMS does not support another dialing plan, such as PSTN.

Dialing plans and NMS user locations

The dialing plan used can affect the flexibility of configuring the user locations in an NMS network.A user location is a logical grouping of mailboxes. A user location may be the mailboxes on one switch or the mailboxes on two or more switches.

ESN dialing plan

If the ESN dialing plan is used, there must be a one-to-one correspondence of switch locations to user locations.

CDP dialing plan

If the CDP dialing plan is used, there are two ways to define the correspondence of switch locations to user locations:

- a one-to-one correspondence
- an all-to-one correspondence

Define one switch location as one user location

Typically, each switch location is represented by a user location. If this is done, ensure that there are no conflicts. For example, the same extension cannot exist on two different switch locations. Configuration of satellite switch locations, and the configuration of phantom DNs for services at all locations are simplified. However, defining one user location means that the spoken name for each individual location is lost.

Define two or more switch locations as one user location

By defining two or more switch locations as one user location, you do not have to check for conflicts. This option also allows you to maximize the number of users supported. You can combine all switch locations into one user location, or you can combine some switch locations into one user location.

How two or more switch locations are combined into one user location

When implementing NMS, if each switch location is a user location, on CallPilot you add and configure each satellite switch. However, each switch is configured individually. To combine two or more switch locations into a single user location, you add and configure only one satellite switch location. The CDP steering codes for the switch locations are added to a single list. Note, however, that a switch location can have a maximum of 500 CDP steering codes. If, by defining a single user location, you require more than 500 CDP steering codes, you cannot use this option. If a CDP dialing plan is used, the CDP code must overlap the mailbox number sufficiently.

Hybrid dialing plan requirements

If a hybrid dialing plan is implemented in the NMS network, the following requirements must be met:

- All switches must support ESN and have ESN prefixes.
- The prime switch must support both ESN and CDP.
- CDP can exist on any satellite switches.
- The general restrictions that apply to CDP also apply to CDP when used in a hybrid dialing plan.

If all CDP switches share the same ESN prefix, configure the prime switch to represent all of the switches that are part of CDP. If each CDP switch has its own ESN prefix, or prefixes, create a location for each ESN switch in the network. That is, group the switches by ESN prefixes.

Implementing NMS

This guide assumes that the following preliminary requirements are met:

- The prime switch is installed and configured.
- The satellite switches are installed and configured.
- CallPilot is installed and configured, except for NMS.
- Sufficient trunks connecting the prime switch to a public switch are available.
- If the implementation is an upgrade from Meridian Mail, all legacy information is available.

The main steps in the implementation process are

1. Configure the local CallPilot server.
2. Configure the prime switch locationCallPilot.
3. Configure the satellite the switch locations.

NMS configuration consists of adding information about the CallPilot Server, the prime switch location, and all satellite switch locations to the database. NMS provides the same CallPilot services to users on satellite switches that are available to users on the prime switch. NMS provides these services transparently. That is, users receive the same services without having to enter any additional numbers, regardless of which switch they are on. To provide these services, the switches and the server in the NMS network must be carefully configured.

Configuring the local CallPilot server

When you configure the local CallPilot server for NMS, you add inbound SDN information to the SND Table for all services provided by all switch locations.

SDN Table

Although the Service Directory Number (SDN) Table on the CallPilot Server is already set up and configured, you must make additions to the table for NMS after configuring the phantom DNs and ACD queues on the satellite switch locations.

To enter a satellite switch SDN, you must know the phantom DNs and ACD-DNs that are set on the satellite switch, and the location codes of the switch in the dialing plan. Usually (for example, if an ESN dialing plan is used) the phantom DNs on the satellite switches are numbered the same as those on the prime switch.

The SDN Table on the CallPilot server contains the SDNs that correspond to the phantom DNs, CDNs, and dummy ACD queues of both the satellite switch locations and the prime switch location.

Services not in the SDN Table

All directly dialed services, such as Express Messaging, must have a corresponding entry in the SDN Table. However, Call Answering services do not have an entry and are treated as a special case. These services do not have an entry because the number dialed (for example, a user's telephone number) is not in the SDN Table. Since the dialed number is not found, the CDN used to route the call to CallPilot is used to determine the appropriate type of call answering service to start.

The CDNs are the prime switch CDNs, even for call answering calls from satellite locations. Typically, two CDNs are used. One CDN is for call answering with the Multimedia Messaging service configured against it, with the media type set to Voice. The second CDN is for voice and fax call answering with the Multimedia Messaging service configured against it, with the media type set to Fax. A result of this configuration is that even if fax call answering is used only on satellites, a corresponding CDN queue and SDN entry for Multimedia (fax media) must be configured.

Note: For detailed information on SDNs and SDN Tables, consult the relevant sections in this guide and in the CallPilot Manage online Help.

Configuring the prime switch location

The prime switch provides the call handling services required by NMS. All requests for services from the satellite switch locations are forwarded to the prime switch location.

Determine the CDNs and the phantom DNs on the prime switch

When you configure the prime switch location for NMS, you complete the required information on the Messaging Network Configuration—Prime Location Properties page. Configuration consists of providing general information about the switch location, such as name and server type, as well as detailed information about the dialing plan used.

Phantom DNs

While some services are accessed by directly dialing a CDN, many services are accessed by dialing a phantom DN. A phantom DN forwards incoming calls to a controlled directory number (CDN) for further call handling. A phantom DN is created for each service offered by the switch. This ensures that each CallPilot service has a unique number that users dial. For example, a user dials 8000 to access Express Messaging and 7040 to access Fax Item Maintenance. Phantom DNs must exist for both services.

Configuring the satellite switch locations

When you configure a satellite switch location, you complete the required information on the Messaging Network Configuration—Server Properties page. Configuration consists of providing general information about the switch location, such as name and server type, as well as detailed information about the dialing plan used.

You must configure the phantom DNs and ACD queues on the satellite switch locations. After adding a phantom DN for a satellite switch, you must add an entry to the SDN Table on the CallPilot server.

The administrators of the satellite switches must know the phantom DNs used on the prime switch. Ensure that every administrator has a complete and accurate list of the phantom DNs and the services they provide.

Upgrading an existing satellite switch

The configuration of satellite switches for NMS in CallPilot is different from the configuration for Meridian Mail. Meridian Mail uses dummy ACD-DNs, rather than phantom DNs, to forward a call to another ACD-DN on a satellite switch. These ACD-DNs forward to ACD-DNs for Meridian Mail on the prime switch. If you are upgrading an existing system, you must decide how you will configure the satellite switches. You can either reuse the existing legacy configuration or reconfigure the system.

To continue to use the dummy ACD-DNs instead of phantom DNs with CallPilot, make sure that the ACD-DN that is forwarded to is, in turn, configured to night call forward to the CDN on the prime switch, specified in network format.

You can also upgrade the existing dummy ACD-DNs and replace them with phantom DNs. Remove the unused dummy ACD-DNs.

Satellite switch location SDNs

The dialing plan prefix distinguishes the SDNs for satellite switch locations from the SDNs for the prime switch location. If an ESN dialing plan is used, the satellite switch location SDN entries do not include the ESN access code. Only the location code is required. For example, if the ESN access code is 6, the location code is 339, and the DN is 8000, enter 3398000 for the service in the SDN Table.

Satellite switch location phantom DNs

The phantom DNs of the satellite switch location are separately defined on the satellite switch. This allows users on the satellite switch to dial a local number rather than using the prime switch phantom DNs with a prefix. For example, a user enters 63388000 for Express Messaging.

Although the satellite switch locations are installed and set up before you implement NMS, some additional configuration is required, since Satellite switches must forward to the prime switch.

Phantom directory numbers (DNs) have been set up on the prime switch. These phantom DNs are used by the switch to route calls to services. Phantom DNs forward incoming calls to the appropriate CDN queues on the prime switch for further call handling. By creating a phantom DN for CallPilot services, every service has a unique number that users dial. Some services, such as Integrated Voice and Fax, may be configured to use the CDN numbers directly.

To make the services that are available to users on the prime switch available to users on the satellite switches, the phantom DNs on the satellite switches must be configured to forward to the ACD queues on the satellite switch. In turn, the ACD queues on the satellite switch forward to the CDN queues on the prime switch. Ask the switch technician responsible for configuring the prime switch location for this information.

Add phantom DNs for services that you want available at that satellite switch location.

Note: You can add additional phantom DNs to account for additional services that you plan to implement in the future.

For detailed instructions on how to add a phantom DN to a satellite switch location, consult the documentation for the switch. The procedures for entering phantom DNs on the prime switch are the same as the procedures for entering phantom DNs on a satellite switch.

Dummy ACD-DNs on satellite switch locations

Every phantom DN that is added to a satellite switch location must be call forwarded to the dummy ACD-DN on a satellite switch. CDNs exist on the prime switch only. Satellite switch locations have dummy ACD-DNs. A dummy ACD-DN forwards a request for a service by a user on the satellite switch location to a CDN on the prime switch. To provide the service, a dummy ACD-DN forwards the request through a night call forward (NCFW) DN. The NCFW DN determines the CDN to which calls are routed.

Number of dummy ACD-DNs required

The number of dummy ACD-DNs on a satellite switch location must be the same as the number of CDNs on the prime switch. For example, if there are two CDNs on the prime switch, one for voice and one for fax, there must be two dummy ACD-DNs on each satellite switch location, one for voice and one for fax.

Switch overlays

Note: For actual procedures and more information about NMS and switch overlays see the CallPilot Manager online Help.

Satellite switch locations for NMS are configured on the following overlays:

Task	Overlay
Define a dummy ACD-DN.	23
Configure a phantom DN.	10

Responses to overlay prompts

To program an overlay, you respond to a series of prompts. You must respond to these prompts in a certain way. Any prompt that is not mentioned can be programmed in any way. To accept the default value for other prompts, press Enter. You must know the CDNs and phantom DNs that are used on the prime switch location to configure the phantom DNs and dummy ACD-DNs on the satellite switch locations.

Define the dummy ACD-DNs

Define a dummy ACD-DN for each media type used. Usually, for each type of CDN on the prime switch, there is a corresponding dummy ACD-DN on the satellite switch.

If this is on the prime switch	Then this is on a satellite switch
CDN Media type: Voice	Dummy ACD-DN Media type: Voice
CDN Media type: Fax	Dummy ACD-DN Media type: Fax
CDN Media type: Speech recognition	Dummy ACD-DN Media type: Speech recognition

If a satellite switch does not provide any of the services provided by a type of CDN queue, it is not necessary to define a dummy ACD-DN. For example, if a satellite switch does not provide any speech recognition services, a speech recognition dummy ACD-DN is not required.

Setting the dummy ACD-DNs to night call forward

Every dummy ACD-DN must be configured to night call forward to the corresponding CDN on the prime switch location. The forwarding address must be in network format. For example, to night call forward to 63387000,

- ESN access code = 6
- Location code of prime switch = 338
- Voice CDN on prime switch = 7000

By configuring night call forwarding in this way, users on the satellite switch location can access the CallPilot service by entering the local satellite switch ACD queue number, 7000. They do not have to explicitly dial the CDN on the prime switch location.

NMS time zone conversions

If Network Message Service is installed on your CallPilot server, and you have switch locations that are in different time zones from the CallPilot server, you can define for each switch location, the time zone in which the switch is located. This results in time and date stamps on messages and voice prompts to be indicated in the mailbox owner's time zone, instead of in the time zone of the CallPilot server.

Network Message Service description

The Network Message Service (NMS) feature in CallPilot enables your CallPilot system to provide voice messaging services to mailbox owners who reside at different switches. All user mailboxes are located on the CallPilot server. This setup is more cost-effective than installing and running a CallPilot system at each switch location.

Each switch is defined in the CallPilot network database as a switch location that is associated with the CallPilot site. The switch that is directly connected to CallPilot is defined as the prime switch location. All other switches are defined as satellite switch locations.

Network Message Service operation in multiple time zones

Network Message Service supports mailbox owners residing on switches in different time zones. Prior to CallPilot 2.0, time and date stamps on messages and voice prompts were indicated in the CallPilot server's time zone, without the time zone name. This would lead to a situation where, for mailbox owners in time zones to the west of the CallPilot server, time and date stamps could potentially be in the future.

CallPilot time zone conversion

When Network Message Service is used in CallPilot, all time and date stamps can be presented to the mailbox owner in his or her switch location's time zone. This is accomplished by specifying the time zone for each local satellite switch location in the network database. The time zone setting can be set to one of the following:

- CallPilot server's time zone
- switch location's time zone (that is, the satellite switch location's time zone is different from the CallPilot server's time zone)

Note: The local prime location automatically acquires its time zone setting from the CallPilot server. On the CallPilot server, the time zone setting is defined in the Control Panel (which is defined when the Configuration Wizard is run).

How time zone conversion affects mailbox owners and administrators

Phoneset users

Phoneset users benefit the most from the time zone conversion feature. All time and date stamps are converted to the time in the phoneset user's time zone.

Desktop messaging users

There is little impact to desktop messaging users since most desktop messaging clients already convert time and date stamps to the time zone configured on the PC used to access CallPilot messages. The PC must be configured with the correct time zone setting in the Date/Time component of the Windows Control Panel.

Exception: Non-delivery notifications and acknowledgments received by desktop messaging users contain a CallPilot server-generated time and date stamp in the CallPilot server's time zone, with the time zone name.

Web messaging users

For web messaging users, time and date stamps are presented in the time zone configured on the CallPilot server for the switch location at which the users reside.

CallPilot administrators

Many configuration and administration pages in CallPilot Manager contain a time field that applies to the item being configured or viewed. When Network Message Service is installed, these pages also contain a read-only time zone name field.

In some situations, an administrator can define whether the time should be presented to administrators in the server's time zone, or in the mailbox owner's time zone. The options are available only when Network Message Service is installed, and applies to the following:

- User Properties and User Creation:
  - Remote Notification
  - Security
  - Status (for Temporary Absence Greeting expiry)
- Message Network Configuration for the local satellite switch location

How time zone conversion affects networking recipients

VPIM Networking recipients

VPIM Networking recipients are not affected since time zone information is included during transmission of VPIM Networking messages. Time and date stamps on VPIM Networking messages include the time zone name.

AMIS Networking recipients

The AMIS Networking protocol does not support the inclusion of time information in messages during transmission. The sent and received time and date stamps are always set to the time when the message is received, which is, therefore, presented in the mailbox owner's time zone.

Enterprise Networking recipients

How Enterprise Networking recipients are affected depends on whether the sending and receiving CallPilot systems are Release 2.0 or later.

Enterprise Networking cannot send or receive time zone information if the messaging server is running a release prior to CallPilot 2.0. Therefore, the time zone feature affects only the messages that are transmitted between systems that are running CallPilot Release 2.0 or later.

chapter 7

About VPIM Networking

In this chapter

Overview 119
Sending VPIM Networking messages to other sites 121
Receiving VPIM Networking messages 122
TCP/IP 125
TCP/IP protocols 127
Implementation overview 128
VPIM-compliant messaging systems requirements 130
VPIM Version 2 conformance table 131

Overview

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. 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.

VPIM address

A VPIM address is similar in form to an e-mail address. 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

- maximum length of 255 characters

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. A telephone user uses VPIM prefixes and shortcuts.

Sending VPIM Networking messages to other sites

Open sites

An open site is not part of the private messaging network. It can be any VPIM-compliant system. 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 via 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 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 exchange 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 a 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 consists of the PSTN address and the CallPilot FQDN. 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 CallPilot. This FQDN is defined in the local network database and is added to the outbound address automatically.

Receiving VPIM Networking messages

The way your local system receives inbound VPIM Networking messages depends on how your data network is set up. CallPilot continuously monitors TCP port 25 (and port 465 if SSL is configured) 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.

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.

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.

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.

TCP/IP

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

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.

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. 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. For example, 45.211.100.58.

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

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. VPIM Networking uses the following TCP/IP industry-standard application protocols:

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

SMTP/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 has extended features such as 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. 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 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.

Implementation overview

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. There is no one standard procedure for implementing VPIM.

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.
- 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 system network sockets facilities on the CallPilot server.

The CallPilot 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.

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.

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 CallPilot 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.

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.

Windows configuration

Configure Windows for VPIM Networking. Configure

- TCP/IP setup
- server FQDN
- DNS

VPIM-compliant messaging systems requirements

A messaging system must meet certain requirements for VPIM-compliance.

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 limits of disk storage. Mail relays may also impose restrictions on message length.

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.

VPIM Version 2 conformance table

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							

Feature	Area	Must	Should	May	Should not	Must not	Nortel
From	C	X					X
From: addition of text name	C		X				X
To	C	X					X
CC	C		X				X
Date	C	X					X
Sender	C			X			
Return-path	C			X			
Message ID	C	X					X
Reply to	C			X			
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

Feature	Area	Must	Should	May	Should not	Must not	Nortel
Message ID	C	X					X
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
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

Feature	Area	Must	Should	May	Should not	Must not	Nortel
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
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

Feature	Area	Must	Should	May	Should not	Must not	Nortel
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
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
Reply messages: always send error on non-delivery	C	X					X

Feature	Area	Must	Should	May	Should not	Must not	Nortel
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				
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							

Feature	Area	Must	Should	May	Should not	Must not	Nortel
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				

chapter 8

CallPilot networking implementation concepts

This chapter provides an overview of the concepts required to implement CallPilot networking solutions.

In this chapter

About implementing networking 140

Key concepts 147

CallPilot Manager networking configuration pages 149

Coordination among sites 157

About implementing networking

In this section

Overview 140
Designing the messaging network 142
Installation and implementation concepts 145

Overview

This chapter provides an overview of the concepts required to implement CallPilot networking solutions. More detailed information is located in Chapter 10, Implementing & configuring CallPilot networking of this guide, which deals with the specifics of implementing and configuring the networking solutions.

The CallPilot networking solutions allow you to create a multimedia messaging network of up to 500 sites so that mailbox owners at one site can exchange messages with mailbox owners at other sites. Voice, fax, and text messages can be sent and received through the telephone or desktop PC.

Messages are transmitted from the local site to a remote site using one of the following protocols:

- AMIS Networking
- Enterprise Networking
- VPIM Networking

CallPilot can also exchange messages with users at sites that are not defined in your messaging network. Sites that are not defined in your messaging network are referred to as *open sites*. You can exchange messages with open sites using one of the following protocols:

- AMIS Networking (also referred to as Open AMIS Networking)
- VPIM Networking (also referred to as Open VPIM Networking)

In addition to these networking protocols, you can use Network Message Service (NMS). NMS allows two or more switches that are connected by ISDN to share the same messaging system. The users at each switch location have complete CallPilot functionality, and are all maintained on one CallPilot server. The collection of switch locations, connections, and the messaging server is known as an NMS network.

AMIS Networking

AMIS Networking uses the Audio Messaging Interchange Specification-Analog (AMIS-A) protocol, an industry standard for the transmission of voice messages between messaging systems. You can use AMIS Networking to exchange voice messages with any remote sites that support the AMIS protocol. These remote sites can be within a private switch network (integrated sites), or within the public switch network (open AMIS sites).

Note: Remote sites that are configured to use the AMIS protocol in your network database are referred to as Integrated AMIS Networking sites.

Enterprise Networking

Enterprise Networking is a networking solution that transmits voice messages between mailbox owners at different sites in a private messaging network. Enterprise Networking uses a proprietary analog protocol that is based on extensions to the AMIS protocol.

If the Names Across the Network feature is enabled, Enterprise Networking also:

- allows the local mailbox owner to hear a remote user's spoken name while composing and sending messages
- supports the display of text names on the phoneset
- supports name dialing for remote addresses

VPIM Networking

VPIM Networking allows mailbox owners to exchange voice, fax, and text messages with other mailbox owners over a TCP/IP data network. You can use VPIM Networking to exchange messages with any remote site that supports the VPIM protocol. These remote sites can be part of your private network (integrated sites), or they can be in a public network (open VPIM sites). 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.

About implementation

Implementation of CallPilot networking requires planning and coordination between the network administrators of the various sites. The time you spend planning the network saves you time during implementation. It also reduces the time it takes to troubleshoot network problems after implementation.

To properly plan for implementation, you must understand the process and all the information that you are expected to provide. You must also look at the implementation on paper. Analyze it to determine if there are any conflicts or missing information.

Implementation scenarios

There are several possible scenarios for implementing your CallPilot system:

- Your site is part of a new messaging network of CallPilot systems.

  If you are designing a completely new messaging network in which each site uses CallPilot, you can design a simple and elegant messaging network.

  Preliminary planning must be done before you can install any networking solution. This planning results in a messaging network that is perfectly designed for CallPilot networking.
- Your site is being added to an existing, compatible messaging network.
- Your site is part of an existing messaging network that is being converted to CallPilot.

  If your site is part of an existing network that is being converted to CallPilot, the implementation process is somewhat different. For example, a dialing plan already exists. CallPilot networking is easiest to implement and maintain when the messaging network uses a uniform dialing plan. However, you will probably be unable to change the entire dialing plan to suit your preferences. Therefore, you may have to implement the networking solution or solutions using a dialing plan that is more complicated to implement and maintain. For more information about implementing a uniform dialing plan, refer to your switch documentation.

If your site is being converted to CallPilot from Meridian Mail, you can migrate most of the existing information from Meridian Mail into the CallPilot network database. The Meridian Mail to CallPilot Migration Utility automates the movement of data. For more information, refer to the *Meridian Mail to CallPilot Migration Utility Guide* (NTP 555-7101-801).

- Your site is part of an existing messaging network and is being converted to CallPilot, while other sites are not being converted.

The process that you follow is determined somewhat by your particular situation. To simplify the process, follow the guidelines described in this guide, as well as in the online Help.

Network administrators

A network administrator is responsible for the messaging network at one or more sites. You can designate

- one network administrator for all sites
- one network administrator for each site
- several network administrators, with each administrator being responsible for a small number of sites in the network

Your first step in planning is to determine who is responsible for implementing and administering a particular site. Nortel Networks recommends that one network administrator be responsible for coordinating the implementation and administration of the entire messaging network. Communication among site administrators is required to maintain the messaging network. A coordinator can simplify this process.

Designing the messaging network

When you receive your CallPilot server, the basic design of your messaging network is already complete. The planning engineers who determined how CallPilot could be used in your messaging network also decided

- how many sites the messaging network will contain
- which networking protocols will be used

Basic design tasks for network administrators

You must complete the basic design of the messaging network. This includes the following tasks:

- Assign unique, useful names to every site in the messaging network.
- Identify the Network Message Service (NMS) sites in the messaging network.
- Determine the dialing plan that is used among sites.
- Determine the networking solution that will be used between a pair of sites.

Network database

Each site in the messaging network has its own network database that contains all information entered during the implementation and configuration of networking at that site. You must understand the network database structure because it is integral to understanding how to implement a networking solution.

The network database contains three main types of information:

- information about each of the networking solutions installed at the site

- information about the local site
- information about every remote site in the messaging network with which the local site communicates

The local site and each remote site that is configured in the network database consist of:

- a messaging server—the computer on which CallPilot (or for remote sites, some other messaging system) resides
- a prime switch location—the switch that is directly attached to the messaging server

When the site uses NMS, the site configuration consists of

- a messaging server
- a prime switch location
- one or more satellite switch locations

If a remote site is configured in the network database, it is considered to be an *integrated site*. If a remote site is not configured in the network database, it is considered to be an *open site*. For more details, see Networking requirements and considerations on page 158.

The information you enter into your network database for each remote site must be provided by the remote site's network administrator. Most of the information that you enter for a remote site is the same information that is entered for the remote site in its network database. Network databases must be identical across the messaging network. Otherwise, networking will not work correctly.

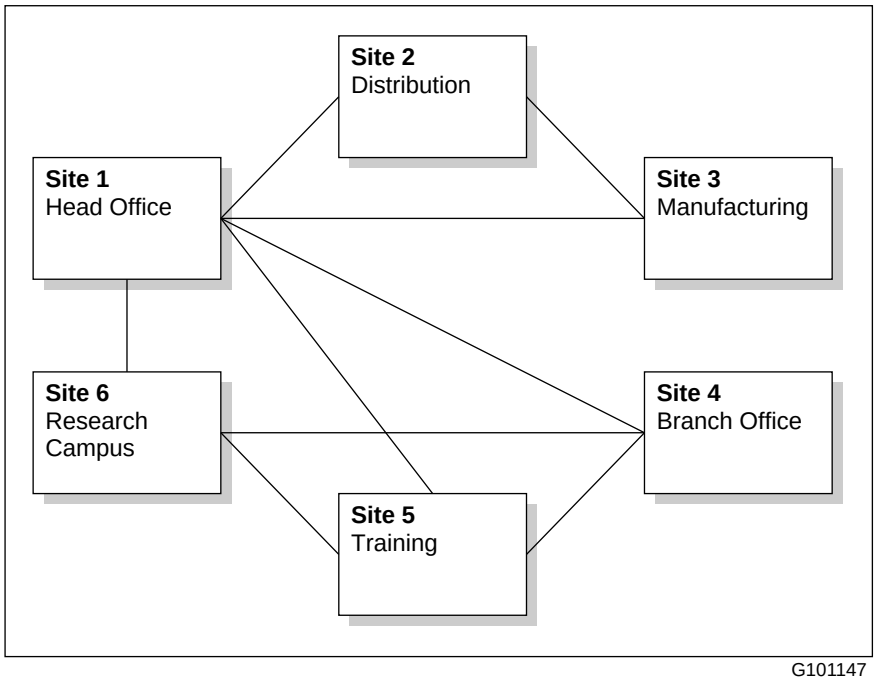
When to add remote sites to the network database

The local network database contains information about the remote sites with which the local site exchanges messages. These sites appear in the messaging network tree in CallPilot Manager.

If the messaging network is a true mesh network, your network database contains information about each site in the network. Each site can exchange messages with all sites in the network.

For larger messaging networks, a mesh network may be impractical or unnecessary. In fact, in most messaging networks, a site connects only to those remote sites with which it commonly exchanges messages. In this case, the database does not contain the sites with which the local site does not exchange messages.

The following diagram illustrates a non-mesh network. In this example, only Head Office (site 1) connects to all sites. The other sites connect only to those sites with which messages are exchanged. The Manufacturing site, for example, connects only with the Distribution and Head Office sites.



The mesh or non-mesh network concepts are important because some values must be unique both in the network database and throughout the messaging network. When you configure CallPilot, CallPilot Manager can identify information that is not unique in the local network database. You must manually ensure that information is unique across the messaging network.

For more information about how CallPilot Manager validates information that you enter, see the following sections:

- Validation on page 154
- Ensuring information is unique on page 155

Open and integrated sites

A messaging network is made up of integrated sites. A site is considered integrated when it is included in the network databases of the other sites in the messaging network.

However, a site can exchange messages with sites that are not part of the messaging network. These other sites are known as open sites. A typical open site can be a major customer or supplier to your company.

Protocols used to communicate with open sites

The ability to exchange messages with open sites is achieved by using industry-standard protocols, such as AMIS or VPIM. As long as the messaging system at an open site complies with either protocol, sites in the messaging network can communicate with the open site.

Implicit open sites

In addition to open and integrated sites, VPIM Networking uses the concept of implicit open sites.

You can use VPIM Networking in an integrated messaging network. Shortcuts for the VPIM Networking addresses of the remote sites with which you want to communicate are listed in your network database. These shortcuts enable users to address their messages using the telephone, because the shortcuts map to the address of the remote site. For more information about VPIM network shortcuts, refer to the online Help in CallPilot Manager.

Installation and implementation concepts

In CallPilot, a distinction is made between a networking solution that is installed and one that is implemented. This concepts detailed in this guide, used in conjunction with the procedures in the online Help, describe the implementation process for each of the networking solutions.

This guide provides:

- a general description of the implementation process and introduces some of the key concepts necessary to understand the process
- implementation checklists and configuration worksheets to help you plan and implement networking on your CallPilot server

The online Help provides the actual procedures for implementing the various networking solutions.

Differences between installation and implementation

The difference between networking installation and implementation is important.

Installation

When you purchase the networking keycode, all networking solutions except NMS are installed and enabled on your CallPilot server.

Implementation

To be available on your server, the networking solution must be implemented. Implementation means that the networking solution is properly configured and the network database is set up.

Network implementation prerequisites

Implementation of a networking solution is an incremental activity. Before you begin to implement a networking solution, you must ensure that the following tasks are already completed:

- The CallPilot server is set up and configured for local use.

  If it is not, refer to the following documents for instructions:
  - *CallPilot Installation and Configuration* guide for your server
  - CallPilot Administrator's Guide (555-7101-301)
- The switch is set up and configured for local use.

  Note: Switch security features should be configured with networking in mind.
- The appropriate number of switch trunks are available.
- The appropriate number of CallPilot channels are available.

Recommended order of implementation

Information that you provide when implementing one networking solution is also required when you implement the next networking solution.

For example, suppose you have Integrated AMIS Networking and Enterprise Networking installed on your system. Several configuration boxes that you must complete during the implementation of Integrated AMIS Networking are enabled because Enterprise Networking is also installed. In some instances, you must enter temporary information (which is called a placeholder), into those boxes before you can save the information in the network database.

The implementation process is easier if you follow this recommended order:

1. Network Message Service (NMS)
2. Desktop or web messaging
   For more information, refer to the *Desktop Messaging and My CallPilot Installation Guide* (555-7101-505). For information about IMAP implementation, refer to the *Desktop Messaging and My CallPilot Administration Guide* (555-7101-503).
3. AMIS Networking, Integrated AMIS Networking, Enterprise Networking or VPIM Networking

Network Message Service implementation

Nortel Networks recommends that you implement and test all NMS sites in the messaging network before you implement any other networking solution.

Nortel Networks also recommends that you verify the accuracy of information for your site before you release it to remote network administrators.

AMIS Networking

If your site uses the AMIS protocol to exchange messages with open sites only, implement AMIS Networking. Follow the procedures in the online Help.

Integrated AMIS Networking

If your local site uses the AMIS protocol to exchange messages with only integrated sites, or with both integrated and open sites, implement Integrated AMIS Networking. Follow the procedures in the online Help.

Implementation checklists

To help you track your progress while implementing one or more networking solutions, you can use the implementation checklists that are provided in Appendix A, “Implementation and planning tools,”:

- AMIS Networking Implementation Checklist: NWP-035 on page 239
- Integrated AMIS Networking Implementation Checklist: NWP-032 on page 241
- Enterprise Networking Implementation Checklist: NWP-031 on page 243
- VPIM Networking Implementation Checklist: NWP-029 on page 245
- Open VPIM Implementation Checklist: NWP-036 on page 247

Key concepts

In this section

Network views 147
Performing local and remote administration 147
Multi-administrator environments 148

Network views

Your view of your messaging network depends on which site you are on. From your perspective, only one site is local. All other sites are remote. However, the administrator of another site sees that site as local and all others as remote.

In most cases, the site where you are physically located is the local site. However, if the necessary permissions are set up on the system, you can administer a remote site. Even though the site is physically remote, from your perspective, it is the local site. For example, while dialing in to Site 2 and performing network administration from another site, Site 2 is considered the local site and all other sites are remote.

Performing local and remote administration

You can implement and administer a CallPilot networking site either locally or remotely.

In most networks, each site has a local on-site messaging network administrator who is responsible for the system. However, CallPilot's remote administration capability allows you to implement and administer sites remotely. If you are implementing and administering sites remotely, follow the procedures in the online Help for each site.

It is important to note, however, that whenever you are administering a site remotely, you are acting as the local administrator of that site.

Site security

CallPilot protects site configuration from unauthorized users. To implement and administer sites remotely, you must have the proper authorization and password for each site.

Logging on to a local or remote server

CallPilot Manager is a web-enabled administration tool that is used to configure and maintain your CallPilot server from any PC that has IP connectivity to your CallPilot server.

You can run CallPilot Manager using one of the following web browsers:

- Internet Explorer (version 5.0 or later)
- Netscape Communicator (version 6.2 or later)

CallPilot Manager provides three pages for implementing and maintaining the CallPilot networking solutions:

- Message Delivery Configuration
- Message Network Configuration
- Message Delivery Status

Message Delivery Configuration

The Message Delivery Configuration page is where message transmissions for each networking protocol are enabled, and settings such as the batch thresholds, delivery schedules, SMTP security, and encryption are defined.

Message Network Configuration

The Message Network Configuration page is where the local site, switch locations, and remote sites are defined.

Message Delivery Status

The Message Delivery Status page provides information that allows you to see the status of message delivery queues, run a diagnostic test to check the protocol connection between sites, and enable or disable a site.

Relationship of the CallPilot Manager web server to the CallPilot server

The CallPilot Manager web server software can be installed on the CallPilot server, or on a stand-alone server. If the CallPilot Manager web server software is installed on a stand-alone server, you must know the CallPilot Manager server's host name or IP address as well as the CallPilot server's host name or IP address.

Logging on

You must use a web browser to log on to and administer the CallPilot server. The process for logging on to a remote CallPilot server is the same as for logging on to the local server. The logon process is detailed in Logging on to the CallPilot server with CallPilot Manager on page 15.

Note: You can use CallPilot Manager to log on to and administer any CallPilot 2.0 or later server in your network. You cannot use CallPilot Manager to administer CallPilot servers that are running CallPilot 1.07 or earlier.

Multi-administrator environments

Multiple administration is a standard database management feature that enables many administrators to work on a database at the same time. For more information on this, refer to Multi-administrator access on page 17.

CallPilot Manager networking configuration pages

In this section

Message Delivery Configuration description 149
Message Network Configuration description 151
Working with the Message Network Configuration page 153
Validation 154
Ensuring information is unique 155
Specifying time periods 156

Message Delivery Configuration description

The Message Delivery Configuration page contains message delivery options information for each of the networking solutions. It is accessible in CallPilot Manager as follows:

- for all networking solutions if you purchased the networking feature
- for Enterprise Networking only, if you did not purchase the networking featureNetworking solutions

You must complete the Message Delivery Configuration page to implement the following networking solutions:

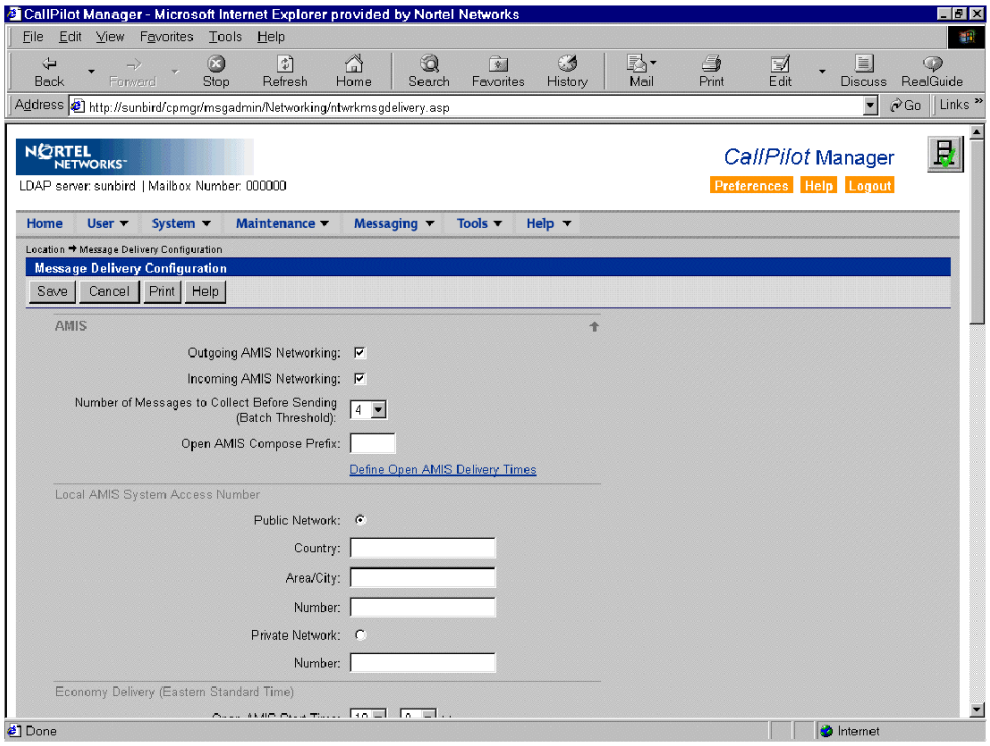
- AMIS /Integrated AMIS Networking
- Enterprise Networking
- VPIM Networking

You do not use the Message Delivery Configuration page to implement NMS.

To open the Message Delivery Configuration page

In CallPilot Manager, click Messaging › Message Delivery Configuration.

Result: The Message Delivery Configuration page appears:



Note: If you want to print the Message Delivery Configuration parameters, follow the procedure detailed in the CallPilot Manager online Help.

To navigate to subsequent pages

Some Message Delivery Configuration options are accessible on separate pages. To access the subsequent pages, click the underlined text on the main Message Delivery Configuration page, or the action button in the area you are configuring. When you click an underlined link or the action button, a new page appears.

To cancel changes on a CallPilot Manager page

Each page has a Cancel button. You must understand how Cancel works to ensure that you do not inadvertently lose configuration information that you have entered.

When you enter configuration information on a page, the information is only saved to the network database when you click Save.

This means that when you click Cancel, the following occurs:

- All of the changes that you enter on the page are deleted.
- You are returned to the previous page.

Click Cancel only if you want to undo all of your changes on the page.

Note: To delete specific information from a field, use the standard Windows methods, such as the Backspace or Delete keys.

To save configuration changes

You do not have to complete the configuration of your entire messaging network at one time. You must save any changes that you do make in a session. If you do not save your changes, the network database is not updated when you go to another CallPilot Manager page.

To save your changes, click Save on the page on which you are working.

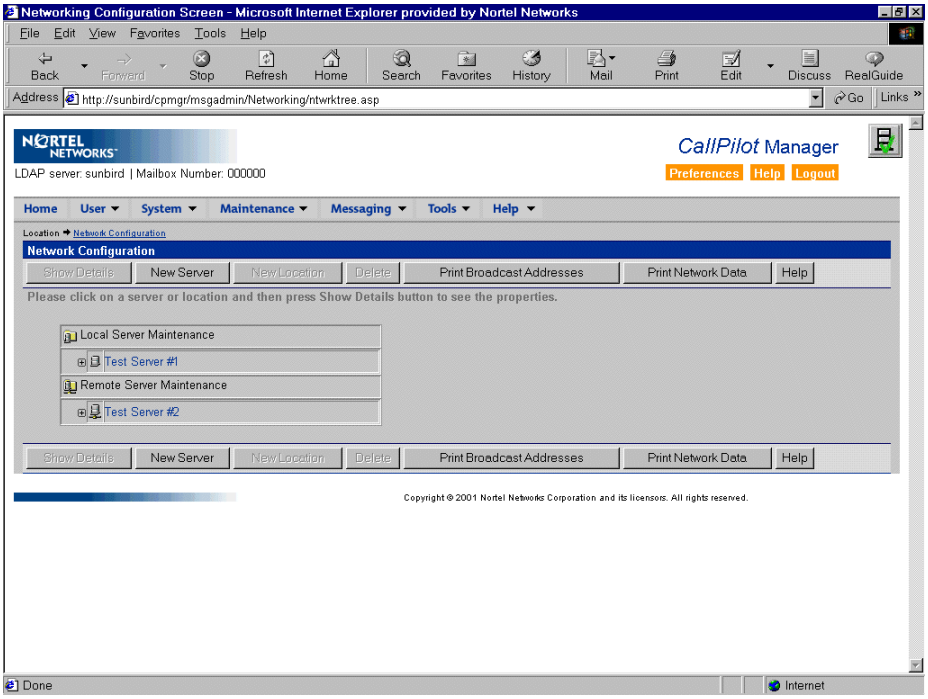
Message Network Configuration description

The Message Network Configuration page contains a graphical representation of your messaging network. It uses a tree to show the local site and all remote sites in the messaging network. Use the tree to add, remove, and modify the configuration of messaging servers and switch locations in your messaging network.

To open the Message Network Configuration page

In CallPilot Manager, click Messaging › Message Network Configuration.

The Message Network Configuration page appears, showing the network tree.



How sites and switch locations are represented

A site consists of a messaging server and a prime switch location. If the site is using NMS, the site also includes one or more satellite switch locations. In the tree view, a site is represented by the messaging server icon. To see the switch locations associated with a site, click the plus sign (+) next to the messaging server.

Note: To reduce the amount of time required to display the network tree, you can expand the tree for only one site at a time. This means that if the switch locations for a particular site are visible when you click another messaging server, the page refreshes to show only the switch locations for the messaging server that you chose.

Local messaging server and prime switch location

The local messaging server and local prime switch location are automatically added to the Message Network Configuration tree when CallPilot is installed on your system. They cannot be deleted.

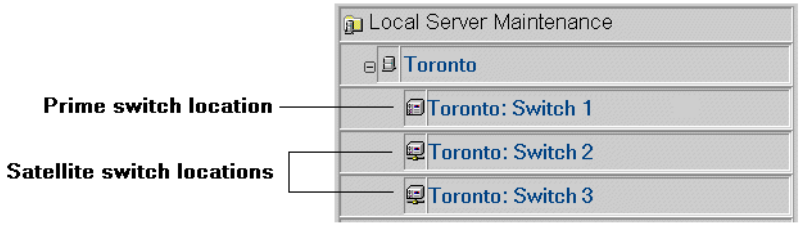
Remote messaging servers and prime switch locations

Each messaging server is associated with a prime switch location. For this reason, when you add a remote messaging server to your messaging network, a prime switch location is automatically created for that remote messaging server. By default, the prime switch location is given the same name as the messaging server. The prime switch location for a remote messaging server cannot be deleted.

Satellite switch locations

The messaging network tree shows which sites in the network are NMS sites. NMS sites have one or more satellite switch locations in addition to the prime switch location.

You can distinguish a prime switch location from a satellite switch location by its icon as follows:



Note the difference between the prime switch and satellite switch icons.

Network tree and maximum number of sites

The Message Network Configuration tree can contain up to 500 sites. An NMS site can have up to 59 satellite switch locations. Therefore, if CallPilot is used to its full capacity, your Message Network Configuration tree can contain 30,000 items. It is very important to be organized when implementing large messaging networks.

If the size of the network tree exceeds the size of the browser window, a scroll bar appears on the right side of the browser window.

Network tree organization

When you are implementing and maintaining large networks, it can be difficult to keep track of sites, messaging servers, and switch locations. For this reason, CallPilot automates some of the organization for you.

Local site

The local site is always shown at the top of the network tree, under the Local Server Maintenance branch.

If the local site is an NMS site, the prime switch location is always listed directly below the messaging server. The satellite switch locations are listed in alphabetical order below the prime switch location.

Remote sites

Remote sites are shown below the Remote Server Maintenance branch. Remote sites are listed in alphabetical order.

The satellite locations, including the prime switch location, are all listed in alphabetical order. Note that the prime location’s icon differs from the remote location icons.

Working with the Message Network Configuration page

Each messaging server and switch location in the Message Network Configuration tree has a page that contains the configuration settings for that messaging server or switch location.

To open a messaging server or switch location page

You can open the page for any messaging server or switch location in the messaging network from the Message Network Configuration tree.

1 In CallPilot Manager, click Messaging › Message Network Configuration.

2 Do one of the following tasks:

To	Click
add a new remote server	New Server. **Result:** A blank page for the new messaging server appears.
add a new switch location	the name of the messaging server in which you are interested, and then click New Location. **Result:** A blank page for the switch location appears.
modify the configuration for an existing server or switch location	the name of the messaging server or switch location in which you are interested, and then click Show Details. **Result:** The page for the messaging server or switch location appears.

3 Configure the settings on the page as required.

For instructions, refer to the CallPilot Manager online Help.

4 Click Save.

To navigate to subsequent pages

Some Message Network Configuration options are accessible on separate pages. To access these pages, click the underlined text on the main Message Network Configuration page, or the action button in the area you are configuring. When you click an underlined link or the action button, a new page appears.

To cancel changes on a CallPilot Manager page

Each page has a Cancel button. You must understand how Cancel works to ensure that you do not inadvertently lose configuration information that you have entered. When you enter configuration information on a page, the information is only saved to the network database when you click Save. This means that when you click Cancel, the following occurs:

- All of the changes that you enter on the page are deleted.
- You are returned to the previous page.

Click Cancel only if you want to undo all of your changes on the page.

Note: To delete specific information from a field, use the standard Windows methods, such as the Backspace or Delete keys.

To save configuration changes

You do not have to complete the configuration of your entire messaging network at one time. You must save changes that you do make in a session. If you do not save your changes, the network database is not updated when you go to another CallPilot Manager page.

To save your changes, click Save on the page on which you are working.

Validation

Validation is the process of checking the information entered during configuration before saving it to the database. Validation identifies any problems with the information that you have entered before it is added to the network database. This minimizes configuration problems and helps to ensure that the information that you have entered works.

Levels of validation

There are two levels of validation:

- field
- record

Field validation ensures that you can enter only valid characters into a box on a page. For example, if a box accepts only numbers, you are not allowed to enter letters. If you are unable to enter characters into a box and do not know why they are being rejected, click the Help button on the page. The online Help appears explaining what the page does, as well as identifying its default values and restrictions, if any.

Record validation ensures that the information you have entered while completing a page is complete and consistent, and does not conflict with any other records in the network database. Record validation occurs when you click Save.

Examples

Many boxes must be unique within the site. If a site uses the Coordinated Dialing Plan (CDP), up to 250 steering codes can be defined. Every steering code must be unique for the site. However, the same steering codes can be used at other sites.

Other boxes must be unique across the messaging network. For example, every messaging server must have a unique name.

For more information, see the following section on ensuring information uniqueness.

Ensuring information is unique

As you configure the messaging network, you must provide information that is unique. When determining if information is unique, you must consider two factors:

- the context in which an item is unique
- the comparison against which an item is unique

Context

There are different contexts in which an item must be unique:

- Some items must be unique for the local site.

  Example: CDP steering codes
- Other items must be unique in the local network database (which contains the local site and all remote sites with which the local site exchanges messages).

  Example: Site ID
- An item may have to be absolutely unique in the context of certain other items.

  Example: Network shortcuts and prefixes (For more details, see Unique numbers on page 155.)

Uniqueness and validation

It is important to keep the uniqueness requirements in mind when implementing a messaging network, because not all boxes are automatically validated for uniqueness.

Whenever a box must be unique against local information or information in the local network database, it is automatically validated. If a box is not unique as required, an error is generated and you must correct the information before it is accepted.

Note: Several boxes (such as the site ID and connection DNs) must be synchronized across the entire messaging network. The information in various network databases cannot be checked automatically. For these types of boxes, the network administrators of all sites must coordinate their efforts and determine if the information entered in each network database is correct. This must be done before implementation begins, ideally as part of the information-gathering phase of the implementation process.

Unique numbers

Most of the information that must be unique is numerical. In a messaging network, unique numbers have a particular definition.

A unique number is one that does not conflict with another number. Conflict occurs when there is an exact or a partial match when compared from left to right. A number is unique when it does not repeat any consecutive digits when read from left to right.

Example

- 6338 conflicts with 6338, 633, 63, and 6.
- If you use 6338 and require a unique number, you must use one that is unique from left to right; for example, 7338 is unique

Specifying time periods

When you implement CallPilot networking solutions, several parameters are expressed as periods of time.

24-hour clock

CallPilot uses a 24-hour clock. Therefore, 3:00 p.m. is expressed as 15:00.

Guidelines

Use the following guidelines to specify time periods:

- The last minute of any hour is expressed as *x*:59 (where *x* represents the hour).
  For example, 8:00–8:00 is actually configured as 8:00–7:59.
- Overlapping time periods are affected accordingly.
  - There is no overlap between 8:00–10:00 (configured as 8:00–9:59) and 10:00–17:00 (configured as 10:00–16:59).
  - There is a 1-minute overlap between 8:00–10:00 (configured as 8:00–9:59) and 9:59–17:00 (configured as 9:59–16:59).

Coordination among sites

In this section

Coordinating network information 157
Networking requirements and considerations 158

Coordinating network information

If a network administrator makes changes to the configuration of one site, often these changes must be communicated to the network administrators of all other sites. The network databases of all other sites must reflect these changes.

Ensuring information is consistent across the network

One of the most important implications of the CallPilot network database system is the interdependence of the databases. Although each site has its own network database, the information in one must be consistent with the information contained in another. If you change one network database, you must ensure that all other network databases are also changed.

Therefore, network administrators must coordinate their efforts before implementing a networking solution or making changes. If changes are made to one network database but not to the other network databases, the messages exchanged with the site that changed its network database may result in non-delivery notifications, depending on what was changed.

Information that must be coordinated

As part of the coordination effort, you must gather information for the whole network and analyze it to ensure that there are no conflicts or oversights. You must also coordinate the following information with the other network administrators before any site in the messaging network can be implemented:

- local messaging server name
- site ID
- protocol used between a pair of sites
- dialing plan used for connecting to each site
- connection information:
  - ESN location codes
  - CDP steering codes
  - connection DNs (Enterprise Networking) or system access numbers (AMIS Networking)
- SMTP/VPIM network shortcuts (VPIM Networking)

Configuration worksheets

You can use the configuration worksheets, which are provided in Appendix A, “Implementation and planning tools.” to record the information that you gather. You can then transfer this information to a messaging network diagram to help you visualize the network. Check the information carefully to ensure that each element is unique.

After all information is configured in CallPilot, you can:

- retain the completed configuration worksheets as a hard copy backup record of your network
- send the completed worksheets to other messaging network administrators to help them configure the network databases at their sites

The following table identifies the configuration worksheets:

Information type	Worksheet name
CDP steering codes	CallPilot Networking—CDP Steering Codes: NWP-027 on page 249
ESN location codes	CallPilot Networking—ESN Location Codes: NWP-037 on page 250
your local site	CallPilot Networking—Local Server Maintenance: NWP-024 on page 251
each remote site	CallPilot Networking—Remote Server Maintenance: NWP-025 on page 252
each switch location	CallPilot Networking—Switch Location Maintenance: NWP-026 on page 254
your local server's message delivery configuration settings	CallPilot Networking—Message Delivery Configuration: NWP-028 on page 256
open VPIM shortcuts	CallPilot Networking—Open VPIM Shortcuts: NWP-038 on page 259

Networking requirements and considerations

When implementing a particular networking solution, consider the items discussed in this section.

Interaction of networking with other CallPilot features

Each CallPilot networking solution supports different features. You must also be aware of how a particular networking solution interacts with other CallPilot features.

Dialing plans

When you begin to implement a networking solution, the dialing plan used by your local site is already configured on the switch. The decision about which dialing plan to use for each site in your network is already determined when you begin to implement a networking solution. Therefore, during implementation, you are simply reflecting the existing plan in your network database.

Even though the dialing plan is already set up, you must understand how to gather the dialing plan information from the switch. You must also understand the implications of the dialing plan for your messaging network.

Refer to Chapter 4, Dialing plans and networking for detailed information on dialing plans.

Channel requirements

To process a call, every analog networking solution requires access to a channel. A channel provides a connection between the switch and the Digital Signal Processor (DSP) cards on the CallPilot server.

CallPilot supports three channel types, each corresponding to different media:

- voice
- fax
- speech recognition

Although a networking solution can work with all three types of channels, voice ports are usually used.

The channel requirements for a networking solution are expressed as a minimum and maximum range.

Coordinate with the system administrator to determine how the channel requirements are set. The system administrator must know about the networking solutions that are implemented and the anticipated traffic before setting up the channels. This ensures that when a networking solution is implemented, the necessary channel resources are available.

If channels are dedicated to networking, the number of channels required for networking must be identified. However, the number required also depends on the traffic requirements of other CallPilot features.

For significant amounts of analog networking traffic and for NMS, additional voice channels may be required.

The table below shows how many networking calls are processed each hour for a specific number of channels. The table is based on the following assumptions:

- Five percent of the recipients of composed messages are at remote sites.
- The message length is 40 seconds.
- The network consists of three sites.

Number of channels	Networking channels	Number of networking calls
72	2	102
96	3	153

NMS and channels

NMS does not require channels to transmit messages. Calls between switches in an NMS network are routed to the CallPilot server over ISDN PRI links.

However, a calculation of the system size must consider all users, even if they are attached to NMS users on satellite switches.

Types of channels required

Networking requires full-service voice channels. Networking does not work on basic-service voice channels.

If full-service multimedia channels are configured, they are used by networking only if all full-service voice channels are busy or out of service

VPIM considerations

When VPIM Networking is installed, the CallPilot server must be attached to the Customer LAN (CLAN). Usually, this connection is already in place. VPIM Networking is transmitted over the TCP/IP network. Therefore, VPIM Networking does not require or use voice channels.

Network security

To maintain the integrity and security of your CallPilot system, each site in your messaging network should follow the recommended security precautions discussed in Chapter 12, Security and encryption.

Consider the following security measures:

- phoneset user, desktop user, and server access restrictions to prevent toll fraud
- switch features, such as the following:
  - Trunk Group Access Restrictions (TGARs)
  - Class of Service (CLS)
  - Network Class of Service (NCOS)
- firewalls and packet filters (if you are using VPIM Networking)
- encryption (if you are using VPIM Networking)

Engineering considerations

You must consider the following engineering issues for each networking solution:

- the impact of VPIM Networking on the local area network (LAN)
- message handling capabilities of the networking solution (throughput)
- message queuing capacities
- message transmission times

Other considerations

Other considerations that you must be aware of are:

- how many sites the messaging network can contain. CallPilot supports a maximum of 500 integrated sites.
- how many delivery sessions can be active at one time
- The maximum number of simultaneous delivery sessions to a single remote site depends on the networking solution.
- the length to which mailbox numbers are limited
- For AMIS Networking, mailboxes cannot exceed 16 digits.
- how messages are handled

All networking solutions deliver all messages in their entirety or not at all. Messages are never delivered in part. A non-delivery notification (NDN) indicates that no part of the message was received.

chapter 9

Gathering information

This chapter describes how to gather the information required to implement message networking. It also provides a checklist for all information that is needed about the switch configuration.

For 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.

In this chapter

Overview 161

Switch information 163

Data network information 162

Information required from switch 164

Evaluating the switch information 166

Information from other sites 166

Overview

Before you can begin to implement networking, gather the information you require. You will speed up the implementation process if you have this information available before you begin. When you analyze the information and look for inconsistencies and incompleteness, you ensure that potential problems are resolved.

Required information

You must gather several types of information:

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

Why gather information?

The gathered information is used to:

- Identify the sites in the messaging network
- Identify the networking protocols used among sites
- Identify how the sites relate to each other
- Identify the dialing plan used by each switch in the network
- Determine if the dialing plan on one or more switches in the network must be modified to support the networking solutions of CallPilot

- Create a messaging network representation (refer to Create a messaging network representation on page 89 for more information)
- Prepare for CallPilot configuration

Information about open sites

If local users exchange messages with open sites, gather the system access numbers of these open sites. You need the system access number of at least one open site that you can use when you test your implementation. Coordinate with the administrator of a remote open site before you begin to test the implementation.

If the implementation is an upgrade

If CallPilot NMS is an upgrade from an existing NMS setup or is being added to an existing site, information must be gathered about the existing site. Whenever possible, the information will be reused so that the implementation of CallPilot NMS will be transparent to users, and they will continue to use the system as they always have.

If the implementation is a new network

If NMS is a new implementation, this information must be created. Information about the administrative setup should be gathered first so that there are no conflicts. For example, prefixes used to dial an exterior number, a long-distance number, or an international call should be gathered.

Much of the required information depends on the dialing plan that will be used. If CallPilot NMS is replacing a current system, usually the existing dialing plan will be re-created. If CallPilot is a new implementation, the choice of dialing plan depends on how the system will be used.

Recommendation

An ESN dialing plan is recommended over a CDP dialing plan. An ESN dialing plan has several advantages, including the following:

- easier to maintain
- easier to add new sites
- minimal conflicts with numbering plans

Data network information

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, you need to know the 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.

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

Switch information

When you begin to implement networking, the switch is already correctly 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 exchange messages among sites.

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

Gathering 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 descriptions of the information in each overlay.

Confirming settings

Usually, when the switch is configured, the switch technician addresses the impact of messaging on the switch. However, to ensure that there will be no problems, you must confirm that the configuration suits the needs of your networking solution and can handle your anticipated volume of traffic. If you discover that changes are necessary, you must complete these changes before you proceed with the implementation of your messaging network.

How dialing plans are used by VPIM Networking

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.

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

You must gather information about the switch. You must verify that the switch supports networking. You use some of the information, such as dialing plan information, to configure CallPilot.

Gather information from:

- the local prime switch location
- the remote switch locations (prime and satellite)

Note: If the local site is an NMS site, you must also gather information from each satellite switch location.

Gather information about used features only

Most of the information that you gather from the switch is related to the dialing plan. Gather information about a dialing plan only if a dialing plan is being used. Do not gather the information if the dialing plan is installed on the switch but is not currently being used.

Example: Your switch has both ESN and CDP installed. However, only ESN is used. Do not gather CDP information.

Local prime switch location information checklist

You need the following information from the switch configuration:

- 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 locations

  - 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
- if another dialing plan, such as PSTN, is used:
  - dialing prefix information
- confirmation that sufficient trunks are available for anticipated networking traffic
- confirmation that restrictions are suitable for the planned messaging network (for example, Trunk Group Access Restrictions [TGAR]) and not too restrictive
- range of extension numbers used at the local site (for example, 7000–7999)
- information about existing CDNs and phantom DNs that are defined on the switch

Remote switch location information checklist

For each remote site in the messaging network, you need the following information about each switch location (prime and satellite):

- name or physical location of switch
- 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 prefix and ESN access code
  - verify the ESN location codes
    - local switch location
    - remote switch locations
  - 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
- if another dialing plan, such as PSTN, is used:
  - dialing prefix information
- 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 location can be dialed in the *same* way
- information about existing phantom DNs and dummy ACD queues defined on the switch

Evaluating the switch information

When you have the dialing plan information from all switches in the messaging network, review the information to ensure that you do not have to make any changes to switch configurations.

Mandatory requirement

The dialing plans of all switches in the network must have a uniform, or standardized, dialing plan. A uniform dialing plan means that users on all switches dial the same way to reach the same recipient. There is only one exception to this rule: ESN access codes can be different. You need a uniform dialing plan to dial users on other switches within the messaging network and at public sites.

A uniform dialing plan offers the following benefits:

- The network is easier to configure and maintain.
- Future growth of the network is allowed.

Configuring dialing plan information

You need extensive switch programming experience to configure dialing plan information on a switch.

ATTENTION!

If you determine that changes to the dialing plan configuration are necessary, ask a switch technician to confirm your conclusion and make the necessary changes.

Information from other sites

Implementation of a networking solution is a coordinated effort. Many decisions must be made before implementation begins. Gather the following information before you begin to implement a messaging network:

- site names
- Enterprise site IDs, if Enterprise Networking is implemented in the messaging network
- passwords—each site must decide on the initiating password and the responding password that is used with every other site (Enterprise Networking)
- fully qualified domain names (FQDNs) of servers
- the protocol used between the local site and all remote sites
- the dialing plan used between the local site and all remote sites
- connection DNs for each site that uses the AMIS protocol to exchange messages with the local site

If any remote sites are NMS sites, also gather the following information for each satellite switch location:

- switch location name, switch type, location ID

chapter 10

Implementing & configuring CallPilot networking

In this chapter

Overview 167

Configuring the switch using phantom DNs 170

Configuring CallPilot 171

SDN Table and message networking 171

Implementing message networking 175

Message Delivery Configuration parameters 176

AMIS message delivery configuration 178

Enterprise message delivery configuration 183

VPIM message delivery configuration 184

Overview

AMIS, Enterprise, and VPIM Networking are the networking solutions offered by CallPilot.

AMIS Networking uses the industry-standard Audio Messaging Interchange Specification (AMIS) analog protocol to exchange messages with AMIS-compliant systems that are configured in the local network database.

> **Note:** There are both analog and digital versions of the AMIS protocol, but CallPilot uses only the analog version. Therefore, AMIS refers to AMIS-Analog throughout this guide.

Enterprise Networking uses a proprietary analog protocol that is based on extensions to the AMIS protocol.

VPIM Networking offers the ability to exchange voice, fax, and text messages with other users over an 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.

The implementation of AMIS, Enterprise, and VPIM Networking requires additional configuration of CallPilot. This configuration determines how your networking solution exchanges messages with other sites in the messaging network.

To implement network messaging you need to:

1. Gather information for the network.
2. Configure the switch for networking. See "Configuring the switch using phantom DNs" on page 170.
3. Configure CallPilot for networking. See "Configuring CallPilot" on page 171
4. Add and configure the remote sites. See Chapter 11, Configuring local and remote networking sites
5. Test the network and back up the system. See the CallPilot Manager online Help.

Note: The CallPilot Manager online Help provides the actual configuration procedures.

As you plan and implement networking, keep detailed records about your site. These records:

- provide a source of information for support personnel
- share information about the site with other network administrators

See also

If you need conceptual information about the general implementation process, consult Chapter 8, CallPilot networking implementation concepts in this guide.

AMIS networking

To be universal, AMIS Networking gives up some advanced messaging functionality. Therefore, AMIS Networking does not support some of the advanced features of CallPilot. CallPilot compensates for some of the shortcomings of the AMIS protocol. For example, the AMIS protocol allows only one recipient for a message. CallPilot enables users to send a message to more than one AMIS recipient by sending the message to each recipient in turn.

AMIS Networking can be used to exchange messages with sites that are part of the private messaging network. When a site is included in the private messaging network, it is called an integrated site. AMIS can also be used to send messages to an open site that is not included in the private messaging network.

When you implement AMIS Networking on a site, you must add information about every integrated remote site that you want to exchange messages with using the AMIS protocol.

Enterprise networking

Enterprise Networking uses a proprietary analog protocol that is based on extensions to the Audio Messaging Interchange Specification (AMIS) protocol. Like the AMIS protocol, the Enterprise Networking protocol uses dual-tone multifrequency (DTMF) tones. Since DTMF is a global standard, Enterprise Networking can be used globally.

The Enterprise protocol typically requires less resource consumption and costs less to operate. For example, when a single message is sent to multiple recipients at the same remote site using AMIS Networking, you make one call for each recipient. With Enterprise Networking, you make only one call.

The Enterprise protocol supports a longer voice message length than AMIS, and Enterprise Networking extensions support additional CallPilot features that are not supported by AMIS Networking.

VPIM networking

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

NMS

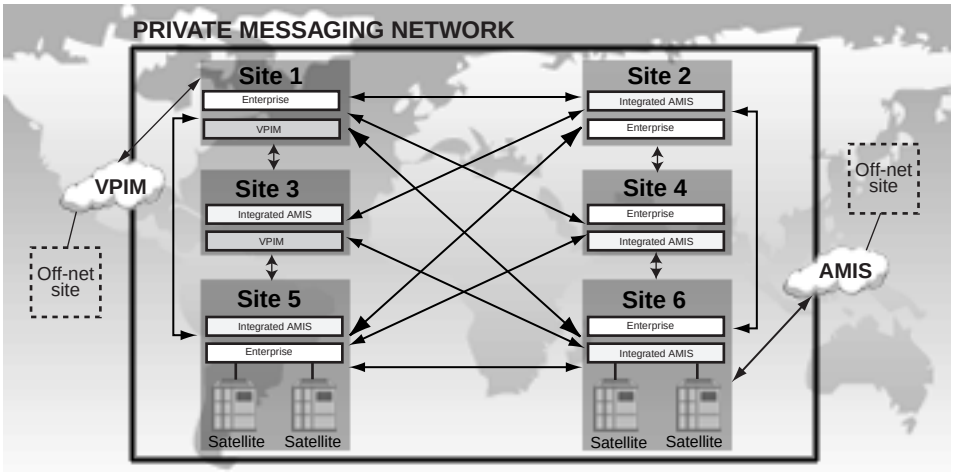
Network Message Service (NMS) is a CallPilot feature that enables one CallPilot Server to provide messaging services to users in a network of compliant switches.

Complex network

You can implement AMIS, Enterprise, and VPIM Networking within a complex network that combines several CallPilot networking solutions. A messaging network is often both open and private, combining various protocols.

The following diagram illustrates a complex network that includes sites with NMS, AMIS Networking, VPIM Networking, and Enterprise Networking implemented.

Because Enterprise Networking is implemented in this messaging network, every site has a unique site ID number.



G101139.eps

While the sites have more than one networking solution implemented, it is recommended that only one protocol be used between any two sites (for example, Site 2 can send messages to site 4 using AMIS, and Site 4 can send messages to Site 2 using Enterprise).

In this example, Site 1 implements VPIM Networking to exchange messages with an open site. Since the AMIS protocol is not used by Site 1 to communicate with any other site within the private messaging network, Site 1 does not implement AMIS Networking.

Site 6 requires the functionality of AMIS Networking to exchange messages with open sites that use the AMIS protocol. Site 6 implements AMIS Networking to exchange messages with integrated sites and open sites.

Configuring the switch using phantom DNs

The switch provides the call handling for CallPilot. When you implement message networking, the switch should be already installed and configured, and is operational. On the switch, you must set up phantom directory numbers (DNs). Message networking needs only one configuration for the switch. A phantom directory number (DN) is required. Review the switch information that you gathered. Confirm the settings to ensure that they are correct.

SDNs on the server have a direct correspondence to phantom directory numbers (DNs) on the switch. If you create a new SDN, you need a phantom DN. If you share an existing SDN with an existing service, networking also shares the phantom DN of that service.

There are two ways to create a phantom DN:

- Use a unique phantom DN. Most switch technicians create additional phantom DNs for use by services like AMIS Networking.
- Share an existing phantom DN.

To access a CallPilot service, a user enters a unique dialable number. The dialable number is known as a directory number (DN). There are different types of DNs, including extension numbers and telephone numbers. The switch uses the DN to route the call to the requested service.

All DNs that you use to access a service correspond to a setting on the switch. To handle calls in sequence of arrival, the system places calls in a queue, called controlled directory number (CDN) queues. Each CDN queue is associated with a dialable number known as the CDN. A user can dial the service directly by entering the CDN. For example, the CDN of Voice Messaging is 7400. A user can dial 7400 to reach Voice Messaging. The call is placed into the queue.

To offer multiple services, the switch uses phantom DNs. A phantom DN is a unique dialable number that is routed to one of the CDN queues. A phantom DN is not a randomly selected number. There is a direct correspondence between the local system access number (SAN) and the phantom DN.

Example

If the local system access number for AMIS Networking is 567-7575, the phantom DN is 7575. If AMIS Networking shares an existing phantom DN, check that the phantom DN is configured to forward messages to the correct CDN queue. For AMIS Networking, the phantom DN should forward messages to the Voice Messaging CDN queue.

Example

The phantom DN for Express Messaging is 7401. A user dials 7401 and expects to reach the requested service. The switch routes the phantom DN to the appropriate CDN queue (in this case, Voice Messaging) before the service is provided.

See also

For detailed information about the configuring the switch, consult your switch documentation.

Configuring CallPilot

The network database contains information about your messaging network. When you configure CallPilot, you add information to the network database. To configure CallPilot for message networking, you must:

- add information to the Service Directory Number (SDN) Table
- define networking information in the Message Delivery Configuration pages
- add detailed information in the Message Network Configuration pages about the local site: information about how the server handles messages and how the switch handles messages
- add detailed information in the Message Network Configuration pages about each integrated remote site that communicates with the local site

SDN Table and message networking

On the server, you must set up inbound and outbound service directory numbers (SDNs). A service directory number (SDN) is a number that enables a user to access a CallPilot service. Each SDN must be unique (except for one exception where SDNs can share a CDN) so that CallPilot can identify the requested service and play the appropriate prompts.

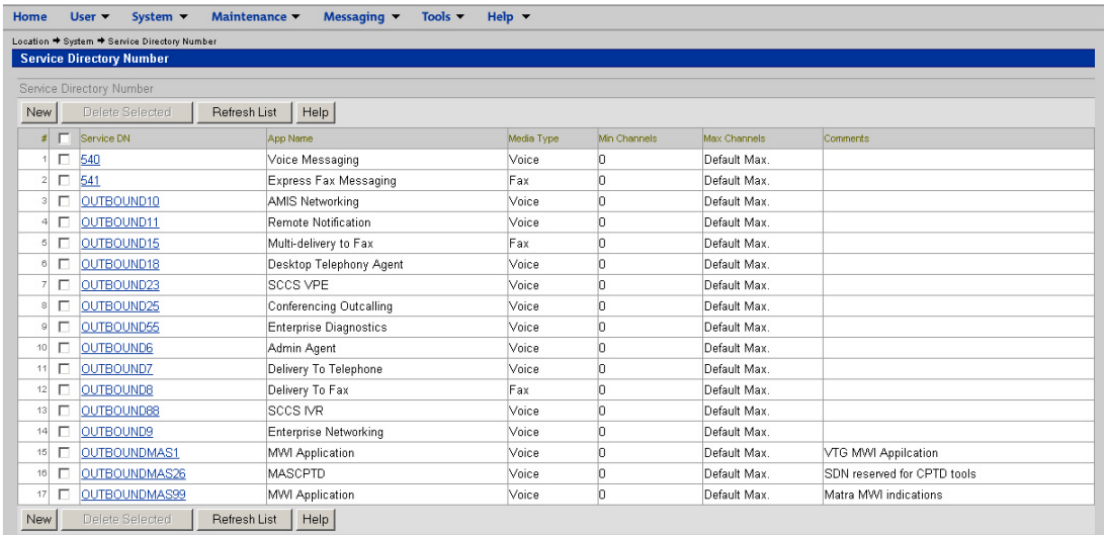
The system automatically creates the Service Directory Number Table during the initial installation of CallPilot. The SDN Table lists all SDNs and provides details about their settings. CallPilot uses the SDN Table to map directory numbers (DNs) to services. The SDN Table lists both inbound and outbound SDNs. You must manually add an inbound SDN. An outbound SDN is created automatically if networking is installed.

For most services, an inbound SDN is a number that a user enters to access a service. However, the message networking inbound SDN is not a directly dialable number. A remote system dials this SDN when it delivers a networking message.

CallPilot uses an outbound SDN to make the requested service available. An outbound SDN consists of the word OUTBOUND and a number.

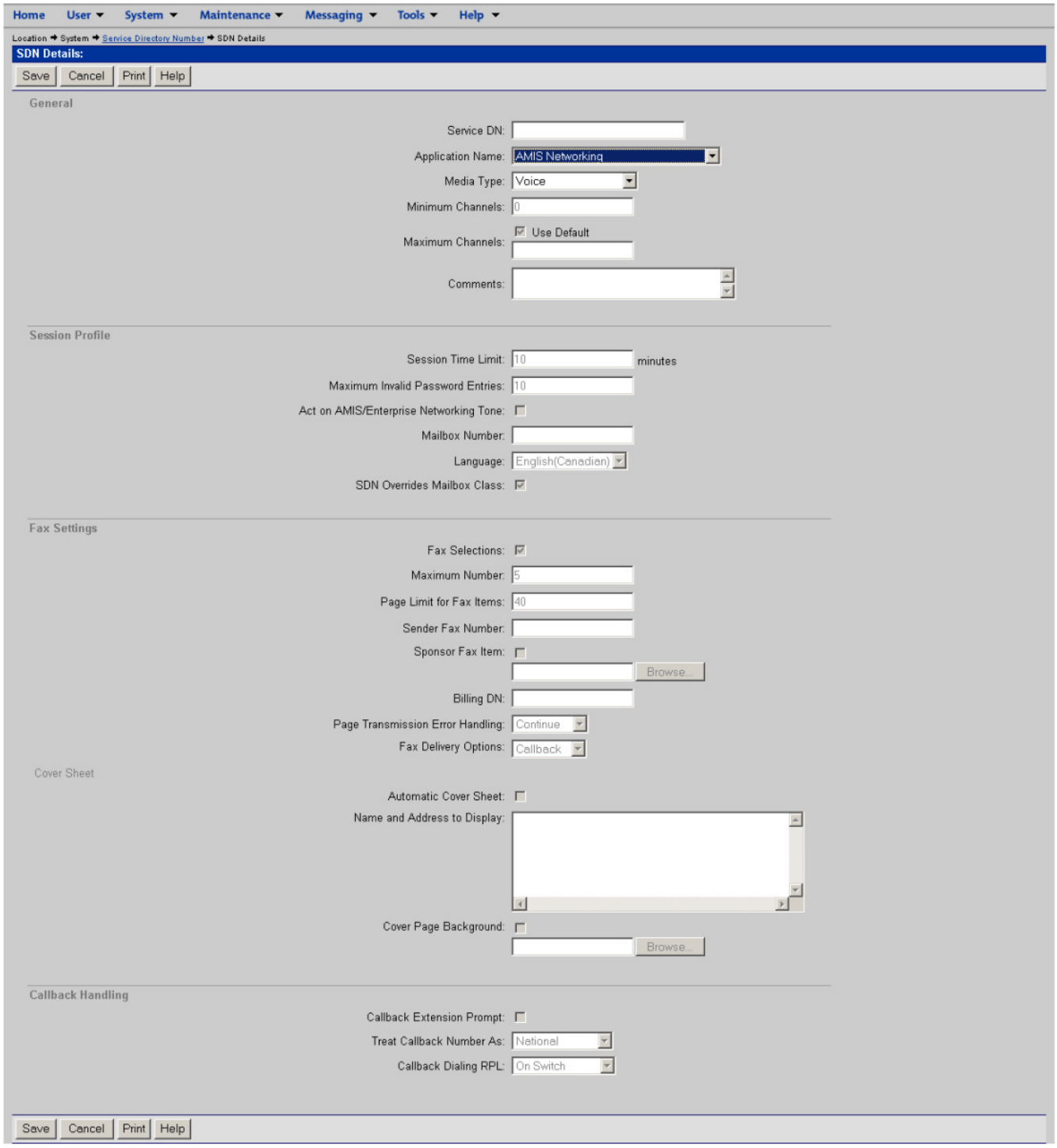
Example: SDN Table

The following image shows an SDN Table that lists both inbound and outbound SDNs.



Creating an SDN

The following image shows the System, Service Directory Number, SDN Details page where you can create an SDN.



SDN numbers

An SDN must be unique, but it is not randomly selected. CallPilot uses SDNs to map numbers to services. There are also important relationships between the SDN and other numbers used by the system.

The CallPilot SDN setup echoes the DN settings on the switch. An important relationship exists between the inbound SDN and the local system access number (SAN), and the phantom DN on the switch.

Example

- The inbound AMIS Networking SDN = 7400.
- The phantom DN for AMIS Networking = 7400.
- The AMIS Networking local SAN = 1-416-597-7400.

The AMIS inbound SDN on CallPilot must correspond to the AMIS phantom DN on the switch. Before you create an SDN, confirm the phantom DN on the switch. To view the phantom DN setting, consult the gathered switch information.

Media type

To process a call, networking needs access to a channel. A channel provides a connection between the switch and the Digital Signal Processor (DSP) cards on the CallPilot server. CallPilot supports three channel types. Each type corresponds to different media:

- voice
- fax
- speech recognition

Networking can use all three channel types. By default, CallPilot automatically assigns a voice port to networking.

Minimum and maximum channels

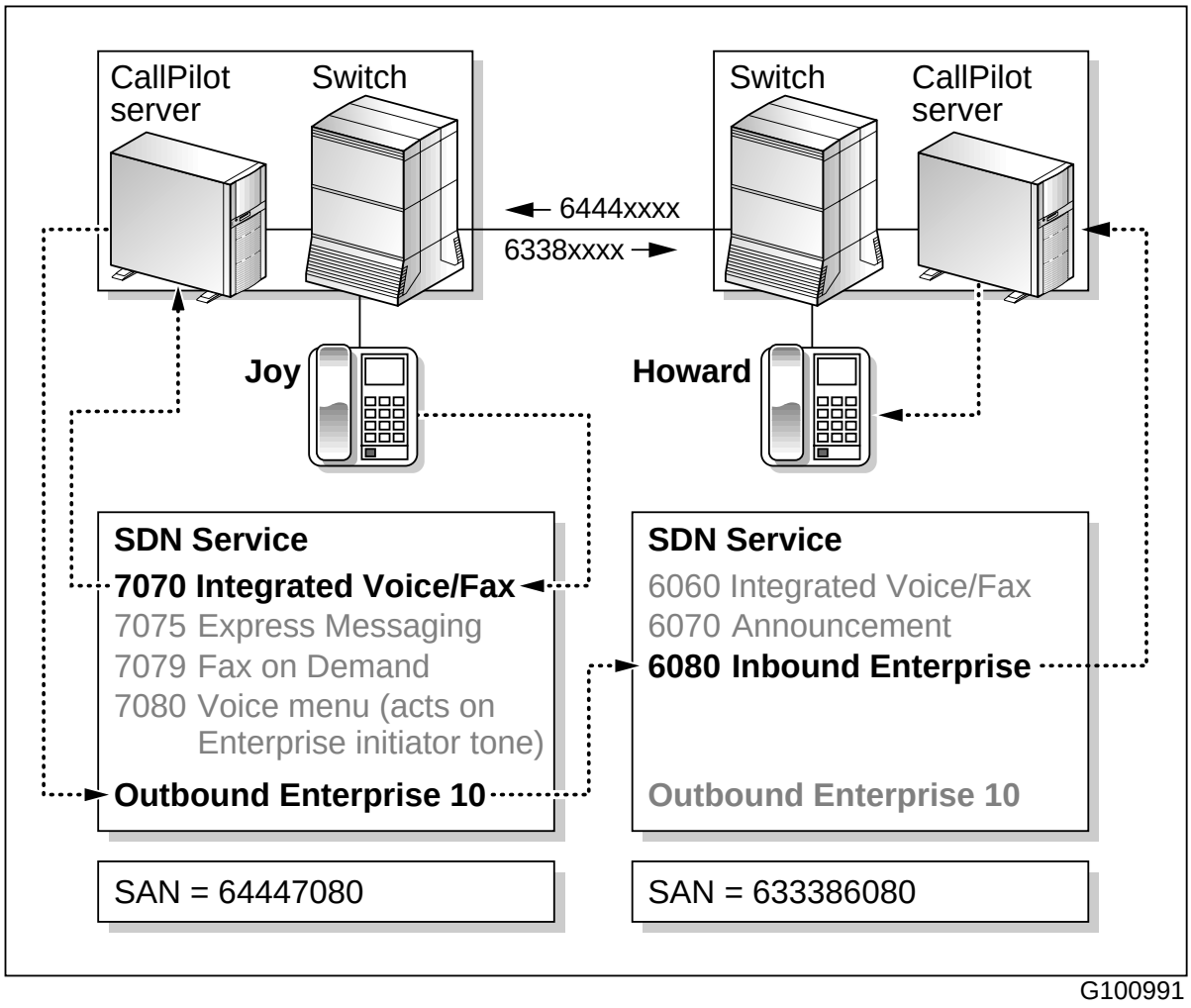
You must determine the channel resources for both inbound and outbound networking SDNs. Every service, including networking, requires channel resources to process calls. Channel resources are the number of channels that networking has available. Channel resources are set as minimum and maximum values. The minimum value is the number of channels that is always reserved for the exclusive use of the service. This setting is important because, if you incorrectly allocate channel resources, users may experience delays in reaching requested services.

Example: Channel allocation

Your system has 96 available channels. You decide to dedicate a minimum of 5 channels and a maximum of 30 channels to networking. If the system handles only 5 networking calls each day, a more appropriate allocation is a minimum of 1 channel and maximum of 3 channels.

Example of unique SDN used with Enterprise networking

Joy wants to send a message to Howard in Philadelphia. She enters 7070, which is directed to the SDN for Integrated Voice/Fax. The request is directed to CallPilot, which routes it to the outbound Enterprise Networking SDN. The system in Chicago calls the remote SAN of the system in Philadelphia, 63386080, and the two systems complete the required handshaking before the message is transferred. The inbound Enterprise Networking SDN receives the message and directs it to Howard's mailbox.



Note: Each SDN must be unique (except for one exception where SDNs can share a CDN). For example, AMIS/Enterprise can be shared with a Voice Messaging SDN because a special tone identifies the switching service.

See also

For detailed information on SDNs and SDN Tables, consult the CallPilot Manager online Help.

Implementing message networking

The following assumptions are made:

- The switch is installed and configured.
- Sufficient trunks that connect the switch to a public switch are available.
- CallPilot is installed and configured, except for networking.
- If it is part of the local site, Network Message Service (NMS) is fully implemented.
- If implementation is an upgrade from Meridian Mail, all legacy information is available or is migrated.
- Contact is made with the network administrators of the remote sites.
- Information is collected from at least one remote system that will communicate with the local system. This information is used to test the system.

The implementation of each networking solution builds upon earlier implementations. Information is often configured only once, and all subsequent networking solutions that are implemented use this configuration.

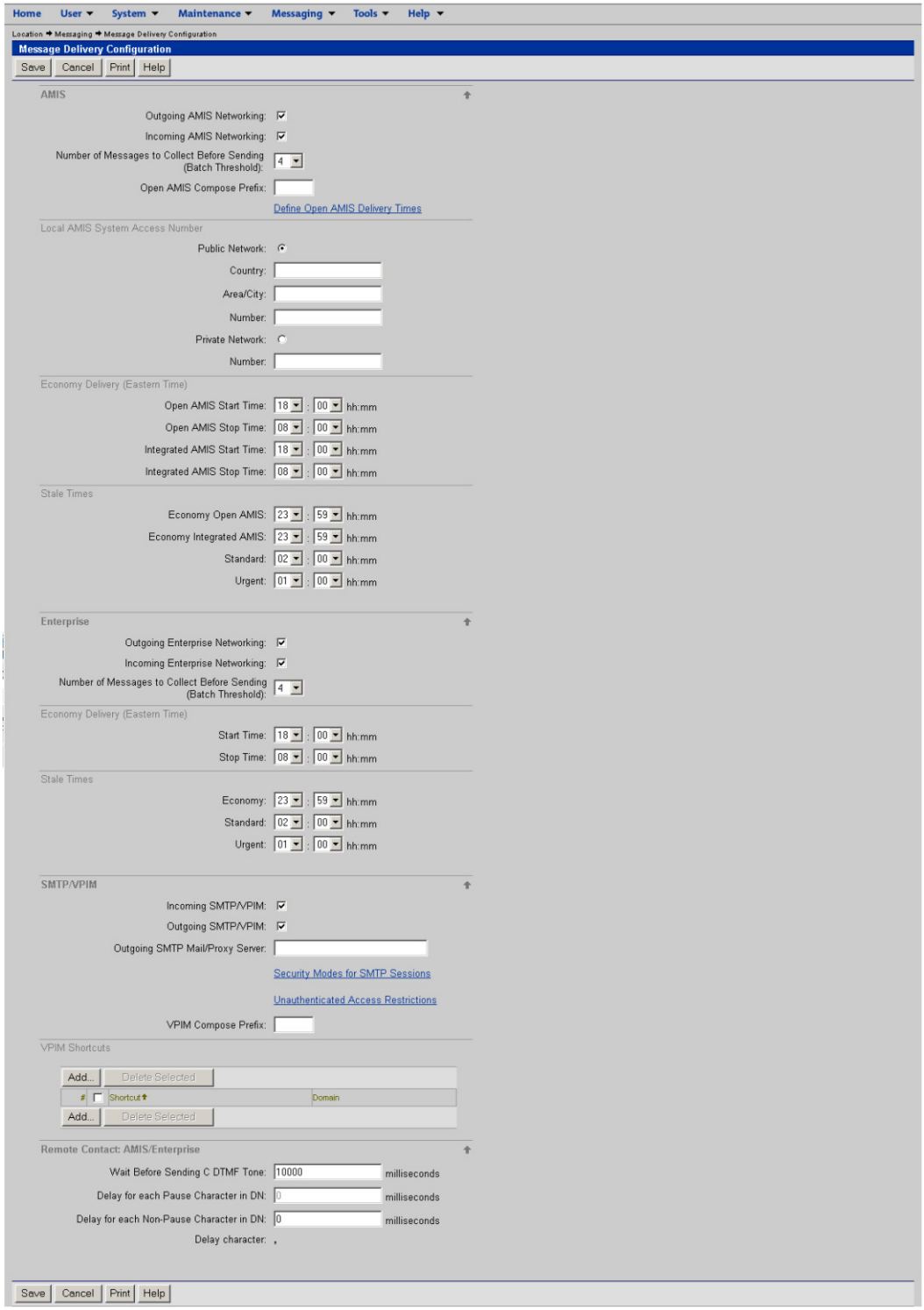
The recommended order for implementation is

- Network Message Service (NMS)—if the local site is an NMS site
- AMIS Networking
- Enterprise Networking
- VPIM Networking

Message Delivery Configuration parameters

You set networking parameters during the implementation process. These parameters work with internal CallPilot settings to control how networking works.

The actual procedures for configuring message networking are detailed in the CallPilot Manager online Help. The following is an overview of the required information. The following image shows the Message Delivery Configuration page from the Messaging menu on CallPilot Manager.



Parameter default values

CallPilot provides default settings for all scheduling parameters. The default values are based on typical requirements. To ensure a quick implementation process, use these default values. After your system is operational, monitor usage to determine if the default settings are serving the needs of your users. You can modify the scheduling parameters whenever users' needs change.

Defaults

CallPilot provides default settings for the message delivery configuration. The default values are based on typical requirements.

To simplify the process of implementing networking, use the default values. After your system is operational, monitor usage and performance to determine if the default settings are sufficient. You can modify the settings whenever users' needs change.

Parameter	Current default
Batch threshold	4 messages
Stale time for standard messages	2 hours
Holding time for standard messages	40 minutes (calculated internally, based on stale time settings)
Stale time for urgent messages	60 minutes
Holding time for urgent messages	6 minutes (calculated internally, based on stale time settings)
Stale time for economy messages	24 hours
Delivery start time for economy messages	6:00 p.m.
Delivery stop time for economy messages	8:00 a.m.

AMIS message delivery configuration

The following message delivery parameters are available for AMIS networking.

As you configure the AMIS Networking message delivery information, you will see several boxes for configuring Open AMIS. If users at the local site exchange messages with open sites, you must configure the Open AMIS boxes.

You must complete all Open AMIS fields when you configure AMIS Networking.

Outgoing and incoming AMIS

If AMIS Networking is installed on your system, the following options are enabled by default:

- Outgoing AMIS Networking
- Incoming AMIS Networking

These boxes restrict the use of AMIS Networking.

If you do not want local users to send outbound AMIS Networking messages, clear the Outgoing AMIS Networking option. If you do not want local users to receive inbound AMIS Networking messages, clear the Incoming AMIS Networking option. To completely disable AMIS Networking, clear both options.

Number of Messages to Collect Before Sending (Batch threshold)

The batch threshold is the number of standard and urgent messages that are held in queue waiting for delivery to a single remote site. When you send messages in batches, you make more efficient use of system resources. However, to ensure that messages awaiting delivery are not held too long in the queue, the holding time overrides the batch threshold. A message is held in a batch until either the batch threshold is exceeded or the holding time for standard or urgent messages is reached.

Holding time

Holding time is the period of time that a message is held in queue before CallPilot attempts delivery. CallPilot holds a message in queue while it awaits the arrival of more messages for the same destination. This bulk sending makes more efficient use of the system.

To ensure that messages are always delivered in a timely fashion and do not wait too long for the arrival of additional messages, they are held for only a set period of time. This is the holding time. CallPilot computes the holding time internally, based on the stale time.

Standard message holding time

The holding time for standard messages is one-third of the stale time for standard messages.

Urgent message holding time

The holding time for urgent messages is one-tenth of the stale time for urgent messages.

Example 1

Milo sends a standard message. The message is held in the queue awaiting the arrival of three more messages. However, when the message has waited in queue for 40 minutes (the holding time for standard messages), the message is sent.

Example 2

Ronnie and Philippe are users at the same site. Ronnie sends three standard messages for users at the remote site in Newmarket. Her messages are held in the queue. Philippe sends a message to a user at the same remote site. The batch threshold is reached, and all four messages are sent.

Example 3

Barney sends an urgent message. It is held in queue. No other messages for the same remote site arrive within six minutes (the holding time for urgent messages). Barney's urgent message is sent.

Open AMIS compose prefix

If users are exchanging messages with open sites, provide the Open AMIS compose prefix. This number alerts the system that the number about to be entered is an Open AMIS address. The Open AMIS compose prefix must not conflict with any other prefixes used in the system, such as the name dialing prefix or the VPIM prefix.

Example

A local user logs in to CallPilot and enters 75 to compose a message. The user enters the AMIS compose prefix (in this example, 13). The system is alerted that this is an AMIS address. To complete the address, the user enters the system access number and the mailbox number, followed by #.

Define Open AMIS delivery times

If local users send AMIS Networking messages to sites that are not part of the messaging network, you must define the Open AMIS delivery times. Open AMIS delivery times determine how AMIS Networking messages are handled during business and nonbusiness days. In some countries, these settings have legal ramifications.

Open AMIS Networking messages are considered computer-generated calls. Since they are sent to recipients who are not part of the private messaging network, there is a risk of disturbing the wrong recipient. For this reason, many countries legally allow computer-generated calls only during set times of the business day.

If your country has these regulations in place, configure the Open AMIS delivery times. If your country does not have these regulations, or if your local site does not send AMIS Networking messages to sites that are not part of the messaging network, do not configure the Open AMIS delivery times.

The legal AMIS delivery times must not conflict with the economy delivery start and stop times. The economy delivery start and stop times must always fit within the legal delivery times.

Parameter	Default
Business days	Monday, Tuesday, Wednesday, Thursday, Friday
Nonbusiness days	Saturday, Sunday
Business day hours	9:00 a.m.–5:00 p.m.
Nonbusiness hours	5:00 p.m.–9:00 a.m.

Example

If it is legal to send computer-generated messages only between 9:00 p.m. and 1:00 a.m., the economy delivery times cannot be set to 6:00 p.m. and 6:00 a.m. In this example, the economy delivery time must be set within the legal hours (for example, 9:30 p.m. and 12:30 a.m.).

Local AMIS System Access Number

The destination system uses the local system access number (SAN) to identify the source system of the message. The system access number is included in the header of all outgoing messages. When a recipient of an AMIS Networking message uses the Reply feature or its equivalent to contact the originator of the message, the caller uses the system access number to send a reply to the originating system.

You can use two types of local system access number:

- **Public network access number** You need this type of local system access number if you use AMIS Networking to send messages to remote sites outside of your private messaging network.
- **Private Network access number** You need this type of local system access number if you use AMIS Networking only to send messages within your private network.

The public network access number consists of the following:

- the country code of the local site (up to four digits long)
- the area/city code of the local system (up to eight digits long)
- the directory number of the voice service (the exchange code and the directory number) that will accept AMIS Networking calls

Example

- The country code is 1, the area/city code is 416, and the number to send an outbound AMIS Networking message is 5553653. The system access number sent with the message consists of 14165553653.

Note: The actual system access number in the header is 1#416#5553653. The system inserts the pound (#) symbols.

The private network access number is made up of the dialing plan prefix and the SDN for AMIS Networking (for example, the ESN prefix 6338, and the SDN 7707). The private system access number must be dialable from all sites in the messaging network. The use of a private network access number is uncommon.

Economy Delivery (Eastern Time)

An economy message is a message that a user tags for economy delivery. Economy messages are treated differently from standard and urgent messages. Economy messages are collected through the day and sent only during designated times, rather than held in queues. The delivery start and stop times determine when the system sends economy messages to their destinations. Economy messages often have a start time set to the beginning of lower-rate telephone services, and a stop time set to the resumption of regular rates. For example, if the telephone rate is lower between 11:00 p.m. and 6:00 a.m., set the start time at 11:00 p.m. and the stop time at 5:59 a.m

Set delivery times for economy messages in the following boxes:

- Open AMIS Start Time
- Open AMIS Stop Time
- Integrated AMIS Start Time
- Integrated AMIS Stop Time

Example

At 8:00 a.m., Marge sends an economy message to a remote site. The message is held in queue until the economy delivery start time. The message is held in queue for a total of 16 hours. The economy message stale time is large enough to take this into account.

Note: You may have to adjust the economy delivery start and stop times if you also configure the Open AMIS delivery times.

The AMIS economy delivery start and stop times must have some overlap with Open AMIS delivery times for both business and nonbusiness days. If there is no overlap, delivery will not be attempted. Allow at least one hour of overlap to allow for retries.

Example

It is legal to send computer-generated messages only between 8:00 p.m. and 1:00 a.m. on business days, and between 10:00 a.m. and 8:00 p.m. on nonbusiness days. The economy delivery times are set to between 6:00 p.m. and 6:00 a.m. The economy messages will be delivered only between 6:00 p.m. and 1:00 a.m. on business days, and between 6:00 p.m. and 8:00 p.m. on nonbusiness days.

Note: The stale times for economy messages, if altered from the default values, should allow for the maximum noneligible time period. For this example, therefore, on nonbusiness days allow for 8:00 p.m. to 6:00 p.m. the following day, plus one hour for retries (that is, 23 hours).

Stale Times

Stale time is the period of time that CallPilot holds an undelivered message before it considers the message undeliverable and returns it to the sender with a non-delivery notification (NDN). In the period before a message is considered stale, CallPilot makes repeated attempts at delivery. You set stale times independently for economy, standard, and urgent messages. Typically, the stale time for a standard message is longer than the stale time for an urgent message, because it may be critical for a user to know that an urgent message was not delivered. Stale time is expressed as a time period, such as 10 minutes or 5 hours.

Economy Open AMIS

Set a stale time for economy Open AMIS messages if local users send AMIS Networking messages to open sites.

Economy Integrated AMIS

The economy delivery stale time is usually longer than the standard and urgent stale times. It is expressed as a time period, such as 23 hours. To calculate an appropriate stale time, you must consider other scheduling parameters. The economy stale time that you set must allow for the length of time a message may be held due to the settings for the economy delivery start and stop times.

The default economy delivery stale time is 23:59 (hh:mm).

ATTENTION! It is strongly recommended that you use the default.

Example

If an economy message can only be delivered starting at 6:00 p.m., and an economy message is sent at 8:00 a.m., the stale time must be at least 10 hours. If an hour is allowed for retries, then the minimum stale time is 11 hours.

Stale times affect how long messages are held by CallPilot while waiting for other messages to the same remote site. CallPilot uses stale time settings to calculate holding times.

Standard

For standard messages, the holding time is one-third of the stale time. For example, if you set the standard stale time to 6 hours, the standard message holding time is automatically set to 2 hours.

Urgent

For urgent messages, the holding time is one-tenth of the stale time. For example, if you set the urgent stale time to 30 minutes, the urgent message holding time is automatically set to 3 minutes.

Remote Contact: AMIS

Set time values for the following parameters:

- Wait Before Sending C DTMF Tone
- Delay for each Pause Character in DN
- Delay for each Non-Pause Character in DN

The Delay Character is a default value.

Enterprise message delivery configuration

You must configure various message delivery settings when you implement Enterprise Networking. Determine these settings in cooperation with the network administrators of all sites. The settings must be decided on before any site is implemented.

Outgoing and incoming Enterprise networking

If Enterprise Networking is installed on your system, the following options are enabled by default:

- Outgoing Enterprise Networking
- Incoming Enterprise Networking

These boxes restrict the use of Enterprise Networking.

If you do not want local users to send outbound Enterprise Networking messages, clear the Outgoing Enterprise Networking option. If you do not want local users to receive inbound Enterprise Networking messages, clear the Incoming Enterprise Networking option. To completely disable Enterprise Networking, clear both options.

Number of Messages to Collect Before Sending (Batch threshold)

See "Number of Messages to Collect Before Sending (Batch threshold)" on page 178.

Economy Delivery (Eastern Time)

See "Economy Delivery (Eastern Time)" on page 180.

Stale Times

See "Stale Times" on page 181.

Remote Contact: Enterprise

Set time values for the following parameters:

- Wait Before Sending C DTMF Tone
- Delay for each Pause Character in DN
- Delay for each Non-Pause Character in DN

The Delay Character is a default value.

VPIM message delivery configuration

You must configure various message delivery settings when you implement VPIM Networking. Determine these settings in cooperation with the network administrators of all sites. The Message Delivery Configuration page is shown on page 176.

SMTP/VPIM section

Incoming SMTP/VPIM

Check this option to allow CallPilot to receive messages from other systems using VPIM Networking. To prevent the server from receiving messages from any remote systems, clear this option. This option is checked by default, and must be enabled if you want to allow users to send messages with desktop messaging. The Outgoing SMTP/VPIM option applies to VPIM Networking only and does not affect desktop messaging.

Outgoing SMTP/VPIM

Check this option to allow CallPilot to send messages to integrated and open remote systems using VPIM Networking. To prevent the server from sending messages to any remote systems, clear this option. This option is checked by default.

Outgoing SMTP Mail/Proxy Server

Type the fully qualified domain name (FQDN) for the server to route outgoing messages through an e-mail or proxy server. The maximum length is 255 alphanumeric characters and the default port number is 25. To change the port number, type a colon after the FQDN, followed by the port number.

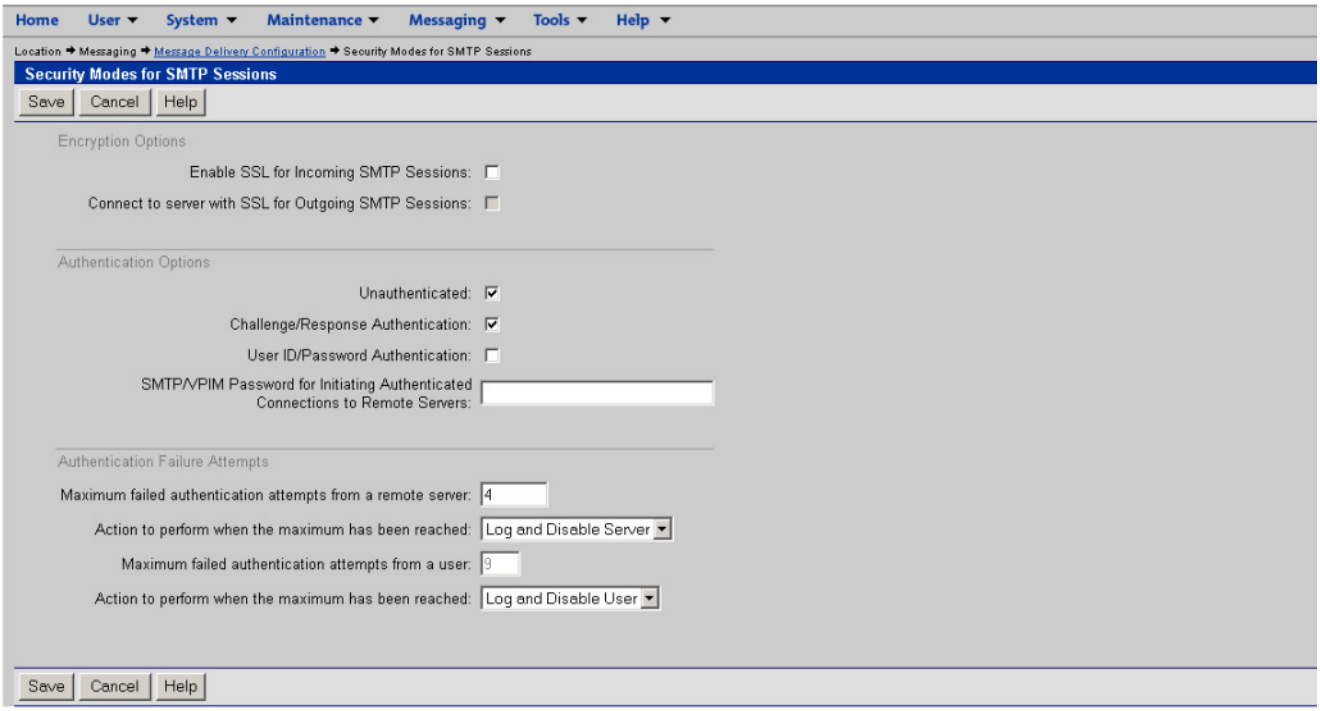
Security and Encryption Modes for SMTP Sessions

The following section deals with the security and encryption options you can set for VPIM SMTP sessions.

For additional information on CallPilot security and encryption techniques and options, refer to Chapter 12, Security and encryption.

Security Modes for SMTP Sessions section

Click Security Modes for SMTP Sessions to display the following page.



Encryption Options section

Enable SSL for Incoming SMTP Sessions

Choose this option if you want to establish secure connections with incoming connecting SMTP hosts. When enabled, the CallPilot SMTP server listens on port 465 for encrypted connection requests. This option is cleared by default.

Connect to server with SSL for Outgoing SMTP Sessions

Choose this option if you want to encrypt outgoing VPIM Networking message transmission sessions. When enabled, the CallPilot SMTP server attempts to initiate secure connections with the SSL port on remote SMTP hosts. This option is cleared by default. If the Enable SSL for incoming SMTP Sessions check box is cleared, this option is not available.

Authentication Options section

Unauthenticated

Choose this option if you want to accept messages from desktop messaging and My CallPilot clients and remote servers in your messaging network without SMTP authentication. This option is checked by default. When checked, CallPilot accepts messages from unauthenticated desktop messaging and My CallPilot users and remote servers. If unauthenticated mode will be used, Nortel Networks recommends that you also enable unauthenticated access restrictions for servers and desktop messaging users.

Challenge/Response Authentication

Choose this option if you want CallPilot to request SMTP authentication using the CRAM-MD5 challenge and response algorithm. This option is checked by default.

User ID/Password Authentication

Choose this option if you want CallPilot to request SMTP authentication using the User ID and Password algorithm. This option is cleared by default. Nortel Networks recommends that you also enable encryption to prevent password transmission in the clear.

SMTP/VPIM Password for Initiating Authenticated Connections to Remote Servers

If authentication will be used, type the password that CallPilot should send when initiating outgoing message transmissions to remote servers. A blank password means that CallPilot will not attempt to perform SMTP authentication when connecting to remote servers. The password should:

- contain a minimum of 6 characters
- be mixed uppercase and lowercase
- contain both letters and digits or special characters
- have a maximum length of 30 alphanumeric characters

Authentication Failure Attempts section

Maximum failed authentication attempts from a remote server

Type a number to identify how many times a remote server can fail SMTP authentication before an event is logged. Default: 4

Action to perform when the maximum has been reached

Choose one of the following options:

- Log only: To report an event in the event log only.
- Log and Disable Server: To report an event in the event log and disable incoming message receipts from the server that failed SMTP authentication. This option is enabled by default. When the remote server is disabled, CallPilot rejects all incoming VPIM messages from that server (both authenticated and unauthenticated). This prevents hackers from trying all the possible password combinations, and eventually obtaining the correct password. If unsuccessful authentication attempts continue, CallPilot reports an event for each time the maximum number of failed attempts is exceeded.

Maximum failed authentication attempts from a user

This option identifies how many times a desktop messaging or My CallPilot client can fail SMTP authentication before an event is logged. The default is 9 (it can be changed on the Security page).

Action to perform when the maximum has been reached

Choose one of the following options:

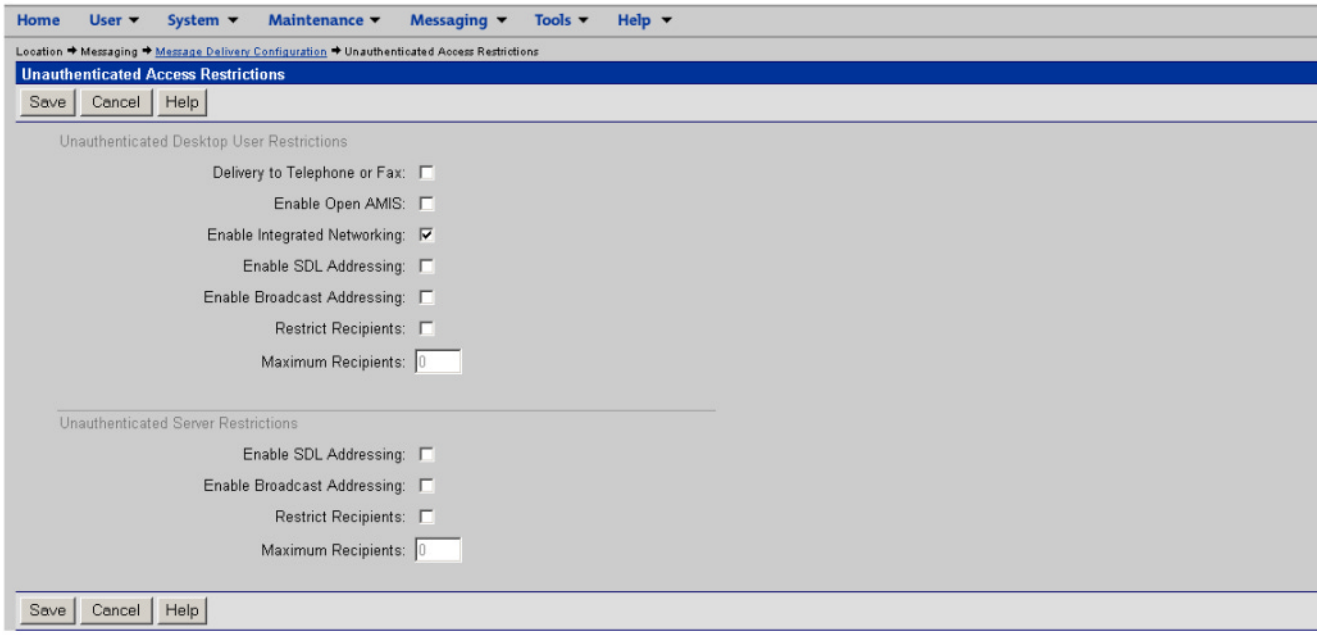
- Log only: To report an event in the event log only.

- Log and Disable User: To report an event in the event log and disable the mailbox belonging to the desktop messaging or My CallPilot user that failed SMTP authentication. This option is enabled by default. When the user's mailbox is disabled, CallPilot rejects the following from the user:
  - all attempts to log on to the mailbox (including logon attempts from a phoneset)
  - all incoming VPIM messages from a desktop messaging or My CallPilot client that is configured as belonging to the user.

This prevents hackers from trying all the possible password combinations, and eventually obtaining the correct password. If unsuccessful authentication attempts continue, CallPilot reports an event for each time the maximum number of failed attempts is exceeded.

Unauthenticated Access Restrictions

Click Unauthenticated Access Restrictions to display the following page. UARs are used to restrict the capabilities of desktops or servers who use an unauthenticated SMTP login to send messages to CallPilot.



Unauthenticated Desktop User Restrictions section

Delivery to Telephone or Fax

Choose this option if you want to allow desktop messaging and My CallPilot users to send Delivery to Telephone (DTT) or Delivery to Fax (DTF) messages. When checked, users are still constrained by the desktop restriction/permission list and their own mailbox class restrictions. This option is cleared by default.

Enable Open AMIS

Choose this option if you want to allow desktop messaging and My CallPilot users to address messages to open AMIS sites. When checked, users are still constrained by the desktop restriction/permission list and their own mailbox class restrictions. This option is cleared by default. If AMIS Networking is not enabled on CallPilot, this option is not available.

Enable Integrated Networking

Choose this option if you want to allow desktop messaging and My CallPilot users to address messages to users at integrated sites. When checked, users are still constrained by the desktop restriction/permission list and their own mailbox class restrictions. This option is enabled by default.

Enable SDL Addressing

Choose this option if you want to allow desktop messaging and My CallPilot users to address messages to shared distribution lists. When checked, users are still constrained by their own mailbox class restrictions. This option is cleared by default.

Enable Broadcast Addressing

Choose this option if you want to allow desktop messaging and My CallPilot users to address messages to location broadcast or network broadcast addresses. When checked, users are still constrained by their own mailbox class restrictions. This option is cleared by default.

Restrict Recipients

Choose this option if you want to limit the number of recipients that a message from a desktop messaging or My CallPilot user can contain. This prevents hackers from copying the contents of a large address book into the recipient list. The limit applies to all recipients within the message, including recipients in nested messages. This option is cleared by default. When cleared, CallPilot allows messages that contain any number of recipients.

Maximum Recipients

Type a number to identify how many recipients the message can contain in each of the TO, CC, and Blind CC recipient lists. CallPilot enforces the limit separately for each address list. For example, if the limit is defined as 100, the user can enter 100 addresses in each of the TO, CC, and Blind CC recipient lists. If any recipient list exceeds this limit, CallPilot rejects the entire message and sends a non-delivery notification (NDN) to the user. Range: 0 (no restrictions on the number of recipients) to 999 (maximum of 999 recipients). The default is 10.

Unauthenticated Server Restrictions section

Enable SDL Addressing

Choose this option if you want CallPilot to accept messages from remote servers that are addressed to shared distribution lists. This option is cleared by default. When cleared, CallPilot rejects messages addressed to shared distribution lists and sends non-delivery notifications (NDNs) to the senders.

Enable Broadcast Addressing

Choose this option if you want CallPilot to accept messages from remote servers that are addressed to location broadcast or network broadcast addresses. This option is cleared by default. When cleared, CallPilot rejects messages addressed to broadcast addresses and sends non-delivery notifications (NDNs) to the senders. You can also block incoming network broadcasts from a specific network site or all sites in the network database. This capability is in addition to the SMTP authentication feature. See Network and location broadcasts.

Restrict Recipients

Choose this option if you want to limit the number of recipients that a message from a remote server can contain. This prevents hackers from copying the contents of a large address book into the recipient list. The limit applies to all recipients within the message, including recipients in nested messages. This option is cleared by default. When cleared, CallPilot allows messages that contain any number of recipients.

Maximum Recipients

Type a number to identify how many recipients the message can contain in each of the TO, CC, and Blind CC recipient lists. CallPilot enforces the limit separately for each address list. For example, if the limit is defined as 100, the sender can enter 100 addresses in each of the TO, CC, and Blind CC recipient lists. If any recipient list exceeds this limit, CallPilot rejects the entire message and sends a non-delivery notification (NDN) to the sender. The Range is 0 (no restrictions on the number of recipients) to 999 (maximum of 999 recipients). The Default is 10.

VPIM Compose Prefix

The open VPIM compose prefix is a number that identifies a message that is to be delivered to an open site using the VPIM protocol. When users address a message to an open VPIM site, they enter the compose prefix before entering the address. Define the open VPIM compose prefix if any local users want to exchange VPIM messages with open sites. The open VPIM compose prefix must not conflict with any other prefixes, shared distribution lists (SDLs), broadcast mailboxes, or a dialing plan access code.

If you are verifying settings for desktop messaging, you do not need to define the open VPIM compose prefix. The open VPIM compose prefix does not affect desktop messaging. Type the prefix in the VPIM Compose Prefix box The maximum length is 5 digits (0–9).

VPIM Shortcuts section

If users want to send messages to VPIM-compliant sites that are not defined in your network database, you must create open VPIM shortcuts since alphabetic characters cannot be entered from the telset. The open VPIM shortcut can be any number. Nortel Networks strongly recommends using the open site's Public Switched Telephone Network (PSTN) number because it is familiar to your users, so it is easy to remember, and it is a unique number that is unlikely to conflict with neighboring voice mail systems when users send and receive open VPIM messages.

When defining the shortcut, use a long number to ensure that the mapping is correct and no conflict occurs. A short number can conflict with the left side of another SMTP address. To address a message to the open VPIM site, users must enter the VPIM compose prefix (which tells CallPilot that the message is destined for an open VPIM site), the open VPIM shortcut, and destination mailbox number. For example:
1905225 is created as a shortcut for an open VPIM site at another_company.com. If a phoneset user wants to address a VPIM message to mailbox 1234 at that open site, he or she must first enter the VPIM compose prefix, and then enter 19052251234 as the address. When CallPilot sends the message, the message header's To: address is generated as 19052251234@other_server.another_company.com.

In the VPIM Shortcuts section, click Add.

Shortcut and Domain

Type the numeric shortcut for the open VPIM site in the Prefix box. The maximum length is 20 digits (0–9). Type the open VPIM site's FQDN name in the Domain box. The maximum length is 255 alphanumeric characters. The maximum number of open VPIM shortcuts is 500.

chapter 11

Configuring local and remote networking sites

In this chapter

Overview 191

Configuring the local messaging server 192

Configuring the local prime switch location 195

Adding and configuring a remote site 200

Configuring a remote messaging server 200

Configuring a remote prime switch location 207

Configuring a remote satellite switch location 210

Overview

This chapter describes how to configure the local messaging server and prime switch location. It also explains how to add and configure remote messaging servers and switch locations. 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, you do not add it to the tree view.

When CallPilot is initially installed on your system, a local messaging server and local switch location are automatically added to the Messaging Network Configuration tree view. To implement networking, configure the local site and add and configure all remote sites that will transfer messages with the local site.

ATTENTION!

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

Before you begin

You should have already configured the Message Delivery Configuration options.

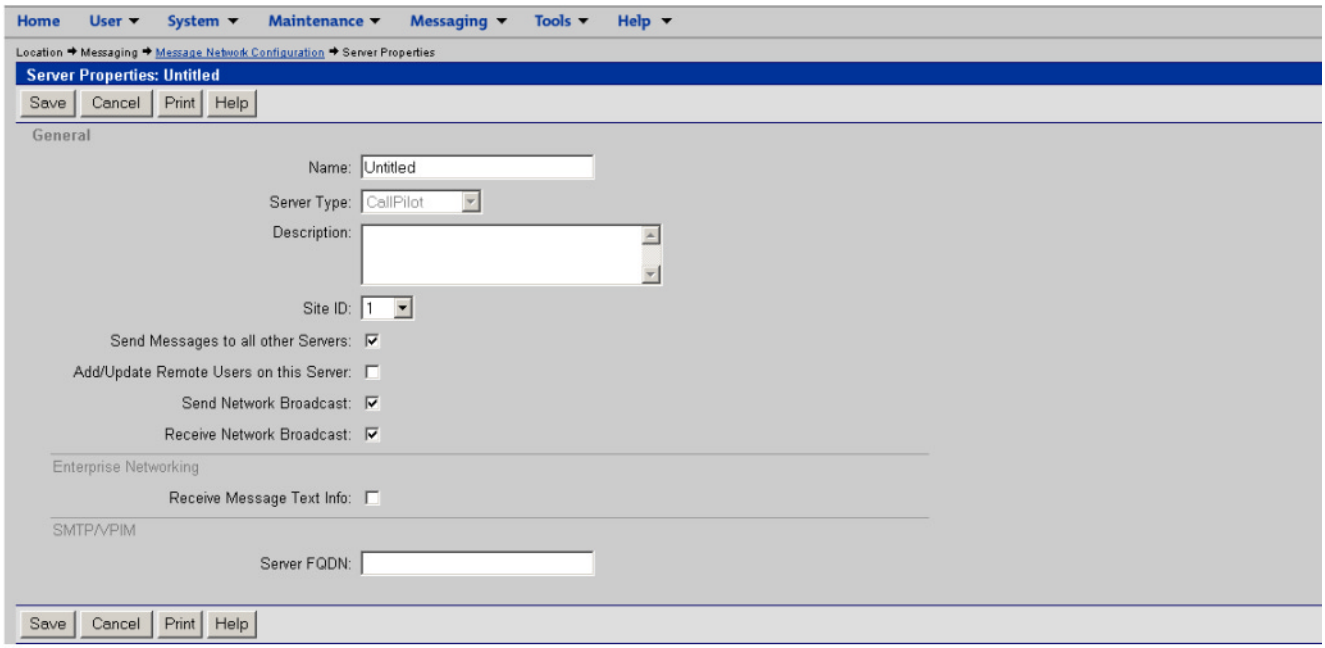
If your local site is an NMS site, NMS should be configured and tested. If NMS is installed, the NMS satellite switch locations for the local site appear in the Messaging Network Configuration tree view in alphabetical order.

Your messaging network representation should be complete and available. This representation provides a blueprint for the implementation process.

Configuring the local messaging server

You must configure the local messaging server to implement message networking.

The local messaging server is configured from the Message Network Configuration page that shows the local messaging server on the Network Tree. Doubleclick the local server to display the Server Properties. The following image shows the Server Properties page for the local messaging server.



General section

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. 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.

Site ID

To implement networking, you must assign a site ID to your local messaging server. The site ID, combined with the location ID, identifies the local site to remote sites in the messaging network.

The site ID is one of the pieces of information included in a message header. When networking is implemented on any site in a messaging network, every site that exchanges networking messages with it must have a site ID.

If the Site ID box is enabled, the Local Messaging Server Properties information cannot be saved to the network database unless the Site ID box contains some information. If you do not know the Site ID, enter a valid placeholder and then enter the correct ID when you implement networking.

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.

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

To prohibit the local messaging server from sending messages to a particular remote site, clear the Send Messages to this Server check box in the Remote Messaging Server Properties page. For example, your messaging network has six sites. You do not want to send messages to one of these sites. You select the Send Messages to all other Servers option while you configure the local messaging server. You clear the Send Messages to this Server box while you configure the remote server to which you do not want to send messages.

Note: When the Send Messages to all other Servers box is cleared, users can still send messages to open sites using the VPIM and AMIS protocols.

Add/Update Remote Users on this Server

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 available with Enterprise Networking only.

This box controls your local server. You must coordinate with the network administrator of each remote site with which you want to enable Names Across the Network. You can use Names Across the Network only with remote sites that use Enterprise Networking and have the Send Remote User Info feature enabled.

The Names Across the Network feature is not the only way to add remote users to your local network database. You can also add remote users manually with User Administration. For a detailed discussion of remote users and Names Across the Network, consult Chapter 3, Understanding CallPilot networking solutions in this guide.

Send Network Broadcast and Receive Network Broadcast

Both check boxes apply to network-wide broadcasts, and location-specific broadcasts to and from all locations associated with remote sites.

Enterprise Networking section

Receive Message Text Info

The Receive Message Text Info check box is enabled only if Enterprise Networking is installed on your local messaging server. Configure this box when you implement Enterprise Networking.

The local messaging server can receive message subject headers in the messages sent by all remote sites that are enabled to send message subject headers. The message subject header is available to desktop users. In most environments, the Receive Message Text Info check box is selected. However, if voice ports become tied up for too long, you may want to clear this option because these messages take longer to send.

SMTP/VPIM section

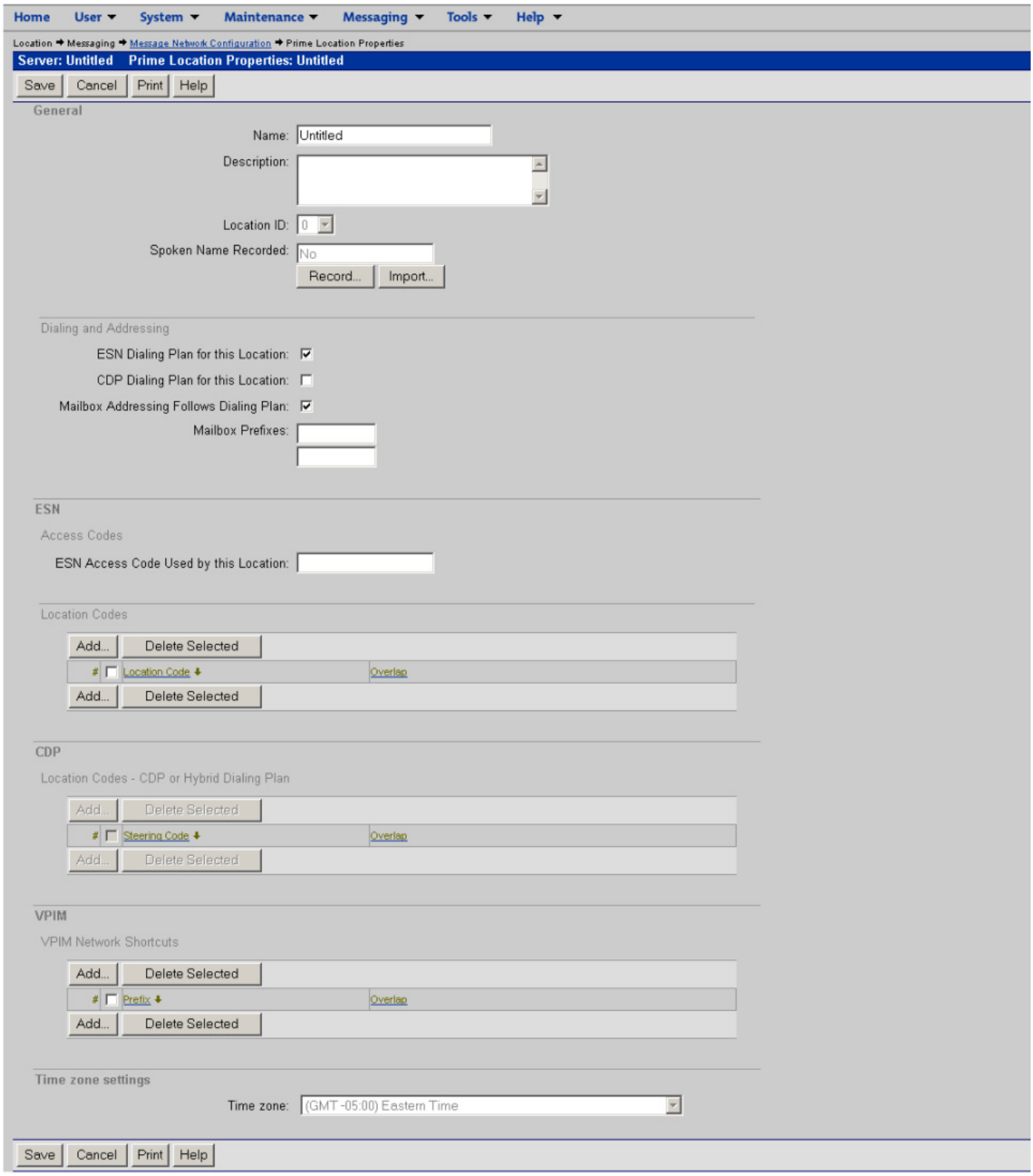
Server FQDN

The Server FQDN box is enabled only if VPIM Networking is installed on your system. It is configured during the implementation of VPIM Networking. However, the message delivery information cannot be saved to the network database unless the Server FQDN box contains the correct information. Enter the computer name and domain for CallPilot. If you do not know what the FQDN is, to find it use the ‘ipconfig/all’ command from a DOS window, or get the information from the appropriate ‘properties’ window.

Note: Do not continue configuring the system if you do not have the proper FQDN.

Configuring the local prime switch location

You must configure the local prime switch location to implement networking. The final step in configuring the local site is to configure the local prime switch location. The local prime switch is configured from the Message Network Configuration page that shows the local prime switch on the Network Tree. Doubleclick the local prime switch to display the Server Properties. The following image shows the Prime Location Properties page.



Note: If another networking solution has already been implemented on the local site, the local prime switch location is already configured. Check the current configuration information. Make any necessary modifications. Also, If NMS is installed on the local site, the local prime switch location is already configured. All satellite switch locations attached to the local prime switch location are also already configured. Check the current configuration information. Make any necessary modifications. If no other networking solution is implemented on the local site, complete the Prime location Properties page.

General section

Complete the General section no matter what dialing plan is used on your local site. The fields are described below.

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.

Location ID

The Location ID box is not enabled for the prime switch location. The location ID for the prime switch location is always 0 and cannot be changed.

Spoken Name Recorded

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

If a spoken name is not recorded, local users hear a full mailbox address 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, “Mailbox 6444 2346”.

You may decide that you do not want local users to hear a spoken name for a particular site. For example, if CDP is used for messaging with a 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.

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 and Addressing section

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

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

- ESN Dialing Plan for this Location

- CDP Dialing Plan for this Location
- (hybrid, which combines ESN and CDP)

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

Mailbox Addressing Follows Dialing Plan

If NMS is implemented, this check box should be properly configured already.

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, should already be properly configured.

ESN section

Access Codes

If the local prime switch location uses either an ESN dialing plan or a hybrid dialing plan, you must complete the ESN section. You must provide the ESN access codes and ESN location codes. These are combined to create the ESN prefix.

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.

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

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 the 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
6	300	**8**300-8999	6300**8**300-6300**8**999	0
6	30**2**	**2**5000-**2**6999	630**2**5000-630**2**6999	1

CDP section

Location Codes - CDP or Hybrid Dialing Plan

If the local switch location uses either a CDP dialing plan or a hybrid dialing plan, complete the CDP section. You must provide the CDP steering codes.

Steering Code

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

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	Amount of overlap
22	**22**345	**2222**345	0
22	**22**345	**222**345	1
22	**22**345	**22**345	2

VPIM section

VPIM Network Shortcuts

The VPIM network shortcut identifies the switch location to desktop messaging clients. In the VPIM section, click Add. The VPIM Network Shortcut Detail page appears.

Prefix

Type the shortcut in the Prefix box. The maximum length is 30 digits (0–9). The recommended format is the same as the PSTN number (country code + area code + exchange portions).

Overlap

In the Overlap box, specify the number of digits that overlap with the mailbox number.

Time Zone Settings section

Time zone

The time zone for the local prime switch location is automatically the same as the time zone for the CallPilot server. It is configured in the CallPilot Configuration Wizard.

Adding and configuring a remote site

When you implement a protocol, you add to the Messaging Network Configuration tree view all the remote sites that use that protocol to receive messages from the local site. Every remote site added to the tree view must be configured.

The information that you enter when configuring a remote site often reflects the information that is configured for that site in its own local network database. The name for the site can be different however the site IDs must match. You can 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.

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

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

Correcting information about remote sites already added to the network database

If you are implementing a network solution, and another messaging network solution is already implemented on your local site, check the information for the remote messaging servers that you added to your local network database during that configuration.

For example, if you added remote sites to your network database during the installation of Integrated AMIS Networking, you added the remote sites that use the AMIS protocol to send messages to and receive messages from your local site. When configuring these remote sites, the validation process forced you to enter an Enterprise site ID for the remote site to save the configuration to your network database.

You must check the Enterprise site IDs that you entered for these sites to ensure that they are valid and correct. If you entered a random number as a placeholder, change them to actual site ID numbers.

Configuring a remote messaging server

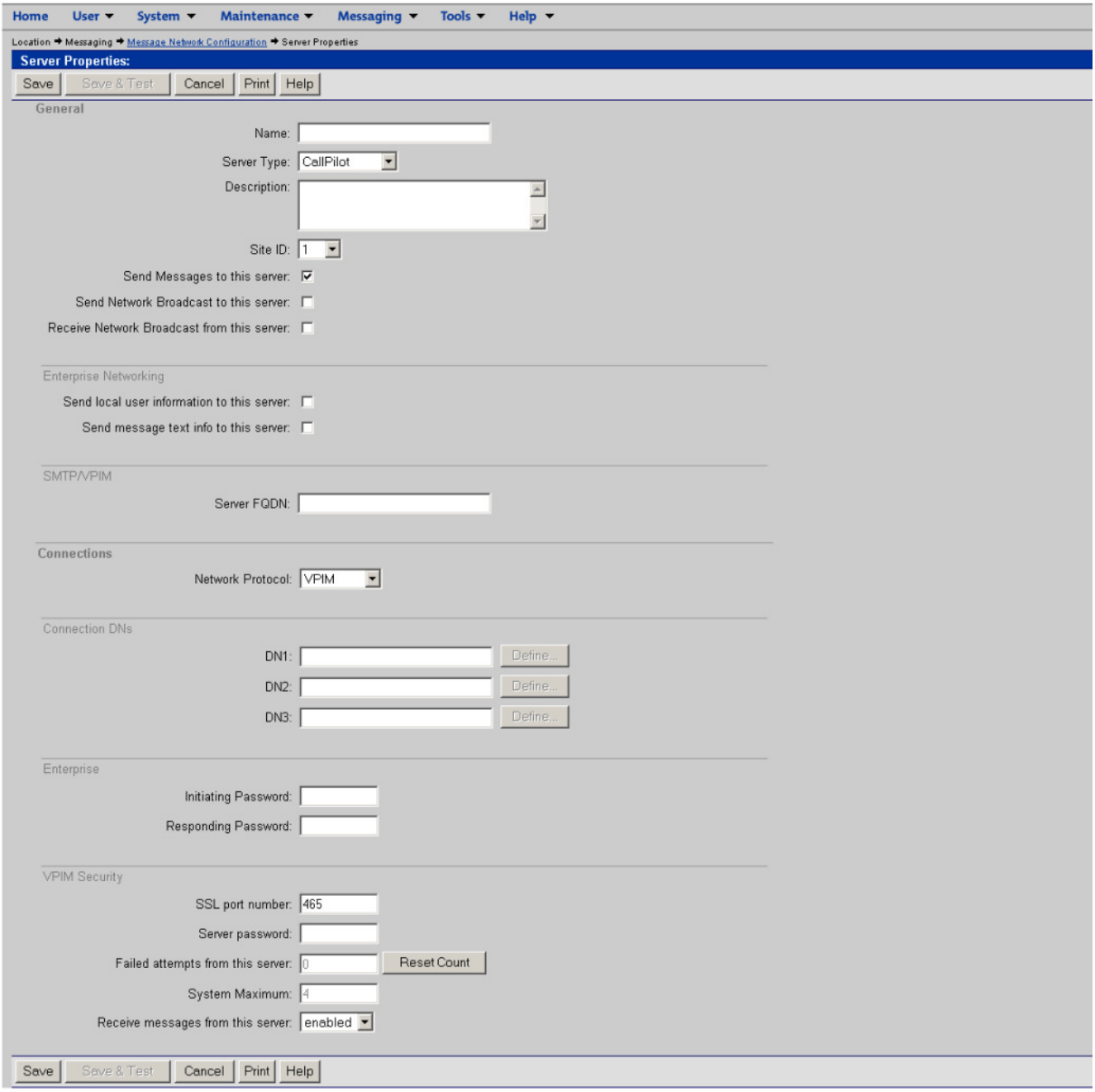
When you initially install CallPilot on your system, your local site, which consists of a local messaging server and a local prime switch location, is automatically added into the Messaging Network Configuration tree view.

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

You must complete the following sections for each remote messaging server:

- Remote Messaging Server Properties—General information
- Remote Messaging Server Properties—Connection information

A remote server is configured from the Message Network Configuration page. Click New Server or doubleclick an existing server on the network Tree. The following image shows the Server Properties page for a remote server.



General section

Name

You should assign the remote messaging server the same name that was assigned to it by its local network administrator. This correspondence in naming sites 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
- (Meridian Mail Net Gateway) MMNG
- Meridian Mail
- other Nortel
- 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.

Site ID

Every remote site in your network database requires a Site ID. All site IDs must be unique. You need to coordinate with remote network administrators to ensure that this rule is observed before any site is implemented. Site ID is mandatory regardless of the protocol.

If your implementation of Enterprise Networking is an upgrade of an existing voice messaging system that used Enterprise Networking, maintain the Site ID numbers of the previous system.

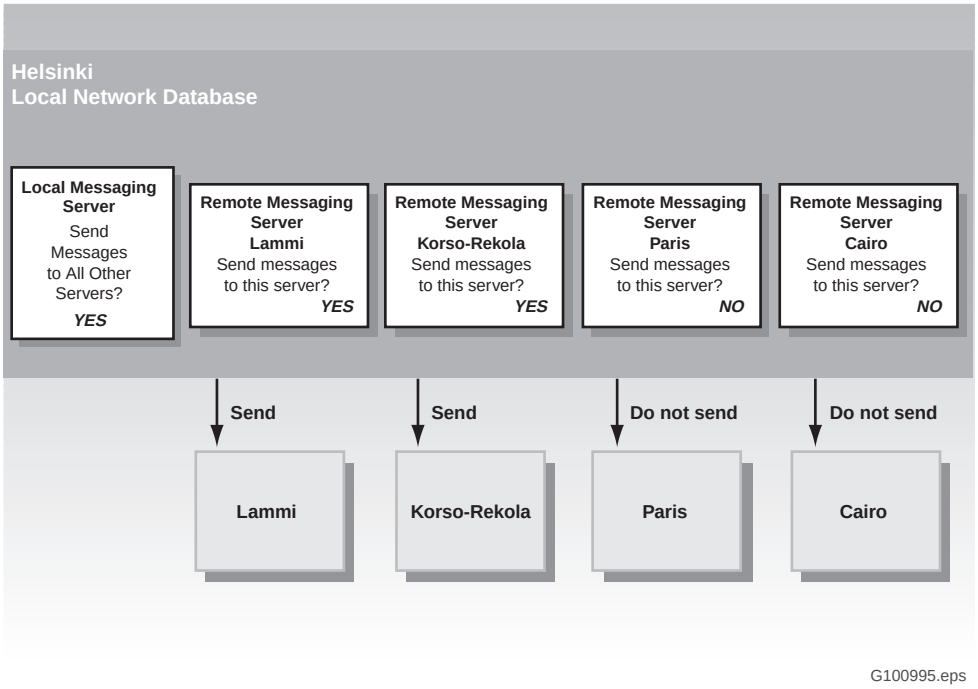
Send Messages to this Server

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 section.

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

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 remote sites. Messages are sent to Lammi and Korso-Rekola. Therefore, while the potential exists for sending messages to both remote sites, only two sites in the messaging network receive messages from Helsinki.



G100995.eps

Send Network Broadcast to this server and Receive Network Broadcast from this server

Both check boxes apply to network-wide broadcasts, and location-specific broadcasts from all locations associated with the remote site. This is particularly useful when sites that do not belong to your company or organization are included in the network tree.

Enterprise networking section

Send local user information to this Server (for Names Across the Network)

The Send local user information to this Server check box determines if the Names Across the Network feature is sent to this remote site.

Names Across the Network is an Enterprise and VPIM Networking feature that automatically adds temporary remote users to the local database and maintains them. You enable Names Across the Network for incoming and outgoing messages separately. A temporary remote user can be added when

- A user at a remote site addresses a message to a local user. The remote user information is taken from the header of the message that is received.

The setting to add remote users with Names Across the Network is on the Messaging Network Configuration page for your local server. This setting controls your local server. You must coordinate with the system administrator of each remote site with which you want to enable Names Across the Network. You can use Names Across the Network only with remote sites that have Enterprise or VPIM Networking installed.

The setting to add remote users with Names Across the Network is on the Messaging Network Configuration page for your local server. This setting controls your local server. You must coordinate with the system administrator of each remote site with which you want to enable Names Across the Network. You can use Names Across the Network only with remote sites that have Enterprise or VPIM Networking installed.

When you select Names Across the Network for incoming messages, you add temporary remote users from all sites in the messaging network. However, because outgoing messages must carry additional information with them, which results in longer transmission time, you can select Names Across the Network for outgoing messages for individual sites. For example, you might select the feature for outgoing messages to a site that does not incur long-distance toll charges, but clear the feature for a site that incurs these charges.

Example

As the local administrator of the Helsinki site, when you select Add Remote Users, temporary remote users will get created if both ends support Names Across the Network. You receive messages from all other sites that are configured to send the information. However, when you configure information about the remote servers in your local database, you clear the Send Local User Information to this Server option for the sites to which you do not want to send remote user information. Names Across the Network is also affected by the way the network administrator at a remote site configures the system.

Names Across the Network has the following limitations:

- Users at remote sites are added to your system as temporary remote users only when messages are received from them. Users at remote sites who do not send network messages are not added to your system, even if they are regularly name-dialed or have messages sent to them.
- Operational measurements are not collected for remote users.
- If the sender's site does not have mailbox numbers that match the dialing plan, the Call Sender and Name Dialing features are not available.
- While the nightly audit is in progress, temporary remote users cannot be added or updated.
- Only 18 characters of the remote voice user's text name are sent.

IF	THEN
the first and last names are 18 characters or less	the first and last names of the user are sent.
the initials and last name are 18 characters or less	the initials and last name of the user are sent.
the last name only is 18 characters or less	only the last name is sent.
the last name is longer than 18 characters	only the last name, truncated to 18 characters, is sent. Note: This does not apply to VPIM.

When the local site initiates an Enterprise Networking session to a remote site, the two sites negotiate whether spoken names are sent. This negotiation occurs as follows:

IF	THEN
the local site chooses to send spoken names and the remote site has selected the Add/Update Remote Users on this Server option	■ the local site includes the sender's text and spoken name with each message. ■ the remote site adds or updates the sender's remote user information.
the local site chooses not to send spoken names and/or the remote site has not selected the Add/Update Remote Users on this Server option	■ the local site does not include the spoken names for the senders. ■ the remote site does not add or update the sender's remote user information.

When a message is received from a user who already exists in the local database as a temporary remote user, the time stamp of the remote user is updated with the current date and time.

Send Message Text Info to this Server

This feature allows the subject portion of a message to be sent to a remote site. Since a subject cannot be added from the telset, it is only useful if there are desktop users.

SMTP/VPIM section

Server FQDN

If VPIM Networking is installed on your local site, the VPIM Networking Server FQDN box is enabled.

Note: VPIM cannot be installed separately from other protocols. When networking is installed, all protocols become available (but not NMS; it is packaged separately).

Connections section

Network protocol

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

If a remote site is not configured to 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 on the local system.

Connections section—Connection DNs

When CallPilot initiates a call to a remote site, it uses the networking connection DN that is specified for the remote site in your network database. You can define up to three DNs. DN1 is mandatory. DN2 and DN3 are optional.

At least one connection DN must be the networking system access number for the remote site, as defined on the Message Delivery Configuration page for the remote site. You should include the system access number of the remote site on the network representation.

The first Enterprise Networking connection DN is the Enterprise Networking SDN for the remote site, as defined in the SDN table of the remote site. If Enterprise Networking is sharing an SDN with another service, such as AMIS Networking, then the networking connection DN is the DN that accepts such network calls.

You must contact the administrator of the remote site for the connection DN. The connection DNs are entered in a format that is dialable from the local site.

The system always uses DN1 to call the remote site unless it encounters problems. If the system does encounter a problem, it attempts to contact the remote site using DN2, then DN3. In general, the DNs are ordered from least expensive to most expensive connections. For example, DN1 could be a private number and DN3 could be a public telephone number.

Connections section— Enterprise

Unique passwords are used between each pair of sites in an Enterprise messaging network. They are used to secure the messaging network and the integrity of the messages. Two passwords are used to verify that any two sites may communicate with each other:

- Initiating Password
- Responding Password

The passwords on your site must match the site you are calling or from which you are receiving messages.

Initiating Password and Responding Password

Enterprise Networking uses passwords to send messages securely. When a message is sent from one site to another, the two sites trade two passwords, an initiating password and a responding password. Both passwords must match before a message is sent. You establish passwords between pairs of sites. For this reason, you must contact the network administrator of each remote site in the messaging network and agree on the passwords that will be used.

Connections section—VPIM Security

Ensure that VPIM is selected in the Network Protocol box.

SSL port number

If encryption will be used, type the port number designated as the Secure Socket Layer port on the remote messaging server. The default is 465. When the SSL port is specified, and if the Connect to server with SSL for Outgoing SMTP Sessions option is enabled in Message Delivery Configuration, CallPilot attempts to establish an encrypted connection with this port when connecting to this remote server.

Server password

Type the SMTP authentication password that the remote server must send when the local CallPilot server requests SMTP authentication. The maximum length is 30 alphanumeric characters.

Failed attempts from this server

This box displays the number of failed SMTP authentication attempts that have occurred to date. If this value reaches the maximum number of failures defined on the local server (specified in the System Maximum box, below), CallPilot will disable incoming VPIM message transmissions from this remote server, if configured. After you resolve the cause of SMTP authentication failures from the remote server, click Reset Count to set the counter back to 0.

System Maximum

This box displays the maximum number of SMTP authentication failures that the local server will tolerate from any server.

Receive messages from this server

Choose Enabled from the list box to allow the local server to receive messages from this remote server.

Configuring a remote prime switch location

When you add a remote messaging server to the Message Network Configuration tree view, a corresponding prime switch location is added. A remote prime switch location must be configured. This process is almost identical to configuring the local prime switch location.

General section

Complete the General section no matter what dialing plan is used on your local site.

Name

Assign a unique name to each switch location. The name should correspond to the switch location to make the location easy to identify. The remote 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 switch location in this box.

Location ID

The 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 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, “Dallas, Mailbox 2346”.

If a spoken name is not recorded, local users hear a full mailbox address 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, "Mailbox 6444 2346".

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.

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 and addressing section

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

- ESN
- CDP
- (hybrid, which combines ESN and CDP)

Mailbox addressing follows dialing plan

When a mailbox follows the dialing plan:

- 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.

Mailbox prefixes

Mailbox prefixes are used by local users to address users at a remote site if mailboxes at the remote site do not follow the dialing plan. 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 cannot 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. 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 dialing prefix to reach users at this remote site. 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, without 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.

ESN information

If the remote prime switch location uses an ESN or hybrid dialing plan, complete the ESN section. The procedure for configuring the ESN information for a remote prime switch is identical to the procedure used for the local prime switch location.

Note: You must provide the ESN access code used at the remote site. Do not enter the access code used locally.

For a review of the ESN access codes, ESN location codes, and overlap, consult the ESN section on page 197.

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 section. 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 the CDP section on page 198.

VPIM section

If you are using desktop messaging and My CallPilot, VPIM Networking, or both, define the VPIM network shortcuts for this switch location. The VPIM network shortcut identifies the switch location to desktop messaging clients. It also facilitates the delivery of VPIM messages that are addressed to recipients at sites that do not use the VPIM protocol.

VPIM Network Shortcuts

The VPIM network shortcut identifies the switch location to desktop messaging clients. In the VPIM section, click Add. The VPIM Network Shortcut Detail page appears.

Prefix

Type the shortcut in the Prefix box. The maximum length is 30 digits (0–9). The recommended format is the same as the PSTN number (country code + area code + exchange portions).

Overlap

In the Overlap box, specify the number of digits that overlap with the mailbox number. Typically, a shortcut overlaps with the first digit of the mailbox number. The Range is 0 to the length of this shortcut. For more information on VPIM shortcuts refer to Chapter 7, “About VPIM Networking.”

Time Zone Settings section

Time zone

The time zone for the prime switch location is automatically the same as the time zone for the CallPilot server. It is configured in the Date/Time component of the Windows Control Panel.

Configuring a remote satellite switch location

Configuring a satellite switch location for a remote site is identical to configuring a remote prime switch location for a remote site.

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.

Where to configure a satellite switch location

To configure a satellite switch location, complete the General section of the Server Properties page. You must also complete the sections that correspond to the dialing plan used by the local site.

ESN

Complete the ESN section if you use an ESN or hybrid dialing plan.

CDP

Complete the CDP section if you use a CDP or hybrid dialing plan.

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.

chapter 12

Security and encryption

In this chapter

Networking and security 212
SMTP security 217
Encryption 230

Networking and security

In this section

Overview 212
Open AMIS Networking and security 212
VPIM Networking and security 213
Switch security and networking 216

Overview

It is important to maintain the integrity and security of your CallPilot system.

Every site in your messaging network should follow the recommended security precautions. In addition to these general security precautions, there are some precautions specific to a messaging network. These specific precautions are described in this section.

ATTENTION! This description is intended only as an overview. For more detailed information about switch security features and how they must be set, consult your switch documentation and/or a security specialist.

Open AMIS Networking and security

With AMIS Networking, local users can dial out to the public network. This means that the messaging network is susceptible to toll fraud. You must take precautions to ensure that the network is not exploited at your company's expense.

All AMIS Networking messages sent to sites that are not part of your private messaging network will appear on the telephone bill for your site.

Long-distance toll charge features

Several features minimize the likelihood of long-distance toll fraud from an AMIS Networking site:

- CallPilot feature
  - Restriction/Permission Lists (RPLs)
- switch features, such as:
  - Trunk Group Access Restrictions (TGARs)
  - Class of Service (CLS)
  - Network Class of Service (NCOS)

Assigning user access and Restriction/Permission Lists

If you allow local users to send messages to open sites, you must establish user access because long-distance toll charges may be incurred when messages are sent to open sites.

There are two basic levels of control:

- When you define message delivery parameters, you define general system-wide controls over networking messages.
- When you define different classes of users, you define the access level individual users have to networking.

Mailbox class settings

You control a user's access to networking, in part, by the mailbox class to which the user is assigned. The following options for each mailbox class are available:

- default message priority—standard or economy
- permission for exchange of messages with open sites
- Restriction/Permission List for open messages, if you allow users to send messages to open sites

You must set the options for each mailbox class.

If you allow local users to exchange messages with open sites, create any necessary Restriction/Permission Lists (RPL). An RPL defines any restrictions to access and also lists any exceptions to these restrictions. An RPL provides additional security and prevents unauthorized long-distance toll charges.

Example

Local users can send messages to open sites. However, you want to ensure that different classes of users can send messages only to specific sites. Users with a manager-level mailbox class can send messages to any site. Users with a summer student mailbox class can send messages to any open site that does not incur long-distance toll charges.

Usually, you will assign a pre-existing Restriction/Permission List. However, if no pre-existing list satisfies your requirements, you can create a new list.

See also

For further information consult the CallPilot Manager online Help.

VPIM Networking and security

There are special security considerations if VPIM Networking is used to send messages over the Internet.

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.

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. VPIM Networking connects sites with links created over the Internet. Basically, network connections are created over the public Internet rather than over private leased lines or public packet-switched networks.

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.

Firewalls

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.

It is not possible to give specific recommendations for setting up a firewall, since many configurations are possible. Note however, that it is strongly recommended that you use a router to create a sub-net for the CallPilot system to separate it from the larger data network.

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

Encryption

Encryption enables you to protect the integrity of messages sent over the Internet. It provides a way to send encoded messages from one site to another in a form that only the two sites can understand.

If you must transmit messages that contain information important to your business, encryption may be required. Information that may need to be secure includes:

- financial data
- proprietary information, such as product development information
- confidential personnel information

VPIM Networking and Meridian Mail Net Gateway

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.

VPIM Networking and Windows

Windows includes its own encryption features. If you want to use the Windows encryption feature with VPIM Networking, you must thoroughly test how this feature works.

Malicious attacks

Hackers use several types of attacks against sites that are connected to the Internet.

Some of the most common malicious attacks include:

- service attacks
- e-mail flooding
- spamming

Service attacks

Service attacks are intended to bring down a data network. A service attack is designed to keep a data network continuously occupied so that it cannot perform its usual tasks.

Ping attacks

One of the most common types of service attacks is the continuous use of the Packet Internet Groper (ping) utility.

The ping program is an echo utility that tests continuity and path delay. Pinging is used to determine if a remote site is reachable and is an invaluable tool for testing your system.

However, the process of pinging uses system resources. If continually pinged, the system is unable to provide other services. Although it is illegal to do so in many countries, hackers have created programs that ping a server continually until the system is brought down.

Security against ping attacks

Ping attacks can be deflected by using packet filters. A packet filter examines the TCP/IP header of each incoming message and rejects all those that are specified as not allowed or restricted. The list of rejected headers is maintained in a filter table. The ping protocol, which usually uses port 7, is usually allowed but restricted.

Setting up filter tables is complicated. The syntax and format used by each vendor's router is different.

Work with your data network administrator to set up the necessary defenses against service attacks.

Switch security and networking

The switch location is already set up and configured when you begin to implement a networking solution. Several switch security features have already been set. These must be considered when implementing a networking solution. Switch security must be tight enough that restricted activity is not allowed, but not so tight that networking messages that should be allowed are restricted.

Switch security features

The following switch security features may affect the exchange of networking messages:

- Restriction Permission Lists (RPLs)
- ACD agent restrictions
  - Trunk Group Access Restrictions (TGARs)
  - Class of Service (CLS)
  - Network Class of Service (NCOS)

These features offer multiple layers of defense against fraud and other system abuses. However, if these features are set without considering the needs of networking, they may also block legitimate messages from reaching their destinations.

ATTENTION! It is strongly recommended that you review the switch security settings with the switch technician before you begin to implement a networking solution. Compare the networking needs with the current security settings, and ensure that necessary changes are made.

SMTP security

In this section

Overview 217
Unauthenticated mode 219
Authenticated mode 220
Mixed authentication mode 221
SMTP authentication methods 222
Authentication failures 224
Enabling CallPilot SMTP authentication 227
Configuring unauthenticated access restrictions 227
Monitoring suspicious SMTP activity 227

Overview

CallPilot uses Simple Mail Transport Protocol (SMTP) to send:

- VPIM Networking messages between the local CallPilot server and remote CallPilot servers
- VPIM Networking messages between the local CallPilot server and remote messaging servers that are VPIM compliant
- messages from desktop messaging and My CallPilot users to the CallPilot server

In CallPilot, the component that implements SMTP is known as the Internet Mail Agent.

Simple Mail Transport Protocol authentication

CallPilot supports SMTP authentication, which is a hacker and toll fraud prevention method. CallPilot authenticates message transmission sessions from the following:

- desktop messaging and My CallPilot users
- voice messaging servers that have been defined as remote sites in the CallPilot network database

Two methods of authentication are supported:

- Challenge and Response authentication, using the CRAM-MD5 algorithm
- User ID and Password authentication

For more information about the authentication methods, see SMTP authentication methods on page 222.

This guide focuses on SMTP authentication and messaging activity between remote messaging servers and CallPilot. For more information about SMTP, desktop messaging, and My CallPilot activity, refer to the CallPilot online Help.

Modes of authentication

You can configure SMTP authentication in one of the following modes on CallPilot:

- unauthenticated mode

  CallPilot does not request authentication from a sender. Therefore, message senders are never authenticated.

  Note: CallPilot, however, can limit the addressing capabilities of the sender by enforcing the unauthenticated access restrictions for users and servers, if they are configured.

- authenticated mode

  CallPilot always requests authentication. Successful authentication must occur before the message can be transmitted.

  You enable authentication by choosing one or both of the following authentication methods:

  - Challenge and Response
  - User ID and Password

- mixed authentication mode

  Authentication is optional. It is performed only if it is supported at both ends of the connection. If authentication is not being performed, CallPilot may limit the addressing capabilities of the sender by enforcing the unauthenticated access restrictions for users and servers, if they are configured.

  If authentication is being used, and it fails, the session is disconnected.

  You enable mixed authentication by choosing both the unauthenticated mode, and one or both of the following authentication methods:

  - Challenge and Response
  - User ID and Password

ATTENTION

When defining the authentication settings, remember that the settings also affect the addressing capabilities of desktop messaging and My CallPilot users who want to compose messages.

Monitoring suspicious SMTP activity

You can use one of the following methods to monitor suspicious SMTP and VPIM Networking activity:

- *Automatic monitoring:* review SMTP-related events in the Windows event log
- *Manual monitoring:* enable monitoring of activity from specific origins on the Security Administration page in CallPilot Manager

Encryption

Optionally, you can use encryption to secure all message traffic. Encryption prevents:

- password transmission in the clear
- eavesdroppers from gaining access to the contents of the message (thereby guaranteeing user privacy)

CallPilot networking, desktop messaging, and My CallPilot use encryption. Encryption is enabled and configured independently from SMTP authentication configuration.

For more information about encryption, see the section Encryption on page 230

Unauthenticated mode

In unauthenticated mode, CallPilot does not request authentication from a sender. The Internet Mail Agent (SMTP) transports message without authentication:

- from a remote voice messaging server to the CallPilot server
- from a desktop messaging or My CallPilot user to the CallPilot server

How to enable unauthenticated mode

The unauthenticated mode is enabled by default when you install or upgrade your CallPilot server.

When to use the unauthenticated mode

Use the unauthenticated mode if:

- you are not experiencing problems with inappropriate access
- you do not want to use SMTP authentication in your network
- the desktop messaging or My CallPilot clients used in your organization do not support SMTP authentication
- your messaging network contains:
  - messaging servers that do not support SMTP authentication
  - VPIM-compliant sites that are not defined in CallPilot's network database (open VPIM sites)

Note: Open VPIM sites can use only the unauthenticated mode when connecting to CallPilot.

Preventing denial-of-service attacks and junk e-mail in unauthenticated mode

To prevent denial-of-service attacks and junk e-mail proliferation, Nortel Networks recommends that you restrict the following from remote messaging servers that are not authenticated:

- incoming messages that are addressed to shared distribution lists (SDLs)
- incoming location and network broadcast messages

  Note: You can block incoming network broadcasts from a specific network site or all sites in the network database. This capability is in addition to the SMTP authentication feature, and is discussed in CallPilot server capabilities for broadcast messages on page 100.
- the number of recipients on incoming messages

  This prevents hackers from copying the contents of a large address book into the recipient list. The limit applies to all recipients within the message, including recipients in nested messages.

  CallPilot enforces the limit separately on each of the TO, CC, and Blind CC lists. For example, if the limit is defined as 100, the sender can enter 100 addresses in each of these recipient lists.

  If any recipient list exceeds the recipient limit, CallPilot rejects the entire message.

If CallPilot rejects a message as a result of any of these restrictions, the sender receives a non-delivery notification (NDN).

Preventing toll fraud

ATTENTION

To prevent toll fraud by desktop messaging and My CallPilot users who are not authenticated, Nortel Networks recommends that you restrict user addressing capabilities and the number of recipients on outgoing messages. These restrictions are enforced by:

- unauthenticated desktop user restrictions on the Unauthenticated Access Restrictions page in CallPilot Manager
- the desktop restriction/permission list (RPL)
- mailbox class

For more information about these items, refer to the CallPilot Manager online Help.

Authenticated mode

Authentication verifies the authenticity of the sender, which can be a desktop messaging user, My CallPilot user, or a remote messaging server.

In authenticated mode, CallPilot always requests authentication from the sender. Successful authentication must occur before the message is transmitted and received by the CallPilot server.

SMTP authentication can also be performed on outgoing sessions to remote servers. The receiving system advertises the methods it supports, and CallPilot responds accordingly. If authentication fails, the CallPilot SMTP server attempts to send the message without authentication. If the receiving system rejects any SMTP commands, the connection is dropped, and a non-delivery notification is generated.

How to enable the authenticated mode

To enable authenticated mode, you choose one or both of the following authentication methods in CallPilot Manager:

- Challenge and Response
- User ID and Password

For more information about the authentication methods, see page 222.

When to use the authenticated mode

SMTP authentication provides maximum security in which spoofing is virtually impossible. You can only use the authenticated mode when all messaging servers in the network, desktop messaging clients, and My CallPilot clients support authentication.

SMTP authentication is supported in closed networks only. SMTP authentication cannot be performed between CallPilot and open VPIM sites (that is remote messaging servers that are *not* defined in the CallPilot network database). If the message transmission session cannot be authenticated, the messages themselves cannot be transmitted.

Note: You must use the mixed authentication mode if:

- your voice messaging network contains messaging systems, desktop messaging clients, and My CallPilot clients that do not support SMTP authentication

- your users want to receive messages from open VPIM sites

For more details, see Mixed authentication mode on page 221.

Denial-of-service attacks, junk e-mail, and toll fraud

The authenticated mode prevents denial-of-service attacks, junk e-mail, and toll fraud. Therefore, it is not necessary to enforce the restrictions that are described in:

- Preventing denial-of-service attacks and junk e-mail in unauthenticated mode on page 219
- Preventing toll fraud on page 220

Mixed authentication mode

In mixed authentication mode, SMTP authentication is optional. CallPilot requests authentication, but does not require it for a successful connection.

Authentication is performed only if it is supported at both ends of the connection. If authentication is not supported, CallPilot accepts the message without authentication, but limits the addressing capabilities of the sender.

How to enable mixed authentication

To enable mixed authentication, you choose both of the following in CallPilot Manager:

- unauthenticated mode
- one or both of the following authentication methods:
  - Challenge and Response
  - User ID and Password

By default, unauthenticated mode and Challenge and Response are both enabled.

When to use mixed authentication

Use mixed authentication if your messaging network contains any of the following:

- VPIM-compliant sites that are not defined in CallPilot's network database
- messaging servers that support SMTP authentication
- messaging servers that do not support SMTP authentication
- desktop messaging or My CallPilot clients that support authentication
- desktop messaging or My CallPilot clients that *do not* support authentication

CallPilot accepts messages from both authenticated and unauthenticated senders, but restricts the capabilities of senders that are not authenticated.

How mixed authentication affects users

In mixed authentication mode, message receipts and hence, user addressing capabilities are affected as follows:

When the server or user is	incoming messages
unauthenticated	■ from remote servers can be blocked as described in Preventing denial-of-service attacks and junk e-mail in unauthenticated mode on page 219 ■ from desktop messaging or My CallPilot users can be restricted as described in Preventing toll fraud on page 220
authenticated	do not have to be blocked. The restrictions for users and remote servers *are not* enforced. **Note:** Users are still restricted to the capabilities allowed in their mailbox classes.

When you *should not* use mixed authentication

If you are concerned about security, Nortel Networks recommends that you use the authenticated mode only.

SMTP authentication methods

CallPilot supports the following SMTP authentication methods:

- Challenge and Response
- User ID and Password

The method used to perform SMTP authentication on a remote server, desktop messaging client, or My CallPilot client depends on what is supported by both the sending and receiving systems. If both authentication methods are supported, the sending system chooses the authentication method.

Challenge and Response authentication is the preferred method on CallPilot because it provides authentication with inherent encryption and is, therefore, always secure.

ATTENTION

Nortel Networks recommends that if you want to use the User ID and Password authentication method, you also use Secure Socket Layer (SSL) to encrypt the connection. SSL encryption prevents password transmission in the clear and ensures content privacy while the message is in transit.

For more information about encryption, see the section Encryption on page 230

Note: Authentication of remote servers can occur only if the remote server is defined in the CallPilot network database. Open VPIM sites cannot be authenticated.

Challenge and Response authentication process

The Challenge and Response authentication method uses the CRAM-MD5 algorithm. The following steps describe the Challenge and Response authentication process for an incoming message session:

1. The sending system (remote server, desktop messaging user, or My CallPilot user) connects to the CallPilot Internet Mail Agent (SMTP server).
2. CallPilot advertises that it supports Challenge and Response authentication.
3. One of the following occurs:

IF the sending system	THEN
supports Challenge and Response authentication	the sending system requests authentication.
does not support Challenge and Response authentication	authentication fails and the message transmission is handled as described in Authentication failures on page 224.

4. CallPilot generates and passes a string containing a time stamp and other text.
5. The sending system generates and sends a response that contains the string, user ID, and password.
   - For a desktop messaging or My CallPilot user, the user ID is the user's PSTN number (SMTP/VPIM shortcut and mailbox number). The password is the mailbox password.
   - For a remote messaging server, the user ID is the remote server's fully qualified domain name (FQDN). The password is the server's SMTP/VPIM password.
6. CallPilot generates a string that contains the user ID and password.
   - For a desktop messaging or My CallPilot user, the mailbox and user password are obtained from the user database.
   - For a remote messaging server, the remote server's FQDN and SMTP/VPIM password are obtained from the network database.
7. CallPilot compares the two strings.

IF the strings	THEN
match	the sending system is authenticated and message transmission continues.
do not match	authentication fails and the message transmission is handled as described in Authentication failures on page 224.

User ID and Password authentication process

The following steps describe the User ID and Password authentication process for an incoming message session:

1. The sending system (remote server, desktop messaging user, or My CallPilot user) connects to the CallPilot Internet Mail Agent (SMTP server) through either the SMTP port or the SSL port.

   Notes:

   - By default, 465 is defined as the SSL port that listens for encrypted sessions. Port 25 listens for unencrypted sessions.
   - The CallPilot SMTP server does not require SSL on incoming transmissions, but does support it. On outgoing sessions, SSL must be enabled if User ID and Password authentication is being used.
2. CallPilot advertises that it supports user ID and password authentication.

3. One of the following occurs:

IF the sending system	THEN
supports User ID and Password authentication	the sending system requests authentication.
does not support User ID and Password authentication	authentication fails and the message transmission is handled as described in Authentication failures on page 224.

4. CallPilot requests the user ID.
5. The sending system responds with the user ID:
   - For a desktop messaging or My CallPilot user, the user ID is the user's PSTN number (SMTP/VPIM shortcut and mailbox number).
   - For a remote messaging server, the user ID is the remote server's FQDN.
6. CallPilot requests the password.
7. The sending system responds with the password.
8. CallPilot verifies the user ID and password:
   - For a desktop messaging or My CallPilot user, the mailbox and user password are obtained from the user database.
   - For a remote messaging server, the remote server's FQDN and SMTP/VPIM password are obtained from the network database.

IF the user ID and password	THEN
match	the sending system is authenticated and message transmission continues.
do not match	message transmission is handled as described in Authentication failures on page 224.

Authentication failures

This section describes:

- situations in which SMTP authentications can fail
- what happens when SMTP authentication failures occur

You can specify the maximum number of authentication failures that can occur from remote messaging servers, desktop messaging users, or My CallPilot users.

You can also specify what CallPilot should do when the number of failed authentication attempts exceeds the maximum limit that you specify.

When authentication can fail

SMTP authentication can fail in the following situations:

- Passwords are not configured correctly in CallPilot Manager for the local CallPilot server and the remote messaging server.

- The user's user ID, password, or both are not configured correctly in the desktop messaging or My CallPilot client.
- The requested authentication method is not supported at both ends of the connection.

  This can occur when:
  - a desktop messaging or My CallPilot user is using a desktop client or web browser that does not support SMTP authentication at all
  - the desktop messaging or My CallPilot user is using a client or web browser that does not support the SMTP authentication method requested by CallPilot
  - the remote messaging server does not support SMTP authentication
  - the remote messaging server does not support the SMTP authentication method requested by CallPilot

What happens when authentication fails

CallPilot cannot receive messages when authenticated mode only is used and authentication fails. If mixed authentication is being used on CallPilot, a message transmission can still occur *without* authentication.

Incoming messages from desktop messaging or My CallPilot users

For incoming messages from desktop messaging or My CallPilot users, the message must leave the user's outbox and be received by the CallPilot server before CallPilot can deliver the message to the destination.

IF CallPilot is configured to use	THEN
authenticated mode only, and authentication fails for an incoming message from a desktop messaging or My CallPilot user	the message remains in the user's outbox in the desktop messaging client or web browser. An NDN is not sent to the user because the user can immediately determine that the message was not sent.
mixed authentication, and authentication fails for an incoming session from a desktop messaging or My CallPilot user	the message remains in the user's outbox in the desktop messaging client or web browser. An NDN is not sent to the user because the user can immediately determine that the message was not sent.
mixed authentication, and authentication is not attempted for an incoming message from a desktop messaging or My CallPilot user	CallPilot accepts the message *without* authentication. The unauthenticated desktop user restrictions are enforced. See Preventing toll fraud on page 220.

Incoming messages from remote servers

IF CallPilot is configured to use	THEN
authenticated mode only, and authentication fails for an incoming VPIM Networking message transmission	CallPilot drops the connection. The sender may receive an NDN if the remote server supports NDNs.
mixed authentication, and authentication fails for an incoming VPIM Networking session	CallPilot drops the connection. The sender may receive an NDN if the remote server supports NDNs.
mixed authentication, and authentication is not attempted for an incoming VPIM Networking message transmission	CallPilot accepts the message *without* authentication. The unauthenticated server restrictions are enforced. See Preventing denial-of-service attacks and junk e-mail in unauthenticated mode on page 219.

Outgoing messages to remote messaging servers

When an initiating SMTP password is defined on your CallPilot server, SMTP authentication is performed on outgoing sessions to remote servers. If authentication is attempted and fails, CallPilot still attempts to send the message. If the advertised authentication method is not supported, CallPilot attempts to send the message without authentication.

If the outgoing message was initiated by a desktop messaging or My CallPilot user, the unauthenticated desktop user restrictions are enforced. See Preventing toll fraud on page 220.

If the remote server rejects any SMTP commands, and the message cannot be sent after several attempts, CallPilot sends an NDN to the sender and logs an event.

What happens when there are too many failed authentication attempts?

You can specify the maximum number of failed authentication attempts that can occur from remote messaging servers, desktop messaging users, or My CallPilot users, and what action to perform when the limit is exceeded. You can choose to:

- report the event in the event log and generate an alarm
- disable the remote messaging server in your network database and report the event

  When the remote server is disabled, the following results occur:
  - CallPilot rejects all incoming VPIM messages from that server (both authenticated and unauthenticated). This prevents hackers from trying all the possible password combinations and eventually obtaining the correct password.
  - If unsuccessful authentication attempts continue, CallPilot reports an event for each time the maximum number of failed attempts is exceeded.
- disable the user's mailbox and report the event

  When the user's mailbox is disabled, CallPilot rejects the following from the user:
  - all mailbox logon attempts (including logon attempts from a phoneset)
  - all incoming VPIM messages from a desktop messaging or My CallPilot client that is configured as belonging to the user

  This prevents hackers from trying all the possible password combinations and eventually obtaining the correct password.

  CallPilot also reports an event for each time the maximum number of failed attempts is exceeded.

To allow CallPilot to receive incoming messages again, you must re-enable the remote server in your network database or the user's mailbox in user administration.

Enabling CallPilot SMTP authentication

To enable SMTP authentication between CallPilot and remote messaging servers, you must configure specific options on both the local server and on each remote server in the CallPilot network database that is using VPIM Networking. The procedures for the tasks that you must complete are provided in the CallPilot Manager online Help.

To enable SMTP authentication between CallPilot, desktop messaging users, and My CallPilot users, you must also configure the desktop messaging and My CallPilot clients. For instructions on configuring the desktop messaging and My CallPilot clients, refer to the *Desktop Messaging and My CallPilot Administration Guide* (555-7101-503).

Configuring unauthenticated access restrictions

If unauthenticated mode is used, Nortel Networks recommends that you also enable unauthenticated access restrictions for servers and desktop users.

You should perform the following additional tasks, as required:

- Configure the desktop restriction/permission lists (RPLs).
- Assign RPLs to a mailbox class.
- Assign message delivery options to mailbox class members.

For instructions, refer to the CallPilot Manager online Help.

Monitoring suspicious SMTP activity

You can use one of the following methods to monitor suspicious SMTP and VPIM Networking activity:

- review SMTP-related events in the Windows NT event log (automatic monitoring)

  If you choose to use the Windows NT event log as your monitoring method, no action is required from you to initiate SMTP/VPIM monitoring.
- enable monitoring of activity from specific origins on the Security Administration page in CallPilot Manager (manual monitoring)

Automatic monitoring

Automatic monitoring alerts you to suspicious SMTP activity, blocks access to the system, and provides sufficient information for further investigation. No configuration is required for automatic SMTP/VPIM monitoring.

How it works

If CallPilot detects repeated unsuccessful authentication attempts (for example, an incorrect password is presented), the following events occur:

- for a local user: after the specified number of unsuccessful attempts, an event is logged in the Windows NT event log and, if configured, the user's mailbox is disabled.

  If the mailbox is disabled, the user cannot log on either from a phoneset or by using a desktop messaging or My CallPilot client. Messages are no longer accepted via SMTP from that user, regardless of whether the user is authenticated or not.
- for a remote server: after the specified number of unsuccessful attempts, an event is logged in the Windows NT event log and, if configured, message reception from the remote server is disabled.

  If the remote server is disabled, messages from the remote server are no longer accepted.

Note: If the sender presents itself as a local mailbox or a remote server that does not actually exist, the system treats it the same way as when the mailbox or remote server does exist. This prevents the hacker from learning that the mailbox or server are not defined on the local system.

When the mailbox or server becomes disabled, an event is logged in the Windows NT event log. The event includes the following information:

- the User ID used in the authentication attempt

  The user ID can be either a user's public switch telephone (PSTN) number (SMTP/VPIM shortcut and mailbox number) or a remote server's authenticating FQDN.
- the hostname and IP address from which the last authentication failure occurred

You can use this information to investigate the source of the suspicious activity, or enable manual hacker monitoring.

Manual monitoring

You can manually monitor activity based on the following information:

- the authenticating user ID
- the IP address of the remote messaging server, desktop messaging client, or My CallPilot client that is attempting to connect to the CallPilot server
- the FQDN of the remote messaging server, desktop messaging client, or My CallPilot client that is attempting to connect to the CallPilot server

You can define up to 100 activities to monitor. When you enable monitoring, the system provides you with a detailed list of activities received from the user ID, IP address, or FQDN. Activities that appear in the list include:

- all connections with successful authentication attempts
- all connections with unsuccessful authentication attempts
- all unauthenticated connections (that is, where authentication was not attempted)

In addition to the activities list, an alarm message is deposited in the alarm mailbox, if the alarm mailbox is configured and these events have not been throttled. For more information, refer to the following in the *CallPilot Administrator's Guide* (NTP 555-7101-301):

- "Configuring messaging service defaults"
- "Throttling and customizing events"

When you have accumulated enough data about the hacker attack, you can disable monitoring of the offending source to avoid excessive logging. You can disable monitoring by using one of the following methods:

- Click Delete to remove the monitoring activity from the list.

- Click Disable to disable the monitoring activity.
  Note: This retains the activity in the list so that you can enable it again, if required.

Using wildcards

Wildcards are not supported when creating activity specifications.

Encryption

In this section

CallPilot encryption description 230
How CallPilot encryption works 231
Implementing encryption on CallPilot 233

CallPilot encryption description

CallPilot supports Secure Socket Layer (SSL) encryption to encrypt message transmissions between CallPilot and:

- desktop and web messaging clients
- another messaging server

Privacy guarantee

When you use SSL to encrypt message traffic between messaging servers, users are provided with privacy over the network.

Total privacy is obtained only when:

- the message originates from a phoneset, or SSL is used between the desktop or web messaging client and the CallPilot server
- SSL is used end-to-end between messaging servers
- the SSL transaction is successful

When to use encryption

Encryption is optional. However, Nortel Networks strongly recommends that you establish a secure (encrypted) session if you use the User ID and Password authentication method. User ID and password transmission in the clear is strongly discouraged.

Encryption prevents:

- password transmission in the clear
- eavesdroppers from gaining access to the contents of the message (thereby guaranteeing user privacy)

Considerations for implementing encryption

To determine whether you need to implement encryption in your CallPilot network, consider the following questions:

- Is encryption needed for secure desktop or web messaging logon?
- Is encryption required between messaging servers?

- Does your network infrastructure support secure message transmission from end to end?

  If messages cross a firewall or pass through an intermediate mail relay, encryption may not be provided end-to-end.
- Do you need to upgrade any systems?

TCP/IP traffic encryption for SSL requires significant CPU resources. The impact of using SSL depends on:

- total network traffic (desktop and VPIM)
- percentage of traffic that is using SSL

Secure transmission of a message to a remote CallPilot system is pointless if the message is also addressed to another system that does not support SSL. To do so wastes CPU bandwidth.

How CallPilot encryption works

The CallPilot SMTP server monitors port 25 for non-encrypted SMTP sessions. The CallPilot SMTP server also monitors (and connects to) port 465 for encrypted sessions. Encryption is provided by enabling Secure Socket Layer (SSL), which is also known as Transport Layer Security (TLS).

SSL sessions can be established only when SSL is supported at both ends of the connection.

SSL port monitoring

When SSL is enabled, the CallPilot server listens on port 465 for SSL handshake protocol commands. If the remote host sends a request for a connection to this port but does not provide the SSL handshake commands, the session cannot be established.

Similarly, if SSL is required, the CallPilot SMTP server attempts to connect to the SSL port on a remote messaging server. The default SSL port is 465.

SSL with User ID and Password authentication

The following table describes how SSL and the User ID and Password authentication method work together to guarantee user privacy over the network:

IF	THEN
SSL is enabled on the local server	message transmission sessions are encrypted. ■ For outgoing sessions, the CallPilot SMTP server attempts to connect to the SSL port on the remote messaging server. If the connection is successful, the session is encrypted to prevent password transmission in the clear. ■ For incoming sessions, the CallPilot SMTP server listens for non-encrypted connections on port 25 and encrypted connections on port 465 from remote SMTP hosts. If the connection on port 465 is successful, the session is encrypted to prevent password transmission in the clear.

IF	THEN
SSL is not enabled on the local server	message transmission sessions are not encrypted. ■ For outgoing sessions, the CallPilot SMTP server establishes the connection with the remote messaging server, but does not try to authenticate. The session continues without authentication to prevent password transmission in the clear. If the remote server requires authentication, then message transmission will not occur.
SSL is not enabled on the local server (continued)	■ For incoming sessions, the CallPilot SMTP server listens for connections from remote SMTP hosts on port 25 only.
the SSL connection cannot be established on an incoming connection (encryption fails)	the CallPilot SMTP server drops the connection. Message transmission does not occur.
the SSL connection cannot be established on an outgoing connection (encryption fails)	the CallPilot SMTP server drops the connection. CallPilot sends a non-delivery notification (NDN) to the message originator.

CallPilot encryption and Meridian Mail Net Gateway

Meridian Mail Net Gateway encryption (using Entrust) is not supported by CallPilot. Therefore, message transmissions between CallPilot and a Meridian Mail Net Gateway system cannot be encrypted.

CallPilot encryption and VPIM-compliant systems

The SMTP connection is encrypted if:

- SSL is enabled at both ends
- encryption certificates are accepted by each system

Intermediate mail relays and application proxy servers must participate in the establishment of secure sessions.

Encryption, authentication, mail relays, and firewalls

SSL encryption (and authentication) works best when messages are transferred point-to-point (for example, within a firewall).

When messages are not transmitted point-to-point, SSL sessions may still be initiated and authentication may still be performed if the firewalls are configured appropriately. It may also be possible to initiate SSL sessions between intermediary mail relays and proxies if those systems support SSL and are configured appropriately. However, end-to-end authentication may not be possible.

CallPilot encryption and certificates

SSL implementation requires a certificate on the CallPilot server. The CallPilot SMTP server uses the certificate that is provided for Internet Message Access Protocol (IMAP) and Lightweight Directory Access Protocol (LDAP). No specific manual interventions are required by you to create a certificate for SMTP.

Notes:

- Some third-party VPIM-compliant messaging systems may or may not accept the CallPilot certificate. Therefore, it may be necessary to use third-party certificates. The availability of compatible encryption algorithms can limit the use of SSL between some systems.
- You may need to use a certificate import feature to import certificates created from known certificate authorities, such as Verisign.

The CallPilot SMTP server accepts *all* certificates when establishing an SSL session. That is, CallPilot does not verify the digital signature. Therefore, establishing the secure session does not guarantee that CallPilot is actually sending the message to a specific destination.

For example, a tampered router in the network can redirect messages to a server that is spoofing a known site. CallPilot cannot verify that the certificate presented by the remote site is legitimate, and sends the encrypted message to the rogue server, which can decrypt the message with its master keys.

Implementing encryption on CallPilot

Encryption is enabled and configured independently from SMTP authentication configuration. (For information about SMTP authentication, see Enabling CallPilot SMTP authentication on page 227).

SSL configuration consists of the following tasks:

1. On the local server:
    - Enable SSL for incoming sessions from desktop or web messaging clients and remote messaging systems.
    - Enable SSL for outgoing message transmission sessions to remote messaging systems.
2. For each remote server defined in the CallPilot network database, specify the port that the CallPilot server connects to establish an SSL session.

For specific instructions on how to configure the encryption options on the CallPilot server for both the local server and each remote server that is defined in the CallPilot network database refer to the CallPilot online Help.

For instructions on how to configure the encryption options in desktop or web messaging clients, refer to the *Desktop Messaging and My CallPilot Installation Guide* (555-7101-505).

ATTENTION

Ensure that SSL is available on all systems, including intermediate systems such as gateways, mail relays, and so on. For information about implementing encryption on network devices, refer to the device manufacturer's documentation.

appendix A

Implementation and planning tools

In this chapter

Overview 236

Section A: Implementation checklists 238

AMIS Networking Implementation Checklist: NWP-035 239

Integrated AMIS Networking Implementation Checklist: NWP-032 241

Enterprise Networking Implementation Checklist: NWP-031 243

VPIM Networking Implementation Checklist: NWP-029 245

Open VPIM Implementation Checklist: NWP-036 247

Section B: Configuration worksheets 248

CallPilot Networking—CDP Steering Codes: NWP-027 249

CallPilot Networking—ESN Location Codes: NWP-037 250

CallPilot Networking—Local Server Maintenance: NWP-024 251

CallPilot Networking—Remote Server Maintenance: NWP-025 252

CallPilot Networking—Switch Location Maintenance: NWP-026 254

CallPilot Networking—Message Delivery Configuration: NWP-028 256

CallPilot Networking—Open VPIM Shortcuts: NWP-038 259

Overview

This chapter provides checklists and worksheets that you can use while setting up your messaging network.

Implementation checklists

To help you track your progress while implementing one or more networking solutions, you can use the following implementation checklists:

Checklist	For an example, see
AMIS Networking Implementation Checklist (NWP-035)	page 239.
Integrated AMIS Networking Implementation Checklist (NWP-032)	page 241.
Enterprise Networking Implementation Checklist (NWP-031)	page 243.
VPIM Networking Implementation Checklist (NWP-029)	page 245.
Open VPIM Implementation Checklist (NWP-036)	page 247.

For instructions on completing the tasks on these checklists, refer to the following:

- this guide
- CallPilot Manager online Help
- *CallPilot System Administrator's Guide* (555-7101-301)

Implementation process

The implementation process is easier if you follow this recommended order:

1. Network Message Service (NMS)
2. desktop or web messaging
   For more information, refer to the *Desktop Messaging and My CallPilot Installation Guide* (555-7101-505). For information about IMAP implementation, refer to the *Desktop Messaging and My CallPilot Administration Guide* (555-7101-503).
3. AMIS Networking, Integrated AMIS Networking, Enterprise Networking or VPIM Networking

Notes:

- Nortel Networks recommends that you implement and test all NMS sites in the messaging network before you implement any other networking solution.
- Nortel Networks also recommends that you verify the accuracy of information for your site before you release it to remote network administrators.

Configuration worksheets

To help you plan the configuration of your messaging network, you can use the following configuration worksheets:

Worksheet	For an example, see
Messaging Network Configuration worksheets	
CallPilot Networking—CDP Steering Codes (NWP-027)	page 249.
CallPilot Networking—ESN Location Codes (NWP-037)	page 250.
CallPilot Network Information—Local Server Maintenance (NWP-024)	page 251.
CallPilot Network Information—Remote Server Maintenance (NWP-025)	page 252.
CallPilot Network Information—Switch Location Maintenance (NWP-026)	page 254.
Messaging Delivery Configuration worksheets	
CallPilot Networking—Message Delivery Configuration (NWP-028)	page 256.
CallPilot Networking—Open VPIM Shortcuts (NWP-038)	page 259.

The configuration worksheets:

- provide a hard copy record of your network
- help you capture all the information for entry into CallPilot Manager

You can send the completed worksheets to other messaging network administrators to help them configure the network databases at their sites.

Section A: Implementation checklists

In this section

AMIS Networking Implementation Checklist: NWP-035 239
Integrated AMIS Networking Implementation Checklist: NWP-032 241
Enterprise Networking Implementation Checklist: NWP-031 243
VPIM Networking Implementation Checklist: NWP-029 245
Open VPIM Implementation Checklist: NWP-036 247

AMIS Networking Implementation Checklist: NWP-035

Step	Description	Done
Gather information for the network		
1	Obtain the system access number for each open AMIS site with which CallPilot exchanges messages.	❒
Configure the switch **Note:** For the switch requirements, refer to Chapter 10, Implementing & configuring CallPilot networking in this guide. For instructions on configuring the switch, refer to your switch documentation.		
2	Define the ACD queues.	❒
3	Dedicate ACD agents to networking, if required.	❒
4	Verify TGAR and NCOS on ACD agents.	❒
5	Define trunks (if additional trunks are required).	❒
6	Verify access to trunks (TGAR).	❒
Configure the network database in CallPilot **Note:** For instructions, refer to the CallPilot Manager online Help.		
7	Configure the local server. Use the information recorded on the “CallPilot Networking—Local Server Maintenance” worksheet (NWP-024).	❒
8	Configure the prime location for the local server. Use the information recorded on the “CallPilot Networking—Switch Location Maintenance” worksheet (NWP-026).	❒
9	Configure the Network Message Service (NMS) satellite locations for the local server, if required. Use the information recorded on the “CallPilot Networking—Switch Location Maintenance” worksheet (NWP-026).	❒
Configure the AMIS Networking message delivery options in CallPilot **Note:** For instructions, refer to the CallPilot Manager online Help.		
10	Enable AMIS Networking message transmissions to and from open AMIS sites.	❒
11	Define the open AMIS compose prefix.	❒
12	Configure the AMIS Networking batch delivery threshold.	❒
13	Define the allowed open AMIS delivery times.	❒
14	Configure the local server’s system access number.	❒
Configure the System and Messaging options in CallPilot **Note:** For instructions, refer to the CallPilot Manager online Help.		
15	Define the AMIS Networking DN in the Service Directory Number (SDN) table and, if required, dedicate channels. **Note:** For guidelines on channel allocation, refer to CallPilot Manager online Help.	❒
16	Define Dialing Information and Dialing Translations.	❒
Test the network for correct operation **Note:** For instructions, refer to the CallPilot Manager online Help.		
17	Test call routing access by testing each ACD agent.	❒
18	Compose and send a message from a mailbox on the local server to a mailbox on the local server.	❒
19	Send a message from a mailbox on the local server to a user at an open AMIS site, if possible.	❒

Create a backup of the network		
20	Back up CallPilot. **Note:** For instructions, refer to the CallPilot Manager online Help.	❒
21	Print CallPilot network information. **Note:** For instructions, refer to “Printing networking information” in the CallPilot Manager online Help.	❒
22	Back up the switch. **Note:** For instructions, refer to your switch documentation.	❒
23	Print switch network information. **Note:** For instructions, refer to your switch documentation.	❒

Integrated AMIS Networking Implementation Checklist: NWP-032

Step	Description	Done
Gather information for the network		
Note: For instructions, refer to Chapter 10, Implementing & configuring CallPilot networking in this guide. If necessary, consult with a switch technician.		
1	Gather ESN information from the switch.	❒
2	Gather CDP information from the switch.	❒
3	Draw a diagram of the existing network.	❒
4	Assign a unique site ID to each site in the network.	❒
5	Analyze the information and determine if changes are required to the dialing plan configuration on the switch.	❒
Configure the switch		
Note: For the switch requirements, refer to Chapter 10, Implementing & configuring CallPilot networking in this guide. For instructions on configuring the switch, refer to your switch documentation.		
6	Define the ACD queues.	❒
7	Dedicate ACD agents to networking, if required.	❒
8	Verify TGAR and NCOS on ACD agents.	❒
9	Define trunks (if additional trunks are required).	❒
10	Verify access to trunks (TGAR).	❒
11	Modify the dialing plan configuration on the switch if required.	❒
Configure the network sites and locations in CallPilot		
Note: For instructions, refer to the CallPilot Manager online Help.		
12	Configure the local server. Use the information recorded on the “CallPilot Networking—Local Server Maintenance” worksheet (NWP-024).	❒
13	Configure each remote server. Use the information recorded on the “CallPilot Networking—Remote Server Maintenance” worksheet (NWP-025).	❒
14	Configure the prime location for each of the local and remote servers. Use the information recorded on the “CallPilot Networking—Switch Location Maintenance” worksheet (NWP-026).	❒
15	Configure the Network Message Service (NMS) satellite locations for each of the local and remote servers, if required. Use the information recorded on the “CallPilot Networking—Switch Location Maintenance” worksheet (NWP-026).	❒
16	Convert existing sites to AMIS Networking if necessary.	❒
Configure the AMIS Networking message delivery options in CallPilot		
Note: For instructions, refer to the CallPilot Manager online Help.		
17	Enable AMIS Networking message transmissions to and from AMIS sites.	❒
18	Configure the AMIS Networking batch delivery threshold.	❒
19	Define the open AMIS compose prefix (if your network also contains open AMIS sites).	❒

20	Configure the local server's system access number.	❒
21	Define the open AMIS delivery times (if your network also contains open AMIS sites).	❒
22	Define the AMIS Networking economy delivery times.	❒
23	Define the AMIS Networking stale times.	❒
Configure the System and Messaging options in CallPilot **Note:** For instructions, refer to the CallPilot Manager online Help.		
24	Define the AMIS Networking DN in the SDN table and, if required, dedicate channels.	❒
25	Define Dialing Information and Dialing Translations.	❒
Test the network for correct operation **Note:** For instructions, refer to the CallPilot Manager online Help.		
26	Test call routing access by testing each ACD agent.	❒
27	Compose and send a message from a mailbox on the local server to a mailbox on the local server.	❒
28	Send a message from a mailbox on the local server to a user at an integrated AMIS (remote) site.	❒
Create a backup of the network		
29	Back up CallPilot. **Note:** For instructions, refer to the CallPilot Manager online Help.	❒
30	Print CallPilot network information. **Note:** For instructions, refer to "Printing networking information" in the CallPilot Manager online Help.	❒
31	Back up the switch. **Note:** For instructions, refer to your switch documentation.	❒
32	Print switch network information. **Note:** For instructions, refer to your switch documentation.	❒

Enterprise Networking Implementation Checklist: NWP-031

Step	Description	Done
Gather information for the network		
Note: For instructions, refer to Chapter 10, Implementing & configuring CallPilot networking in this guide. If necessary, consult with a switch technician.		
1	Gather ESN information from the switch.	❒
2	Gather CDP information from the switch.	❒
3	Draw a diagram of the existing network.	❒
4	Assign a unique site ID to each site in the network.	❒
5	Analyze the information and determine if changes are required to the dialing plan configuration on the switch.	❒
Configure the switch		
Note: For the switch requirements, refer to Chapter 10, Implementing & configuring CallPilot networking in this guide. For instructions on configuring the switch, refer to your switch documentation.		
6	Define the ACD queues.	❒
7	Dedicate ACD agents to networking (if required). This step is optional.	❒
8	Verify TGAR and NCOS on ACD agents.	❒
9	Define trunks (if additional trunks are required).	❒
10	Verify access to trunks (TGAR).	❒
11	Modify the dialing plan configuration on the switch if required.	❒
Configure the network sites and locations in CallPilot		
Note: For instructions, refer to the CallPilot Manager online Help.		
12	Configure the local server. Use the information recorded on the “CallPilot Networking—Local Server Maintenance” worksheet (NWP-024).	❒
13	Configure each remote server. Use the information recorded on the “CallPilot Networking—Remote Server Maintenance” worksheet (NWP-025).	❒
14	Configure the prime location for each of the local and remote servers. Use the information recorded on the “CallPilot Networking—Switch Location Maintenance” worksheet (NWP-026).	❒
15	Configure the Network Message Service (NMS) satellite locations for each of the local and remote servers (if required). Use the information recorded on the “CallPilot Networking—Switch Location Maintenance” worksheet (NWP-026).	❒
16	Convert existing sites to Enterprise Networking if necessary.	❒
Configure the Enterprise Networking message delivery options in CallPilot		
Note: For instructions, refer to the CallPilot Manager online Help.		
17	Enable Enterprise Networking message transmissions to and from Enterprise Networking sites.	❒
18	Configure the Enterprise Networking batch delivery threshold.	❒
19	Define the Enterprise Networking economy delivery times.	❒
20	Define the Enterprise Networking stale times.	❒

Configure the System options in CallPilot **Note:** For instructions, refer to the CallPilot Manager online Help.		
21	Define the Enterprise Networking DN in the Service Directory Number (SDN) table and, if required, dedicate channels.	❒
Test the network for correct operation **Note:** For instructions, refer to the CallPilot Manager online Help.		
22	Test call routing access by testing each ACD agent.	❒
23	Compose and send a message from a mailbox on the local server to a mailbox on the local server.	❒
24	Send a message from a mailbox on the local server to a mailbox user at a remote Enterprise Networking site.	❒
Create a backup of the network		
25	Back up CallPilot. **Note:** For instructions, refer to the CallPilot Manager online Help.	❒
26	Print CallPilot network information. **Note:** For instructions, refer to “Printing networking information” in the CallPilot Manager online Help.	❒
27	Back up the switch. **Note:** For instructions, refer to your switch documentation.	❒
28	Print switch network information. **Note:** For instructions, refer to your switch documentation.	❒

VPIM Networking Implementation Checklist: NWP-029

Step	Description	Done
Gather information for the network		
1	Obtain the following information for each remote server: — fully qualified domain name (FQDN) — VPIM prefix for each switch location at the remote site — SMTP password (if SMTP authentication is being used)	❒
2	Obtain the fully qualified domain name of the outgoing SMTP mail/proxy server.	❒
3	Draw a diagram of the existing network.	❒
4	Assign a unique site ID to each site in the network.	❒
5	Create a VPIM network shortcut for each switch location in the network (for both the local and remote servers).	❒
Configure the network sites and locations in CallPilot **Note:** For instructions, refer to the CallPilot Manager online Help.		
6	Configure the local server. Use the information recorded on the “CallPilot Networking—Local Server Maintenance” worksheet (NWP-024).	❒
7	Configure each remote server. Use the information recorded on the “CallPilot Networking—Remote Server Maintenance” worksheet (NWP-025).	❒
8	Configure the prime location for each of the local and remote servers. Use the information recorded on the “CallPilot Networking—Switch Location Maintenance” worksheet (NWP-026).	❒
9	Configure the Network Message Service (NMS) satellite locations for each of the local and remote servers (if required). Use the information recorded on the “CallPilot Networking—Switch Location Maintenance” worksheet (NWP-026).	❒
10	Convert existing sites to VPIM Networking if necessary.	❒
Configure the VPIM Networking message delivery options in CallPilot **Note:** For instructions, refer to the CallPilot Manager online Help.		
11	Enable incoming SMTP/VPIM message transmissions from desktop or web messaging users and open VPIM sites.	❒
12	Enable outgoing VPIM Networking message transmissions to open VPIM sites.	❒
13	Configure the Outgoing SMTP mail/proxy server’s FQDN.	❒
14	Define the open VPIM compose prefix (if required).	❒
15	Create an open VPIM shortcut for each open VPIM-compliant site with which CallPilot exchanges messages (if required).	❒
16	Configure the encryption settings (if required).	❒
17	Configure the SMTP authentication settings (if required).	❒
18	Configure the unauthenticated access restrictions for users and remote servers, if users or servers in your network will not be SMTP authenticated.	❒
Test the network for correct operation **Note:** For instructions, refer to the CallPilot Manager online Help.		
19	Perform a connectivity test by pinging the outgoing SMTP mail/proxy server or by establishing a telnet connection to the server.	❒
20	Compose and send a message from a mailbox on the local server to a mailbox on the local server.	❒

21	Send a message from a mailbox on the local server to a mailbox user at a remote VPIM Networking site.	❒
Create a backup of the network		
22	Back up CallPilot. **Note:** For instructions, refer to the CallPilot Manager online Help.	❒
23	Print CallPilot network information. **Note:** For instructions, refer to the CallPilot Manager online Help.	❒

Open VPIM Implementation Checklist: NWP-036

Step	Description	Done
Gather information for the network		
1	Obtain the following for each open VPIM-compliant site with which CallPilot exchanges messages: — fully qualified domain name — VPIM prefix	❒
2	Obtain the fully qualified domain name of the outgoing SMTP mail/proxy server.	❒
3	Draw a diagram of the existing network.	❒
4	Create an open VPIM shortcut for each open VPIM site.	❒
Configure the network database in CallPilot **Note:** For instructions, refer to the CallPilot Manager online Help.		
5	Configure the local server. Use the information recorded on the “CallPilot Networking—Local Server Maintenance” worksheet (NWP-024).	❒
6	Configure the prime location for the local server. Use the information recorded on the “CallPilot Networking—Switch Location Maintenance” worksheet (NWP-026).	❒
7	Configure the Network Message Service (NMS) satellite locations for the local server, if required. Use the information recorded on the “CallPilot Networking—Switch Location Maintenance” worksheet (NWP-026).	❒
Configure the VPIM Networking message delivery options in CallPilot **Note:** For instructions, refer to the CallPilot Manager online Help.		
8	Enable incoming SMTP/VPIM message transmissions from desktop or web messaging users and open VPIM sites.	❒
9	Enable outgoing VPIM Networking message transmissions to open VPIM sites.	❒
10	Configure the Outgoing SMTP mail/proxy server’s FQDN.	❒
11	Define the open VPIM compose prefix.	❒
12	Create an open VPIM shortcut for each open VPIM-compliant site with which CallPilot exchanges messages, if required.	❒
13	Configure the encryption settings, if required.	❒
14	Configure the SMTP authentication settings, if required.	❒
15	Define unauthenticated access restrictions for users and remote servers, if users or servers in your network will not be SMTP authenticated.	❒
Test the network for correct operation **Note:** For instructions, refer to the CallPilot Manager online Help.		
16	Perform a connectivity test by pinging the outgoing SMTP mail/proxy server or by establishing a telnet connection to the server.	❒
17	Compose and send a message from a mailbox on the local server to a mailbox on the local server.	❒
18	Send a message from a mailbox on the local server to a mailbox user at an open VPIM site, if possible.	❒
Create a backup of the network		
19	Back up CallPilot. **Note:** For instructions, refer to the CallPilot Manager online Help.	❒
20	Print CallPilot network information. **Note:** For instructions, refer to the CallPilot Manager online Help.	❒

Section B: Configuration worksheets

In this section

CallPilot Networking—CDP Steering Codes: NWP-027 249
CallPilot Networking—ESN Location Codes: NWP-037 250
CallPilot Networking—Local Server Maintenance: NWP-024 251
CallPilot Networking—Remote Server Maintenance: NWP-025 252
CallPilot Networking—Switch Location Maintenance: NWP-026 254
CallPilot Networking—Message Delivery Configuration: NWP-028 256
CallPilot Networking—Open VPIM Shortcuts: NWP-038 259

CallPilot Networking—CDP Steering Codes: NWP-027

Complete and attach this form to NWP-024, NWP-025 or NWP-026.

Location information

This location belongs to site name:	Site ID:
Location name:	Location ID:

CDP steering codes

(You can define up to 500 steering codes for this switch location. Complete and attach additional pages, as required.)

CDP steering code:	Overlap between CDP steering code and local extensions:	CDP steering code:	Overlap between CDP steering code and local extensions:

Completed by

Administrator:	Date:

CallPilot Networking—ESN Location Codes: NWP-037

Complete and attach this form to NWP-024, NWP-025 or NWP-026.

Location information

This location belongs to site name:	Site ID:
Location name:	Location ID:

ESN location codes

(You can define up to 30 location codes for this switch location.)

ESN location code:	Overlap between ESN location code and local extensions:	ESN location code:	Overlap between ESN location code and local extensions:
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Completed by

Administrator:	Date:

CallPilot Networking—Local Server Maintenance: NWP-024

Note: Complete and attach CallPilot Networking—Switch Location Maintenance (NWP-026) for the prime switch location.

Local server information

Site name:	Site ID:
Does site use Network Message Service? ❒ Yes ❒ No	
Send messages to all other servers: ❒ Yes ❒ No	Activate Names Across the Network (add or update remote users on this server): ❒ Yes ❒ No

Network broadcast ability

Send network broadcast messages to remote sites: ❒ Yes ❒ No	Receive network broadcast messages from remote sites: ❒ Yes ❒ No

Network broadcast addresses

Location broadcast number: Refer to the prime and satellite configuration for each location.
Network broadcast number: **Note:** Configure the network broadcast mailbox number in Messaging › Messaging Administration.

Enterprise Networking options

Receive message text information: ❒ Yes ❒ No

SMTP and VPIM Networking

Local server's FQDN:

Completed by

Administrator:	Date:

CallPilot Networking—Remote Server Maintenance: NWP-025

Note: Complete and attach CallPilot Networking—Switch Location Maintenance (NWP-026) for the prime switch location.

Remote server information

Site name:	Does site use Network Message Service? ❒ Yes ❒ No
Server type: ❒ CallPilot ❒ MMNG ❒ Meridian Mail ❒ Norstar ❒ Other	
Site ID:	Send messages to this server: ❒ Yes ❒ No

Network broadcast ability

Send network broadcast messages to this server: ❒ Yes ❒ No	Receive network broadcast messages from this server: ❒ Yes ❒ No

Enterprise Networking options

Send local user information to this server: ❒ Yes ❒ No	Send message text information to this server: ❒ Yes ❒ No

SMTP and VPIM Networking

Remote server's FQDN:

Connection information

Message transfer protocol: ❒ AMIS ❒ Enterprise ❒ VPIM	Connection DNs (Enterprise Networking only) **Note:** If the remote server is uses the AMIS protocol, complete the "Remote system access number" section below: DN 1: _____ DN 2: _____ DN 3: _____

Remote system access number (complete one only)

Complete this section only if the remote server uses the AMIS protocol.

Public network number: Country code: _____ Area/city code: _____ Number: _____	Private network number: _____

Enterprise Networking passwords

Initiating password: _____
Responding password: _____

VPIM Networking security

SSL port number (for encryption):		
Server password:		
Receive messages from this server:	❒ Yes	❒ No

Completed by

Administrator:	Date:

CallPilot Networking—Switch Location Maintenance: NWP-026

Complete this form for each switch location and attach it to NWP-024 or NWP-025.

Location Information

This location belongs to Site name:	Site ID:	This location is a ❒ Prime switch location ❒ Satellite switch location
Location name:	Do you want to record a spoken name for the location? ❒ Yes (Click Record or import.) ❒ No	
Location ID:		

Dialing plans

❒ ESN (Complete the ESN dialing plan information section below.)	❒ CDP (Complete the CDP dialing plan information section on the next page.)
Mailbox addressing follows the dialing plan: ❒ Yes ❒ No (Complete the Mailbox prefixes field.)	
Mailbox prefixes: _____ _____	Dialing prefix (for remote locations only): _____

ESN dialing plan information

(Complete this section if you have selected the ESN dialing plan.)

ESN access code:
ESN location codes and overlap: Complete and attach “ESN Location Codes” (NWP-037).

CDP dialing plan information

(Complete this section if you have selected the CDP dialing plan.)

CDP steering codes and overlap: Complete and attach “CDP Steering Codes” (NWP-027).

VPIM network shortcuts

(Complete this section to allow phoneset users to send VPIM Networking messages. You can create up to 30 VPIM network shortcuts for this location.)

VPIM prefix:	Overlap between VPIM prefix and local extensions:	VPIM prefix:	Overlap between VPIM prefix and local extensions:
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

VPIM network shortcuts (continued)

VPIM prefix:	Overlap between VPIM prefix and local extensions:	VPIM prefix:	Overlap between VPIM prefix and local extensions:
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____
_____	_____	_____	_____

Time zone

(Complete this section for local satellite switch locations only.)

Use server time zone: ❒ Yes ❒ No (Specify the time zone to be used.)	Time zone (if server time zone will not be used:

Completed by

Administrator:	Date:

CallPilot Networking—Message Delivery Configuration: NWP-028

AMIS Networking options

Enable outgoing AMIS Networking messages ❒ Yes ❒ No	Enable incoming AMIS Networking messages ❒ Yes ❒ No
Number of messages to collect before sending (batch threshold):	Open AMIS compose prefix:

Open AMIS Networking delivery times

Days active: ❒ Monday	❒ Tuesday	❒ Wednesday	❒ Thursday
❒ Friday	❒ Saturday	❒ Sunday	
Outgoing messages allowed on business days (hh:mm)		From: _____ To: _____	
Outgoing messages allowed on non-business days (hh:mm)		From: _____ To: _____	

Local system access number (complete one only)

Public network number: Country code: _____ Area/city code: _____ Number: _____	Private network number: _____

Economy delivery times (hh:mm)

Open AMIS Start time: _____ Stop time: _____	Integrated AMIS Start time: _____ Stop time: _____

Stale times (hh:mm)

Economy Open AMIS: _____ Economy Integrated AMIS: _____	Standard _____ Urgent: _____

Enterprise Networking options

Enable outgoing Enterprise Networking messages ❒ Yes ❒ No	Enable incoming Enterprise Networking messages ❒ Yes ❒ No
Number of messages to collect before sending (batch threshold):	

Economy delivery times (hh:mm)

Start time:	Stop time:

Stale times (hh:mm)

Economy:	Standard:
Urgent:	

SMTP and VPIM Networking options

Enable incoming VPIM Networking messages: ❒ Yes ❒ No	Enable outgoing VPIM Networking messages: ❒ Yes ❒ No
Outgoing SMTP Mail/Proxy server:	
Open VPIM compose prefix:	
Open VPIM shortcuts: Complete and attach “Open VPIM Shortcuts” (NWP-038).	

Security modes for SMTP sessions
Note: These settings apply for VPIM Networking, desktop messaging, and web messaging.

Encryption options

Enable SSL for incoming SMTP sessions:	❒ Yes	❒ No
Connect to server with SSL for Outgoing SMTP sessions:	❒ Yes	❒ No

Authentication options
Note: If you choose Yes for Unauthenticated as well as either Challenge and Response or User ID and Password authentication, this is referred to as *mixed authentication*.

Unauthenticated:	❒ Yes	❒ No
Challenge and Response authentication:	❒ Yes	❒ No
User ID and Password authentication:	❒ Yes	❒ No
SMTP/VPIM password for initiating authenticated connections to remote servers:	_____	

Authentication failure attempts

Maximum failed authentication attempts from a remote server:	_____	
Action to perform when the maximum has been reached:	❒ Log only	❒ Log and disable server
Maximum failed authentication attempts from a user:	_____	
Action to perform when the maximum has been reached:	❒ Log only	❒ Log and disable user

Unauthenticated access restrictions

Enable unauthenticated desktop user restrictions	❒ Yes	❒ No
Delivery to telephone or fax	❒ Yes	❒ No
Enable Open AMIS	❒ Yes	❒ No
Enable Integrated Networking	❒ Yes	❒ No
Enable SDL addressing	❒ Yes	❒ No
Enable broadcast addressing	❒ Yes	❒ No
Restrict the number of recipients		
Maximum recipients	_____	
Enable unauthenticated server restrictions:		
Enable SDL addressing	❒ Yes	❒ No
Enable broadcast addressing	❒ Yes	❒ No
Restrict the number of recipients	❒ Yes	❒ No
Maximum recipients	_____	

Remote contact options (AMIS and Enterprise Networking)

Wait before sending C DTMF tone (milliseconds):
Delay for each non-pause character in DN (milliseconds):

Completed by

Administrator:	Date:

CallPilot Networking—Open VPIM Shortcuts: NWP-038

Complete and attach this form to NWP-028.

Open VPIM shortcuts

(You can define up to 500 open VPIM shortcuts. Complete and attach additional pages, if required.)

VPIM prefix	FQDN (domain name)	VPIM prefix	FQDN (domain name)

Completed by

Administrator:	Date:

appendix B

How AMIS and Enterprise Networking handle messages

In this section

Networking messages 261

What the MTA does 263

What the ANA does 264

Example of message handling with AMIS Networking 266

Networking messages

Every networking message contains two main parts:

- a message header
- the message body

Message header

The message header transmits to the receiving site with DTMF signals. The header contains the following information:

- the sender's address which may include the site or location ID, mailbox number, and text name, depending on how the features are enabled (for Enterprise, the sender's spoken name is recorded)
- each recipient's address (site or location ID, mailbox number)
- the system access number
- the type of message (regular, acknowledgment, or non-delivery notification [NDN])
- the time and date when the message was sent
- for Enterprise only, the priority applied to the message (private, urgent, or acknowledgment)

Message body

The recorded message is played over the voice port of the sending site and are recorded by the receiving site. The recorded message contains the following information:

- the voice portion of the message
- any attachments

Message priorities

The sender can assign a message priority to an Enterprise networking message. There are three priorities:

- economy
- standard
- urgent

Standard is usually the default. Users must assign another message priority manually. In general, you send economy messages during lower long-distance toll charge periods. You send urgent messages quickly, with the emphasis on speed rather than cost.

MTA and ANA

The scheduling parameters that you configure during the implementation of a networking solution work with internal CallPilot networking settings. These internal settings are controlled by the

- Message Transfer Agent (MTA)
- Analog Networking Agent (ANA)

This brief overview provides a general understanding of how networking handles messages to help you interpret Alarm and Event reports.

MTA responsibilities

The MTA provides many of the basic maintenance functions required by CallPilot networking. The MTA is responsible for the following services:

- Queue outgoing network messages.
- Determine when to begin sending messages to a remote system.
- Receive incoming messages for delivery to local users.
- Collect networking traffic Operational Measurements (OM) reports.

To ensure the timely handling of messages, the MTA wakes up every minute. When it wakes up, the MTA does the following:

- initiates calls to remote sites
- checks for stale messages
- checks if any sites are in error status

MTA Monitor

When enabled, the MTA Monitor continuously watches the performance of the MTA. The MTA Monitor provides detailed information and is useful for regular maintenance and troubleshooting.

ANA responsibilities

The ANA sends messages to and receives messages from remote systems configured with either AMIS or Enterprise networking. There is one instance of the ANA for every active analog networking session. An ANA instance terminates once the session is over.

Main steps of message transfer

There are three main steps in the message transfer process:

- The MTA determines if a message destined for an AMIS or Enterprise site is ready for transfer and if so, passes it to the ANA.
- The ANA completes a communication process, known as handshaking, with the receiving site.
- The message, which consists of the message header and the message body, is transferred.

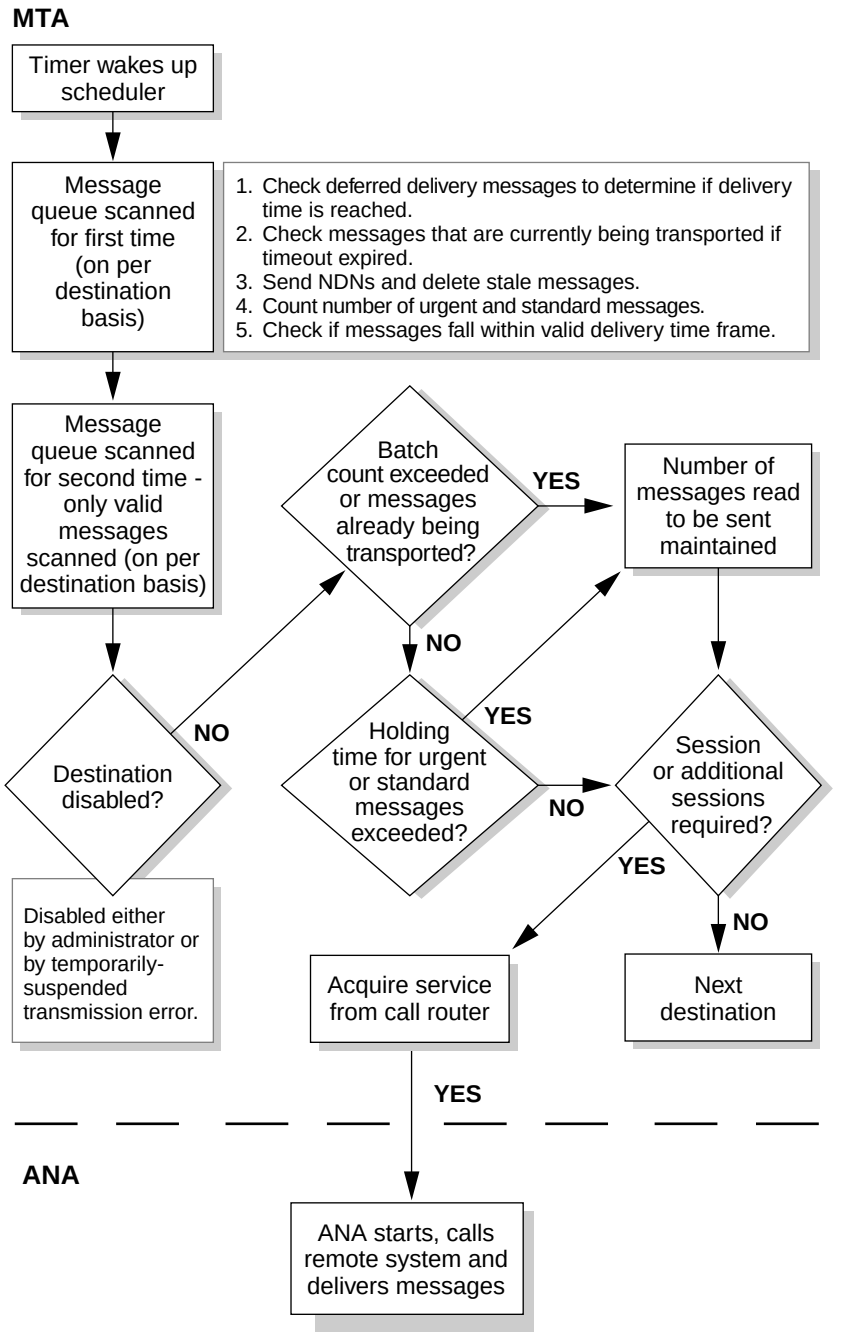
What the MTA does

The MTA handles most aspects of message transmission for CallPilot.

How MTA and ANA handle messages

The following diagram is a graphical representation of how CallPilot handles Integrated AMIS Networking messages.

The diagram shows the activity of both the MTA and the ANA in message handling.



G100969

As the preceding diagram indicates, the MTA handles most of the message processing. Every minute, a scheduler wakes the MTA. The MTA scans the message queue for each destination, and checks the status of messages awaiting delivery. This scan determines if there are valid messages, according to the system parameter configuration. The MTA then determines if the valid messages are ready for delivery, according to the set system parameters. Once the MTA determines that a transmission session is needed, it seeks a method of delivery from the call router. The ANA assumes responsibility for delivering the message.

What the ANA does

The ANA does the actual message delivery or reception. It works with the MTA to handle messages.

How the ANA sets up calls

The ANA calls a remote site and delivers messages. CallPilot originates a network call to the receiving site using the connection directory number (DN) defined for that site. The switch places the call according to switch call-processing parameters. If the call is successful, the call terminates on the networking connection DN at the receiving site.

If the call fails due to a busy or no-answer condition, CallPilot waits until the next wake-up interval before it attempts the call again. If three consecutive attempts fail, CallPilot places the receiving site into error status and an alarm is generated, depending on the nature of the problem. CallPilot waits for half an hour before it repeats the three-call attempt cycle.

When connection between the sending and receiving sites is established, ANA initiates a communication process known as handshaking. Handshaking consists of the following steps:

1. The sending site identifies itself to the receiving site.
2. For the Enterprise solution, the receiving site verifies that the sending site is defined in the network database of the receiving site, and that the site ID and the message transfer protocol agree. If the information does not agree, the receiving site informs the sending site of the error and drops the call.
3. The sending site sends the initiating password and the receiving site ID to the receiving site.
4. The sending site also indicates that it will send a remote user text information if the necessary options are enabled on the site configuration for the receiving site.
5. The receiving site checks the site ID and password:

   If the information is invalid, the receiving site informs the sending site that either the site ID or the password is incorrect, and drops the call.

   If the information is valid, the receiving site proceeds to the following step.
6. The receiving site determines whether remote user or message text information will be received during this session.
7. The receiving site sends the responding password and indicates whether Names Across the Network information and a text subject header will be sent during this session.
8. The sending site checks the password:

   If the password is invalid, the sending site sends an end-of-session message and drops the call.

   If the password is valid, the sending site starts the message transfer to the receiving site.

Message transfer process

The following table describes how messages are transferred for Integrated AMIS networking:

The sending site	The receiving site
uses DTMF tones to send the message header to the integrated site. The message header contains: ■ the sender's mailbox number without location prefixes ■ the sender's system access number ■ the recipient's mailbox without location prefixes	receives the DTMF tones, interprets the tones, and creates the message.
plays the voice portion of the message across a voice port.	records the message body and adds it to the message.
repeats these steps for each message the sending site must send. **Note:** The maximum number of messages in a transfer session is five.	repeats these steps for each message.
terminates the message transfer session.	hangs up.

The following table describes how messages are transferred for Enterprise networking:

The sending site	The receiving site
sends the message information. The message contains the following: ■ time and date stamp ■ subject ■ message priority (private, urgent, or acknowledgment)	receives and intercepts the message information and creates the message.
sends the information about the sender. The information includes the following: ■ mailbox number, including site ID (and location ID if the remote site is using NMS)	receives and adds the sender to the message.
if the Remote User Add/Update option is selected, plays the spoken name.	■ records the spoken name. ■ adds or updates the remote user.

The sending site	The receiving site
sends recipient information. The information includes the following: ■ mailbox number (including site and location ID). ■ recipient's address as text, if the Receive Text Information option is selected.	receives and adds each recipient to the message.
plays the message body.	records the message body and adds it to the message.
plays any attachments.	records each attachment and adds it to the message.
indicates the end of the message.	sends to the local MTA to deposit the message in each local recipient's mailbox.
repeats all of the above for each message.	repeats all of the above for each message.

Example of message handling with AMIS Networking

The following example shows how the message delivery configuration and the internal settings work together. The example offers a high-level overview of how users use AMIS Networking and how the system handles AMIS Networking messages.

How a user sends a message to a remote AMIS user

1. The user logs on to CallPilot.
2. The user enters **75** to compose a message.
3. The user enters the AMIS compose prefix.

   Example: 13

   The prefix alerts the system that the message is intended for an AMIS Networking user.
4. The user enters the number as it normally would be dialed from the system, followed by #.

   Example: 914165553333#

   The # symbol indicates the end of the system access number.
5. The user enters the mailbox number of the intended remote recipient, followed by #.

   Example: 8123#

   The system responds with the following message: `Open network user <mailbox number> at <system access number>`.

6. The user enters **#** and **5** to record the message, records the message, and enters **#** to stop the recording.
7. The user enters **79** to send the message.
8. The user logs out of CallPilot and hangs up.

How CallPilot handles the message

Here is a simplified overview of the process that transfers an AMIS message to a remote user. The MTA periodically checks for new outgoing messages. When the MTA detects a ready message with an AMIS recipient, it starts a queue for the recipient site. Successful delivery results in an acknowledgment if the message was so tagged. An acknowledgment to an AMIS message is sent when the message is transmitted, not when it is listened to.

How a remote user replies to an AMIS message

A remote user at a CallPilot site can easily reply to an AMIS message.

1. While within the received message, the remote user enters **71** to reply to the message.
2. The user enters **5** to record the message, records the message, and then enters **#** to stop the recording.
3. The user enters **79** to send the message.

How the remote system handles the message reply

The remote system uses the system access number contained in the header of the original message to return the call. However, when using the public switch telephone network, the original system access number does not include a network dialing prefix. The missing prefix indicates to the system that the reply is an external call. The remote system must add the network dialing prefix to the system access number.

Example

- The system access number of the original message = 14167779898.
- The remote system adds a dialing prefix (for example, 9) to allow dialing out from the switch.

Relationship of a system access number to a connection DN

A system access number becomes a connection DN in the network database record of a remote messaging server. The system access number uniquely identifies a site. When you send a message to an integrated site, the local site looks up the connection DN for that remote site and initiates the network call. The local site identifies itself to the remote site by including its own system access number in the message header. The receiving site takes that system access number and searches its own network database for a connection DN that matches the system access number.

The receiving site identifies the sending site if it finds a connection DN that matches the system access number it received. When the recipient listens to the message, the sending site is identified.

If the receiving site does not find a connection DN that matches the system access number it received, it treats the message as an Open AMIS message sent from a remote site that is not part of the private messaging network. When the recipient listens to the message, the sending site is identified only as an open site.

Index

A

access code and ESN prefix 80
access code, ESN 197
access mechanism
  direct access 107
  indirect access 107
  offnet access 107
ACD-DNs, on existing satellite switches 113
addressing a message
  to a local user with ESN 81
  to a remote user with ESN 81
  to an integrated site 41
  to an open site 42
addressing plan
  distinguished from dialing plan 86
administering a remote site 15
administration guides 12
administration, network
  about implementation 141
  administrator responsibilities 142
  implementation scenarios 141
administrators
  time zone conversions (Network Message Service) 116
alarm mailbox 49
AMIS compose prefix
  selecting 179
AMIS delivery times
  default values 179
  described 180, 183
AMIS Networking
  broadcast messages 101, 103
  description 140
  disabling 178
  enabling 178
  implementation checklists 236
  in complex network 169
  mailbox length supported 52
  Message Delivery Configuration page, CallPilot Manager .. 149
  message handling 53
  message length supported 39
  message transmission time 65
  message types supported 38
  minimizing risk of long-distance toll fraud 212
  preliminary requirements for configuration 191
  recipients, time zone conversions (Network Message Service) 116
  sending message to remote user scenario 266
  when to implement 146
AMIS protocol 23
  compared with Enterprise Networking protocol 33
AMIS-A protocol. *See* AMIS protocol
AML. *See* Application Module Link
ANA (Analog Networking Agent)
  description 262
analog protocol
  AMIS protocol 23
  compared to digital 24
  Enterprise Networking protocol 23
another dialing plan
  example 93
  recommended relationship between dialing and addressing plans 86
application gateway
  definition 215
  overview 214
Application Module Link
  previously known as 106
Attendant Extended Call feature, interaction with NMS .. 109
Audio Messaging Interchange Specification protocol. *See* AMIS protocol 23
authentication activity, monitoring 218
  automatic monitoring 227
  manual monitoring 228
authentication failures, description 226–227
authentication modes
  description 218
  enabling 220
  when to use 220
authentication, mixed
  enabling 221
  user impact 222
  when to use 221, 222
authentication, SMTP
  broadcast messages 100
  Challenge and Response 222
  description 217
  desktop or web messaging users 218
  disabling 219
  enabling 220
  encryption 218, 232
  location broadcasts 102
  network broadcasts 102
  user ID and password 223
  when to disable 219
  when to use 220

B

Barge-in Attendant feature, interaction with NMS 109
batch threshold
  default value 177
  description 178, 183
benefits of remote users 68
broadcast mailbox 49
broadcast message 108
broadcast, network
  addresses, viewing 104
  addressing rules 98
  description 97
  desktop messaging users, mailbox class validation 100
  distribution lists 99
  location broadcast, description 96

multimedia support 103
Network Message Service (NMS) 100
networking protocols 101
phoneset users, mailbox class validation 100
remote server capabilities 102
requirements 95
server capabilities 101
SMTP authentication 100, 102
user capabilities 99
when to disable 101–102
Business Communications Manager
location broadcasts 103
network broadcasts 103

C

calculating message length 40
Call Forward by Call Type Allowed feature, interaction with NMS 109
Call Forward feature
interaction with NMS 108
types supported 108
calling
local users with CDP 83
remote users with 83
CallPilot
features supported by networking solutions 44
messaging network 21, 25
networking solutions 30
CallPilot 1.0x
location broadcasts 102
network broadcasts 102
CallPilot features, interaction with networking 158
CallPilot Manager
Cancel button 150, 153
logging on 15
Message Delivery Configuration page, accessing 150
Message Network Configuration page, accessing 151
Save button 151, 154
web server, description 148
CallPilot server
and CallPilot Manager 148
logon 15
with integrated web server, diagram 148
Cancel button, CallPilot Manager 150, 153
CDP dialing plan
and user location 110
ESN dialing plan recommended 162
CDP information
remote prime switch location 209
CDP steering code 82
and extension length 84
and nonuniform dialing plan 79
creating 83
location code 77
overlap 198
overview 198
requirement 82
certificates, encryption 233
Challenge and Response authentication, description 222
channel requirements 159
channel resource allocation
minimum and maximum 173
channel types supported 173
channels
impact of NMS on number required 159
types required 159
types supported 50
checklist for gathering information 164
checklists, network implementation 146, 236
CO Loop Start trunk 109
combining several switch locations into one user location 110
Command and Status Link, now known as Application Module Link 106
complex network 169
compose prefix
selecting 179
Conference Call feature, interaction with NMS 109
configuration
prime switch location overview 112
configuration worksheets, network 237
configuring
remote satellite switch location, overview 210
configuring satellite switch locations, overview 112
confirming switch settings 163
connection DN
relationship to system access number 267
remote messaging server 205
controling how Names Across the Network works 71
Coordinated Dialing Plan 82
calling users 83
definition 82
example 91
mailbox address and 84
recommended relationship of dialing and addressing plans. 86
steering code 82
steering code definition 82
CSL (Command and Status Link) 106

D

data network
and VPIM Networking 119
definition 21
private 21
public 21
setup to implement VPIM Networking 128
database, network
description 142–143
information
consistency, ensuring 157
coordinating 157
when to add sites 143
default value
AMIS delivery times 179
batch threshold 177
delivery start time for economy messages 177
delivery stop time for economy messages 177
holding time for standard messages 177
holding time for urgent messages 177
parameters 177

reason to use ... 177
scheduling parameters ... 177
stale time for economy messages ... 177
stale time for standard messages ... 177
stale time for urgent messages ... 177
defining dummy ACD-DNs ... 114
definition
application gateway ... 215
CDP ... 82
data network ... 21
dialing plan ... 76
ESN ... 80
firewall ... 214
messaging network ... 21, 25
network ... 20
prime switch location ... 105
proxy server ... 214
remote user ... 68
satellite switch location ... 105
site ... 26
steering code ... 82
switch network ... 20
tandem switch location ... 105
uniform dialing plan ... 77
user location ... 106
delivery sessions ... 51
delivery start and stop times, economy messages ... 180
delivery start time for economy messages
default value ... 177
delivery stop time for economy messages
default value ... 177
delivery times for AMIS messages ... 180, 183
denial-of-service attacks, preventing ... 219, 221
description
local server ... 192
desktop messaging users
authentication failures, description ... 225
broadcast messages ... 100
time zone conversions (Network Message Service) ... 116
desktop user ... 41
desktop user logon ... 107
desktop users
compared with telephone users ... 120
exchanging messages with open sites ... 121
diagram of how MTA and ANA handle messages ... 263
diagrams
local NMS location broadcast ... 96
mesh network ... 143
network broadcast ... 98
Network Message Service (NMS)
example ... 115
multiple time zones ... 115
non-mesh network ... 144
remote NMS location broadcast ... 97
web server setup ... 148
dialing plan
already set up ... 77
and mailbox address with ESN ... 81
and VPIM Networking ... 163
CDP for remote prime switch location ... 209
changing ... 166
definition ... 76
distinguished from addressing plan ... 86
ESN for remote prime switch location ... 208
from a system perspective ... 76
from a user perspective ... 76
hybrid dialing plan requirements ... 110
information required from switch ... 163
information required to configure switch location ... 196
location code ... 77
mailbox addressing follows ... 197
mailbox addressing follows for remote prime switch location 208
recommended dialing plan ... 162
remote satellite switch location ... 210
requirements ... 166
switch configuration changes ... 86
types supported by CallPilot ... 77
uniform ... 77
used to a remote switch location ... 208
dialing plans
CDP configuration worksheet ... 237
considerations ... 158
ESN configuration worksheet ... 237
dialing restrictions
NMS beyond messaging network ... 62
NMS in messaging network ... 62
within NMS network ... 62
digital protocol
compared to analog ... 24
type used by CallPilot ... 23
direct inward system access, required for offnet access ... 107
DISA (direct inward system access) ... 107
disabling AMIS Networking ... 178
disabling Enterprise Networking ... 183
distribution lists, and broadcast messages ... 99
DN. *See* directory number
DNS
overview ... 126
DNS lookup tables ... 126
DNS server ... 126
and MX records ... 126
implementation ... 128
setup ... 127
domain name ... 125
domain name system. *See* DNS
dual-tone multifrequency ... 168
dummy ACD-DNs
defining ... 114
number required ... 114
setting to night call forward ... 115

E

economy delivery start and stop times ... 180
economy priority messages ... 261
Electronic Switched Network ... 86
addressing a local user ... 81
addressing a remote user ... 81
addressing local user ... 81
and mailbox addresses ... 81
calling local users with ... 80
calling remote users with ... 80

definition 80
ESN prefix 80
example 90
Electronic Switched Network. *See* ESN
e-mail gateway server, implementation with 129
enabling AMIS Networking 178, 193
enabling Enterprise Networking 183
encoding VPIM message parts 120
encryption 218
authentication 232
certificates 233
considerations for implementation 230
description 230
Entrust software 215
firewalls 232
mail relays 232
Meridian Mail Net Gateway 232
security and VPIM Networking 215
SSL 231
VPIM-compliant systems 232
when to use it 230
end-to-end signaling capabilities and NMS 61
engineering network 160
Enterprise Location ID
local prime switch location 196
remote prime switch location 207
Enterprise Networking
broadcast messages 101, 103
controling text information 66
description 33, 141
diagram 33
disabling 183
enabling 183
Enterprise Location ID 196, 207
Enterprise Site ID 192
how sites use Names Across the Network 74
implementation checklist 236
message delivery 57
Message Delivery Configuration page, CallPilot Manager . 149
message length 57
message length and non-delivery notifications 40
message length supported 39
message transmission times with text 66
message types supported 39
Names Across the Network 193
Names Across the Network and message transmission times 67
protocol 23
receiving message text information 193, 194
recipients, time zone conversions (Network Message Service) 117
Enterprise Networking protocol 23
advantages over AMIS protocol 33
Enterprise Site ID
description 192, 202
Entrust, encryption 215
ESN
access code 197
location code 197
location code overlap 198
ESN dialing plan
and user location 110
recommended over CDP dialing plan 162
ESN information, remote prime switch location 208
ESN prefix
and access code 80
location code 77, 80
ESN. *See* Electronic Switched Network
Event Monitor and non-delivery notifications 43
exchanging messages
with integrated sites, telephone and desktop users compared 121
with open sites, telephone and desktop users compared 121
exchanging messages with open sites 28
extension length and CDP steering code 84

F

failures, authentication
description 225–227
limiting 226
potential causes 224
reporting 226
fax channel 159
fax channel type 173
fax message type
support 38
features
networking solutions compared 44
firewall
and implementation 129
definition 214
description 214
security and VPIM Networking 214
firewalls and encryption 232
FQDN
overview 125
right-hand side of VPIM address 122
FQDN of local SMTP/VPIM server 194
From entry, header 122
fully qualified domain name. *See* FQDN

G

gathering information
checklist 164
from open sites 162
purpose 161
remote switch location checklist 165
gathering required information
new implementation 162
upgrade 162

H

header contents 261
header, From entry 122
holding time
description 178
standard messages 178, 181

urgent messages 178, 182
holding time for standard messages, default 177
holding time for urgent messages, default 177
host name 125
hybrid dialing plan
example 92
mailbox addresses and 85
recommended relationship of dialing and addressing plans . 86
hybrid dialing plan, requirements 110

I

IMAP. *See* Internet Mail Access Protocol (IMAP)
implementation
dialing plan setup 77
preliminary requirements 128
with DNS server 128
with e-mail gateway server 129
with firewall 129
implementation, network
about 141
checklists 146, 236
definition 145
Message Delivery Configuration page, CallPilot Manager .. 149
Message Network Configuration page, CallPilot Manager .. 151
prerequisites 145
process 236
recommendations 146
scenarios 141
implementing
remote site 15
implementing a messaging network
network database 27
relationship to existing networks 26
implicit open sites 144
inbound message
from implicit open site 123
from integrated sites 122
from unknown open site 123
industry-standard protocol 23
information in network database
local site 26
remote site 26
initiating password 206
description 206
installation and configuration guides 11
installation, networking (definition) 145
Integrated AMIS Networking
implementation checklist 236
mailbox length 55
message contents 261
message delivery 55
Message Delivery Configuration page, CallPilot Manager .. 149
message length supported 39
message types supported 38
switch settings required 166
when to implement 146
Integrated Service Digital Network (ISDN) 106
Integrated Services Digital Network/Applications Protocol link, now known as Application Module Link .. 106
integrated site 27
combined with open site 28
integrated sites 144
interaction with NMS 109
Internet Mail Access Protocol (IMAP)
already configured 130
implementation order 128
Internet Service Provider (ISP) 129
IP address 125
ISDN signaling capabilities and NMS 61
ISDN/AP (Integrated Services Digital Network/Applications Protocol link) 106
ISDN-PRI, between switches 106

J

junk e-mail, preventing 219, 221

K

keycode, networking 145
keycodes
installation precaution 37
installing networking solutions 36
Networking keycode 36
NMS keycode 36

L

LAN load and impact of VPIM Networking 59
LAN network traffic and impact on VPIM Networking ... 67
left-hand side of VPIM address 120
legal considerations, Open AMIS messages 180, 183
legal delivery times for AMIS messages 179, 180, 183
local broadcast
user capabilities 99
local messaging server 192
local prime switch 195
local prime switch location
description 196
dialing plan information 196
Enterprise Location ID 196
mailbox prefix 197
name 196
local server
broadcast messages
capabilities 101
controlling 101
when to disable 101
broadcast messages, when to disable 102
configuration worksheet 237
description 192
logging on 15
name 192
server type 192
local site

logging on to ... 147
modifying ... 153
tree view ... 152
local site information
in network database ... 26
local site name ... 192
local switch location
configuration worksheet ... 237
tree view ... 152
local system access number
purpose ... 180
location broadcast
addresses, viewing ... 104
description ... 96
distribution lists ... 99
local NMS location broadcast, diagram ... 96
multimedia support ... 103
Network Message Service (NMS) ... 100
networking protocols ... 101
remote NMS location broadcast, diagram ... 97
remote server capabilities ... 102
server capabilities ... 101
SMTP authentication ... 102
user capabilities ... 99
when to disable ... 101–102
location code
CDP steering code ... 77
ESN ... 197
ESN prefix ... 77, 80
overlap ... 198
purpose ... 77
location name, required by desktop users to log on ... 107
log on, desktop users and location name ... 107
logging on
local server ... 15
local site ... 147
remote server ... 15
remote site ... 147
logon ... 15
long-distance toll fraud
minimizing risk with AMIS Networking ... 212

M

mail exchange records. *See* MX records
mail relays and encryption ... 232
mail servers, and MX records ... 126
mailbox address
and CDP ... 84
and ESN dialing plans ... 81
mailbox addressing follows dialing plan, local prime switch location ... 197
mailbox addressing, dialing plan follows for remote prime switch location ... 208
mailbox length
Integrated AMIS Networking ... 55
maximum for AMIS Networking ... 52
mailbox prefix
local prime switch location ... 197
remote prime switch location ... 208
MDN (message delivery notification) ... 124
Meridian 1 (Release 23C), prime switch ... 107
Meridian Mail
location broadcasts ... 103
network broadcasts ... 103
Meridian Mail Net Gateway
encryption ... 232
Entrust and VPIM Networking ... 215
location broadcasts ... 103
network broadcasts ... 103
mesh network, diagram ... 143
message
body contents ... 261
broadcast ... 108
configuration for using priorities ... 261
contents ... 120
encoding ... 120
handling scenario ... 265
header contents ... 261
parts ... 261
priorities ... 261
message center directory number ... 108
message delivery
Enterprise Networking ... 57
Integrated AMIS Networking ... 55
VPIM Networking ... 60
Message Delivery Configuration ... 176
accessing, CallPilot Manager ... 150
description ... 148, 151
worksheet ... 237
Message Delivery Configuration tree view, capacity ... 107
message delivery notification (MDN) ... 124
message handling ... 263
message handling by AMIS Networking ... 53
message header contents ... 120
message length
and non-delivery notification ... 40
calculating ... 40
Enterprise Networking ... 57
Message Network Configuration ... 192
accessing, CallPilot Manager ... 151
description ... 148
sites, maximum number ... 152
switch locations, maximum number ... 152
tree view, description ... 151
worksheets ... 237
Message Transfer Agent (MTA), description ... 262
message transfer, main steps ... 262
message transmission time
AMIS Networking ... 65
assumptions used to calculate ... 65
comparison of networking solutions ... 65
factors affecting ... 64
factors affecting VPIM Networking ... 64
NMS ... 65
voice and text messages compared ... 66
VPIM Networking and network traffic ... 67
message treatment
inbound from implicit open site ... 123
inbound from integrated site ... 122
inbound from unknown site ... 123
message types
and non-delivery notifications ... 39

networking solutions compared 38
messaging network
combining integrated and open sites 28
definition 21, 25
dialing plan setup 77
dialing plans supported 77
hierarchy of protocols 24
implementation, incremental 26
integrated and open 27
messaging network representation
another dialing plan example 93
benefits 89
CDP dialing plan example 91
ESN dialing plan example 90
ESN dialing plan with NMS example 90
hybrid dialing plan 92
hybrid dialing plan example 92
messaging network setup
mesh 22
non-mesh 22
messaging network, basic design tasks 142
messaging networks
and users 38
exchanging messages with open sites 28
migration guides 11
MIME
overview 127
TCP/IP protocol 127
MIME (Multipurpose Internet Mail Extensions) 23
mixed authentication mode
description 218
enabling 221
user impact 222
when to use 221, 222
modes of authentication, description
authenticated mode 218
mixed authenticated mode 218
unauthenticated mode 218, 219
modifications to messaging network configuration
impact on personal distribution lists 48
MTA (Message Transfer Agent), description 262
MTA Monitor, description 262
multimedia messages, and non-delivery notifications 123
Multipurpose Internet Mail Extensions (MIME) 23
Multipurpose Internet Mail Extensions. *See* MIME
MX records
and DNS server 126
and mail servers 126

N

name
local prime switch location 196
remote prime switch location 207
name of a remote site 201
name of the local server 192
Names Across the Network 193
adding temporary remote users 70
considerations 73
controling 71
how sites use 74
when remote user is added 71
when temporary remote user is added 73
NCRD. *See* Network Call Redirection
NDN. *See* non-delivery notification
network
data 21
messaging network 25
switch network 20
network administration
about implementation 141
administrator responsibilities 142
assumptions 145
implementation scenarios 141
network broadcast
addresses
viewing 104
addressing rules 98
description 97
desktop messaging users, mailbox class validation 100
diagram 98
distribution lists 99
location broadcast, description 96
multimedia support 103
Network Message Service (NMS) 100
networking protocols 101
phoneset users, mailbox class validation 100
remote server capabilities 102
requirements 95
server capabilities 101
SMTP authentication 100, 102
user capabilities 99
when to disable 101–102
Network Call Redirection 107
network call forward all calls 107
network call forward busy 107
network call forward no answer 107
network hunting 107
types supported 107
Network Call Redirection feature and NMS 61
Network Call Transfer feature, interaction with NMS 108
Network Class of Service
checking current setting 106
level required by NMS 106
network database
configuration, validating 154
contents 26
description 142–143
implementing CallPilot 27
information
consistency, ensuring 157
coordinating 157
uniqueness, ensuring 155
sites, maximum number 152
when to add sites 143
Network Hunting feature, interaction with NMS 108
network implementation
basic tasks 142
checklists 146
configuration worksheets 157
definition 145
Message Delivery Configuration page, CallPilot Manager 149

Message Network Configuration page, CallPilot Manager . 151
prerequisites ... 145
recommendations ... 146
Network Message Service (NMS)
broadcast messages ... 100
description ... 115
example diagram ... 115
implementation recommendation ... 146
multiple time zones, diagram ... 115
time zone conversion
description ... 115–117
Network Message Service. *See* NMS
network planning
about implementation ... 236
configuration worksheets ... 237
implementation checklists ... 236
network setup
mesh network ... 22
non-mesh network ... 22
network topology. See network setup
network types
mesh ... 143
non-mesh ... 144
networking
about implementation ... 141
and CallPilot feature interaction ... 158
channel requirements ... 159
dialing plans ... 158
engineering issues ... 160
installation versus implementation ... 145
limitations ... 160
security, recommendations ... 160
Networking keycode ... 36
networking solutions ... 51
CallPilot ... 30
channel types supported ... 50
comparison of message lengths supported ... 39
Enterprise Networking ... 33
feature support comparison ... 44
installation and keycodes ... 36
message transmission time compared ... 65
message type support comparison ... 38
personal distribution lists ... 48
night call forward dummy ACD-DNs ... 115
nightly audit
deleting permanent remote users ... 71
time stamps ... 69
NMS (Network Message Service) ... 105
Attendant Extended Call feature ... 109
Barge-in Attendant feature ... 109
Call Forward by Call Type Allowed feature ... 109
Call Forward feature ... 108
CO Loop Start trunk ... 109
Conference Call feature ... 109
dialing plan implications ... 62
dialing restrictions beyond private network ... 62
dialing restrictions in messaging network ... 62
dialing restrictions in NMS network ... 62
example ... 90
impact on channels ... 159
message length ... 40
message transmission time ... 65
message types supported ... 39
Network Call Redirection feature ... 61
Network Call Transfer feature ... 108
Network Class of Service level required ... 106
Network Hunting feature ... 108
NMS network and NMS site distinguished ... 34
signaling considerations ... 61
NMS keycode ... 36
NMS network ... 34
as type of private messaging network ... 105
NMS site ... 34
non-delivery notification ... 122, 123
multimedia messages ... 123
non-delivery notifications
and Event Monitor ... 43
and message length ... 40
and message types ... 39
and personal distribution lists ... 48
non-mesh network, diagram ... 144
non-Nortel Networks systems
location broadcasts ... 103
network broadcasts ... 103
nonuniform dialing plan
CDP steering codes ... 79
examples ... 79
Norstar VoiceMail
location broadcasts ... 103
network broadcasts ... 103
NSM network ... 105
number of delivery sessions compared ... 51
number of dummy ACD-DNs required on satellite switch locations ... 114
number of sites supported ... 50
number of switch locations supported ... 107

O

offnet access ... 107
switch requirements ... 107
OM reports. *See* Operational Measurement reports
online guides ... 14
online Help, accessing ... 14
Open AMIS compose prefix ... 179
Open AMIS delivery times ... 179
open site ... 27
combined with integrated sites ... 28
exchanging messages with ... 28
protocols used with ... 27
open sites ... 144
and protocols ... 144
implicit ... 144
VPIM Networking ... 144
open VPIM Networking
implementation checklist ... 236
shortcuts, configuration worksheet ... 237
Operational Measurement reports ... 124
overlap
CDP steering code ... 198
ESN location code ... 198

P

packet filter, overview 214
parameters
  default values 177
passwords
  description 206
passwords for remote site 206
permanent remote user 69
permanent remote users
  deleting with nightly audits 71
  removing with User Administration 71
personal distribution lists
  and non-delivery notifications 48
  impact of modifications to messaging network configuration 48
  networking solutions 48
phantom DN
  how to select 170
phantom DNs
  determining those used on prime switch location 112
  satellite switch locations 113
phoneset users
  broadcast messages 100
  time zone conversions (Network Message Service) 116
ping attack
  description 216
  security against 216
planning guides 11
prefix
  compose 179
  mailbox 197
prefixes
  location prefix, description 99
  network broadcast prefix
    rules 98
preliminary requirements for implementation
  dialing plan setup 77
preliminary requirements for implementing VPIM Networking 128
prime switch
  satellite switches forward to 113
  type supported 107
prime switch location
  communicating with satellite switch locations using ISDN-PRI 106
  configuration 112
  definition 105
  determining phantom DNs used on 112
  using virtual signaling to communicate with satellite switches 106
prime switch location, configuration worksheet 237
priorities of messages 261
privacy, guaranteeing on CallPilot 230
private data network 21
private switch network 21
proprietary protocol 23
protecting temporary remote user from removal 70
protocol
  analog and digital compared 24
  analog used by CallPilot 23
  digital 23
  hierarchy 24
  industry-standard 23
  proprietary 23
  types 23
  used with open sites 27
protocols
  TCP/IP protocols 127
protocols, open sites 144
proxy server
  definition 214
  overview 214
public data network 21
public switch network 21

R

receiving message text information 193, 194
relationship of dialing and addressing plans 86
remote administration
  how to work remotely 15
  site security 147
remote messaging server 200
  connection DN 205
  name 201
  sending local user information to 203
  sending messages to a remote site 202
  server FQDN 205
  server types supported 202
remote prime switch 207
remote prime switch location
  CDP information 209
  dialing plan for dialing to this location 208
  Enterprise Location ID 207
  ESN information 208
  mailbox addressing follows dialing plan 208
  mailbox prefix 208
  name 207
  spoken name recorded 207
remote satellite switch location
  configuration overview 210
  dialing plan 210
  spoken name recorded 210
remote servers
  broadcast messages
    capabilities 101
    controlling 101
    when to disable 102
  configuration worksheet 237
remote site
  correcting information about 200
  name 201
  passwords 206
  server FQDN required 163
remote site information in network database 26
remote sites
  authentication failures, description 226
  creating 153
  integrated 144
  logging on to 147
  modifying 153
  network database 143

open ... 144
tree view ... 152
remote switch location
configuration worksheet ... 237
information required ... 165
tree view ... 152
remote user
benefits ... 68
definition ... 68
distinguished from user at remote site ... 68
permanent status ... 69
temporary ... 203
temporary status ... 69
responding password ... 206
description ... 206
restricting sending messages to a remote site ... 202
right-hand side of VPIM address ... 120
routing, TCP/IP ... 125

S

satellite switch
forwarding to prime switch ... 113
types supported ... 107
satellite switch location
configuration ... 112
configuration worksheet ... 237
configuring remote ... 210
creating ... 153
defining dummy ACD-DNs ... 114
definition ... 105
included in broadcast message ... 108
modifying ... 153
number of ACD-DNs required ... 114
phantom DNs ... 113
setting dummy ACD-DNs to night call forward ... 115
satellite switch location SDNs, in SDN Table ... 113
Save button, CallPilot Manager ... 151, 154
scenario of how a message is sent to a remote user ... 266
Secure Socket Layer (SSL)
and encryption ... 231
and user ID/password authentication ... 231
security
application gateway ... 214
encryption and VPIM Networking ... 215
packet filter ... 214
proxy server ... 214
recommendations ... 160
service attacks ... 216
types of attacks ... 215
security modes for SMTP ... 184, 185
security, SMTP authentication
activity, monitoring ... 218
automatic monitoring ... 227
manual monitoring ... 228
unauthentication mode, recommendations ... 219, 220
sending local user information to a remote site ... 203
sending messages to other sites ... 193
server FQDN
local SMTP/VPIM server ... 194
relationship to VPIM shortcuts ... 122
remote site ... 205
required for integrated remote sites ... 163
server type
local server ... 192
supported for remote messaging server ... 202
service attack
ping attacks ... 216
security against ping attacks ... 216
service directory number (SDN)
relationship to other numbers ... 173
Service Directory Number (SDN) Table
contents ... 111
example ... 171
satellite switch location ... 113
setting up DNS server ... 127
shortcuts
VPIM open andSMTP/ VPIM network compared ... 121
signaling considerations for NMS
end-to-end ... 61
ISDN ... 61
virtual ... 61
Simple Message Transfer Protocol (SMTP) ... 23
Simple Message Transfer Protocol. *See* SMTP
site
combining open and integrated sites ... 28
definition ... 26
integrated ... 27
maximum number supported ... 50
open ... 27
SMTP
overview ... 127
TCP/IP protocol ... 127
SMTP (Simple Message Transfer Protocol) ... 23
SMTP authentication
and encryption ... 232
broadcast messages ... 100
Challenge and Response ... 222
description ... 217
desktop or web messaging users ... 218
disabling ... 219
enabling ... 220
encryption ... 218
failures, description ... 226–227
location broadcasts ... 102
modes of authentication, description ... 218
network broadcasts ... 102
user ID and password ... 223
when to disable ... 219
when to use ... 220
SMTP authentication activity, monitoring ... 218
automatic monitoring ... 227
manual monitoring ... 228
SMTP authentication, mixed
enabling ... 221
user impact ... 222
when to use ... 221, 222
SMTP/VPIM network shortcut
compared with VPIM open shortcut ... 121
SMTP/VPIM server FQDN ... 194
speech recognition channel type ... 173
speech-recognition channel ... 159
spoken name

recorded for remote satellite switch location 210
spoken name recorded
remote prime switch location 207
ways to record 196, 208
stale time
description 181, 183
stale time for economy messages, default 177
stale time for standard messages, default 177
stale time for urgent messages, default 177
stand-alone server 15
standard message, holding time 178
standard priority messages 261
status
permanent remote users 69
temporary remote user 69
steering code 82
and extension length 84
creating 83
definition 82
requirement 82
steering code for CDP 198
switch
confirming settings 163
dialing plan information required 163
gathering information directly from 163
mandatory requirements 166
switch configuration
changing dialing plan 86
switch location
configuration worksheet 237
corresponds to user location 110
creating 153
modifying 153
prime 105
satellite 105
several correspond to user location 110
tandem 105
tree view 152
switch network
definition 20
private 21
public 21
system access number
relationship to connection DN 267
system access number (SAN)
purpose 180
types 180
system mailbox
alarm 49
broadcast 49

T

tandem switch location, definition 105
TCP/IP
overview 125
protocols 127
routing 125
TCP/IP application protocols, types supported 23
TCP/IP protocols
MIME 127
SMTP 127
technical support 14
telephone user 41
telephone users
compared with desktop users 120
exchanging messages with open sites 121
temporary remote user 69
adding with Names Across the Network 70
adding with User Administration 70
deleting 71
Names Across the Network options 71
protecting from removal 70
system capacity 69
temporary remote user, Names Across the Network 203
text information in messages 193, 194
text message type support 38
text messages
transmission time and control of use 66
TIFF format 120
time periods
guidelines 156
time stamp
updating 74
time zones, Network Message Service (NMS)
administrators 116
AMIS Networking recipients 116
description 115–117
desktop messaging users 116
Enterprise Networking recipients 117
phoneset users 116
VPIM Networking recipients 116
web messaging users 116
toll fraud, preventing 220, 221
topology. *See* network setup
training users
to address integrated sites 41
to address open sites 42
transmission time of messages
AMIS Networking 65
assumptions used to calculate 65
comparison of networking solutions 65
factors affecting 64
NMS 65
voice and text messages compared 66
VPIM Networking 64
VPIM Networking and network traffic 67
Transport Control Protocol/Internet Protocol. *See* TCP/IP
tree view
Message Network Configuration 151
organization of 152
troubleshooting
authentication failures 224
technical support 14
types of sites
integrated 144
open 144
types of system access number 180

U

unauthenticated access restrictions 187
unauthentication mode
  description 218
  enabling 219
  security recommendations 219, 220
  when to use 219
uniform dialing plan
  definition 77
  example 78
unsuccessful delivery of VPIM Networking message 122
upgrade, information required to 162
upgrading existing satellite switches
  using existing ACD-DNs 113
urgent messages 261
  holding time 178
user
  desktop user 41
  teaching to address integrated sites 41
  teaching to address open sites 42
  telephone user 41
  terminology note 38
  terminology used in guide 41
User Administration
  adding temporary remote users 70
user guides 12
user ID and password authentication
  and SSL 231
  description 223
user location
  and CDP dialing plan 110
  and ESN dialing plan 110
  corresponds to several switch locations 110
  corresponds to switch location 110
  definition 106
users and broadcast messages
  capabilities 99

V

validation
  levels of 154
validation, CallPilot Manager 154
  unique information 155
virtual signaling 106
virtual signaling capabilities and NMS 61
voice channel 159
voice channel type 173
voice encoding 130
voice message type support 38
Voice Profile for Internet Mail (VPIM) 23
Voice Profile for Internet Mail. *See* VPIM
VPIM (Voice Profile for Internet Mail) 23
VPIM address
  compared with e-mail address 119
  example 119
  left-hand side 120
  parts 119
  restrictions 120
  right-hand side 120
VPIM message
  contents 120
  encoding of parts 120
  header 120
VPIM Networking 59
  and dialing plans 163
  and Meridian Mail Net Gateway 215
  broadcast messages 101, 103
  description 141
  desktop and telephone users 120
  Entrust encryption 215
  impact of text on message transmission time 66
  impact on LAN load 59
  implementation checklists 236
  implicit open sites 144
  message delivery 60
  Message Delivery Configuration page, CallPilot Manager . 149
  message delivery notification 124
  message length supported 40
  message transmission time and network traffic 67
  message transmission time traffic calculations 67
  message types supported 39
  planning and engineering considerations 59
  protocols used 127
  recipients, time zone conversions (Network Message Service) 116
  relationship to data network 119
  security and firewalls 214
  TCP/IP 125
VPIM Networking, server FQDN of remote site 205
VPIM open shortcuts
  compared with SMTP/VPIM network shortcut 121
  relationship to server FQDN 122
VPIM systems and encryption 232
VPIM Version 2
  conformance 130

W

web messaging users
  authentication failures, description 225
  time zone conversions (Network Message Service) ... 116
web server
  and CallPilot server integration, diagram 148
  CallPilot Manager 148
worksheets, configuration 157, 237

CallPilot
Network Planning Guide

Copyright © 2004 Nortel Networks. All Rights Reserved.

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: 555-7101-102
Product release: 3.0
Document release: Standard 1.0
Date: November 2004

NORTEL NETWORKS™